Computer Science & Information Technology 72

Dhinaharan Nagamalai
Abdúlkadir ÖZCAN (Eds)

Computer Science & Information Technology

3rd International Conference on Artificial Intelligence and Soft Computing
(AIS 2017)
August 26~27, 2017, Dubai, UAE

Volume Editors

Dhinaharan Nagamalai,
Wireilla Net Solutions, Australia
E-mail: dhinthia@yahoo.com

Abdúlkadir ÖZCAN,
Professor, KTO Karatay University, Turkey
Email : akadirzcn@gmail.com

Preface

The 3rd International Conference on Artificial Intelligence and Soft Computing (AIS 2017) was held in Dubai, UAE, during August 26~27, 2017. The 4th International Conference on Computer Science and Information Technology (CSIT-2017), The 3rd International Conference on Image Processing and Pattern Recognition (IPPR 2017), and The 6th International conference on Parallel, Distributed Computing and Applications (IPDCA 2017) was collocated with The 3rd International Conference on Artificial Intelligence and Soft Computing (AIS 2017). The conferences attracted many local and international delegates, presenting a balanced mixture of intellect from the East and from the West.

The goal of this conference series is to bring together researchers and practitioners from academia and industry to focus on understanding computer science and information technology and to establish new collaborations in these areas. Authors are invited to contribute to the conference by submitting articles that illustrate research results, projects, survey work and industrial experiences describing significant advances in all areas of computer science and information technology.

The AIS-2017, CSIT-2017, IPPR-2017, IPDCA-2017 Committees rigorously invited submissions for many months from researchers, scientists, engineers, students and practitioners related to the relevant themes and tracks of the workshop. This effort guaranteed submissions from an unparalleled number of internationally recognized top-level researchers. All the submissions underwent a strenuous peer review process which comprised expert reviewers. These reviewers were selected from a talented pool of Technical Committee members and external reviewers on the basis of their expertise. The papers were then reviewed based on their contributions, technical content, originality and clarity. The entire process, which includes the submission, review and acceptance processes, was done electronically. All these efforts undertaken by the Organizing and Technical Committees led to an exciting, rich and a high quality technical conference program, which featured high-impact presentations for all attendees to enjoy, appreciate and expand their expertise in the latest developments in computer network and communications research.

In closing, AIS-2017, CSIT-2017, IPPR-2017, IPDCA-2017 brought together researchers, scientists, engineers, students and practitioners to exchange and share their experiences, new ideas and research results in all aspects of the main workshop themes and tracks, and to discuss the practical challenges encountered and the solutions adopted. The book is organized as a collection of papers from the AIS-2017, CSIT-2017, IPPR-2017, IPDCA-2017.

We would like to thank the General and Program Chairs, organization staff, the members of the Technical Program Committees and external reviewers for their excellent and tireless work. We sincerely wish that all attendees benefited scientifically from the conference and wish them every success in their research. It is the humble wish of the conference organizers that the professional dialogue among the researchers, scientists, engineers, students and educators continues beyond the event and that the friendships and collaborations forged will linger and prosper for many years to come.

<div align="right">

Dhinaharan Nagamalai
Abdúlkadir ÖZCAN

</div>

Organization

General Chair

David C. Wyld   Southeastern Louisisna University, USA
Jan Zizka   Mendel University in Brno, Czech Republic

Program Committee Members

Abdelkarim Mars   Alpes University, France
Ahmad Rawashdeh   University of Central Missouri, United States
Ahmed Korichi   University of Ouargla, Algeria
Amal Al-Dweik   Palestine Polytechnic University, Palestine
Antonia Plerou   Ionian University, Greece
Asma Ayed Al Drees   King Khalid University, Saudi Arabia
Atallah M, AL-Shatnawi   Al al-Byte University, Jordan
Azeddine Chikh   University of Tlemcen, Algeria
Biing-Feng Wang   National Tsing Hua University, Taiwan
Dabin Ding   University of Central Missouri, United States
David Defour   University of Perpignan, France
Dawei Li   Temple University, USA
Deron Liang   National Central University, Taiwan
Dongfang Zhao   University of Nevada, USA
Dongpo Xu   Northeast Normal University, China
Efthimios Alepis   University of Piraeus, Greece
Elaheh Pourabbas   National Research Council, Italy
Emad Awada   Applied Science University, Jordan
Erman Cakit   Aksaray University, Turkey
Fatma A. Omara   Cairo University, Egypt
Feng Yan   University of Nevada, USA
Fernando Bobillo   University of Zaragoza, Spain
Ferran Torren   Universitat de Girona, Girona
Gammoudi Aymen   University of Tunis, Tunisia
George C Fletcher   Harvard University, USA
Gerassimos Barlas   American University of Sharjah, UAE
Ghasem Mirjalily   Yazd University, Iran
Gonzalo Hernandez   University of Santiago, Chile
Guey-Yun Chang   National Central University, Taiwan
Guilherme Galante   Western Parana State University, Brazil
Hamid Alasadi   Basra University, Iraq
Hamzeh Boul   Universiti Teknologi Petronas, Malaysia
Hang Zhou   Shanghai University, China.
Hao Ji   California State Polytechnic University, USA
Hayet Mouss   Batna Univeristy, Algeria
Hongyang Sun   Ens De Lyon University, France
Horacio Paggi   Universidad Politecnica de Madrid, Spain

Irtefaa A. Neamah	University of Kufa, Iraq
Isa Maleki	Islamic Azad University, Iran
Ismail Abdullah Hasan Humied	University of Modern Sciences, Yemen
Ismail Elbazi	Hassan 1st University, Morocco
Ivana Cardial de M. Pereira	Federal University of Rio de Janeiro, Brazil
Jamal El Abbadi	Mohammadia V University Rabat, Morocco
James Smith	Webscale Networks, USA
Jang-Eui Hong	Chungbuk National University, South Korea
Jingyan Wang	New York University, UAE
John Tass	University of Patras, Greece
Jun Zhang	South China University of Technology, China
Ken Ehimwenma	Sheffield Hallam Umivetsity, United Kinkdom
khidir Shaib Mohamed	Dalian University of Technology, China
Lenka Vyslouzilova	Czech Technical Univerzity, Czech Republic
Liana Duenha	University of Mato Grosso do Sul, Brazil
Liangxiao Jiang	University of Geosciences, China
Mahdi Salarian	University of Illinois, USA
Majid Moradi Zirkohi	Behbahan University of Technology, Iran
Marat Akhmet	Middfle East Technical University,Turkey
Martins Irhebhude	Nigerian Defence Academy, Nigeria
Masnida Hussin	University Putra Malaysia, Malaysia
Md Forhad Rabbi	Curtin University, Australia
Minho Lee	Kyungpook National University, Korea
Mohamedmaher Benismail	King Saud University, Saudi Arabia
Mohammad alsarem	Taibah University, KSA
Mostafa Ashry	Alexandria University, Egypt
Mostafa Ghobaei Arani	Islamic Azad University, Iran
Ramgopal Kashyap	Sagar Institute of Science and Technology, India
Rana Rahim	Lebanese University, Lebanon
RandaHerzallah	Aston University, United Kinkdom
Ranesh Kumar Naha	University Putra Malaysia, Malaysia
Sotos Kotsiantis	University of Patras, Greece
Soujanya	Nanyang Technological University, Singapore
Stephan	Alpen-Adria Universitat Klagenfurt, Austria
Taeghyun Kang	University of Central Missouri, United States
Tak-Lam Wong	The Education University of Hong Kong, China
Truong Huu Tram	National University of Singapore, Singapore
Uri J. Schild	Bar Ilan University, Israel
Wonjun Lee	The University of Texas at San Antonio, USA
Xuechao Li	Auburn University, USA
Yang Wang	Shenzhen Institutes of Advanced Technology, China
Yonggui Kao	Harbin Institute of Technology, China
Yu Sun	California State Polytechnic University, USA
Yun Tian	Eastern Washington University, USA
Yu-Sheng Su	National Central University, Taiwan
Zaid Hussain	Kuwait University, Kuwait
Zhang jianhong	North China University of technology, China
Zhao Peng	Huazhong University of Science and Technology, China

Technically Sponsored by

Computer Science & Information Technology Community (CSITC)

Artificial Intelligence Community (AIC)

Soft Computing Community (SCC)

Organized By

Academy & Industry Research Collaboration Center (AIRCC)

TABLE OF CONTENTS

3rd International Conference on Artificial Intelligence and Soft Computing (AIS 2017)

4th International Conference on Computer Science and Information Technology (CSIT-2017)

3rd International Conference on Image Processing and Pattern Recognition (IPPR 2017)

6th International conference on Parallel, Distributed Computing and Applications (IPDCA 2017)

COMPUTER AIDED LIVER TUMOUR DETECTOR – CALTD

Thayalini Prakash

Department of Software Engineering, University of Westminster, UK

ABSTRACT

Computer-aided liver tumour detection can comfort the radiologists to detect the liver tumours from the abdominal CT image. This research proposes a software solution to illustrate the automated liver segmentation and tumour detection using artificial intelligent techniques. Evaluate the results of the liver segmentation and tumour detection, in-cooperation with the radiologists by using the prototype of the proposed system. This research overcomes the challenges in medical image processing. The 100 samples collected from ten patients and received 90% accuracy rate.

KEYWORDS

CT abdominal image, Image processing, liver segmentation, Tumour region extraction

1. INTRODUCTION

Nowadays, the medical world moving towards to advance technologies to screen the liver tumour, such as Ultrasound, MRI and CT scans. As stated by Radiological Society of North America, Inc., 2010; the CT imaging is one of the finest and fastest techniques to identify the abdominal and pelvis due to high-quality, also screening the cross-sectional view of entire tissue. On top of this, fully-automated system for remedial diagnoses is getting demand among medical experts. This research engages to overcome the existing problem and propose an automated liver segmentation and tumour detection solution.

2. METHODOLOGY

2.1. Liver Segmentation

Identifying liver from CT abdominal image is generally a challenging task due to other organs with same intensity as liver, adjacent to the liver makes segmentation more difficult. Nonetheless, as define by Zayane. O, et al., (2011), and according to the anatomic studies (Abrahams, P., 2002), the liver is constantly locates at the upper right side of the abdomen and takes up the largest area among the various organs included in the abdomen image. In this experiment liver region will be extracted by using the following 2 steps.

In the first step: Using anatomical knowledge of the liver and histogram analyser, adaptive threshold is fixed to extract the liver pixels from the CT abdominal image which usually contains other organs including stomach, kidney, spleen, pancreas, etc.

In the second step: Morphological operations like closing and opening operations are used to preserve the structure of the liver and to remove the small fragments of other organs adjacent to the liver with the same intensity as that of liver.

This research recommends the following approaches to segment the liver and tumour region with more affluence and accurate manner. The original CT abdomen image has been processed through the steps as shown in the below illustration.
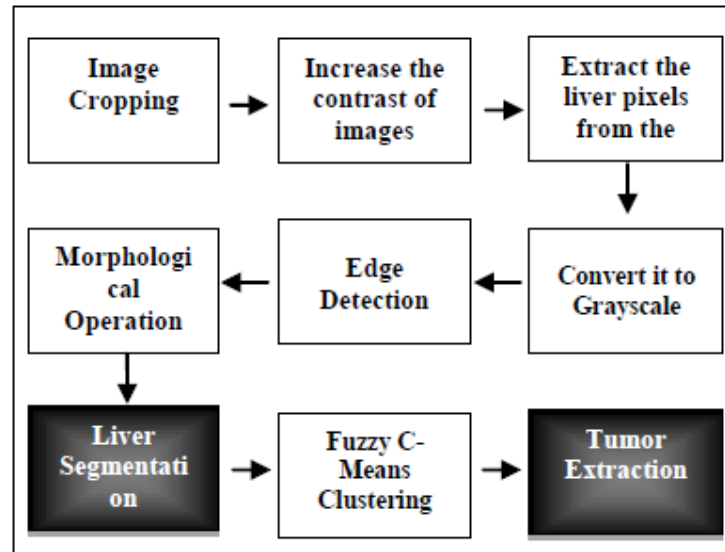
Figure 1: Automatic Liver and Tumour Region Extraction Approach

2.1.1. Image Cropping

Each image was cropped before any processing or visualization was performed. The main reason for doing this was to decrease the computational time, but there was also the added benefit in that focuses on only the target area liver and it became the main organ in each image. Each image was cropped at rows 30 and 190 and columns 15 and 240. Referring to figure 2, it can be seen how cropping the image resulted in placing the liver as the focus of the CT scan. For the CT abdominal image, Resize the input image and a window is fixed by using cropping technology to remove the last 30 rows and 15 columns from the right since this area usually does not contain liver region.

The liver is extracted along with the fragments of other organs located near to it and with the intensity same as that of liver. Based on certain conditions, the fragments of adjacent organs can be removed.

The first condition is the location of the object: The liver is placed at a constant area in the upper right side of the image.

The second condition is the area: The area of the liver is large when it is compared with the fragments of other organs. After removing the fragments, the image obtained is complemented and multiplied with the original image to get the segmented liver in the CT abdominal image.

2.1.2. Histogram Equalization

Histogram Equalization works by improving the contrast of images by stretching the intensity distribution of the image or by changing the values in a colour map being used. An image can then be produced that approximately matches the specified histogram. The image that received by running a Histogram Equalization on this image can be seen in Figure 2. The change is quite noticeable as this slice is the same slice. It can be seen that the image detail is more apparent and that the tumour and blood vessels can be seen much more easily than before. It is experimented with 100 images and supported with 90% accurate.

2.1.3. Adaptive threshold

The liver region maintains a constant intensity throughout, a fixed threshold is impossible because the intensity differ from patient to patient also depends on the quality of a CT image. Therefore, a system has to be developed to extract the liver automatically with the adaptive threshold decision.

The threshold is called adaptive threshold when a different threshold is used for different regions in the image, as stated above, can't use the same threshold for the entire image, thus this research recommends that the adaptive threshold is appropriated.

2.1.4. Convert it to Grayscale

Converts the true colour image RGB to the grayscale by eradicating the hue and saturation information while retentive the luminance. RGB values to grayscale values by calculating a prejudiced sum of the R, G, and B components:

$0.2989 * R + 0.5870 * G + 0.1140 * B$

2.1.5. Edge detection

Yu-qian.Z., et al. (2005) recommended a novel mathematic morphological algorithm for lung detection from CT image. They acknowledged that, this is as a better algorithm for medical image detection and de-noising than the template-based edge detection algorithms and general morphological edge detection algorithm. Nevertheless, Hiransakolwong et al., (2003), and Maini.R and Sobel.J.S., (2006), proposed the Sobel edge detection for medical image segmentation. However, according to the author's experiments of edge detection algorithms for 100 samples, "Sobel" supports 80% while "Canny" supports 40%. As a result, this research recommends the "Sobel" algorithm for liver segmentation.

2.1.6. Morphological Operation

Morphological operation has been applied in the research as part of the liver segmentation process; the octagonal structuring element approach segmented with only 30% of accuracy, for another 70% of images segmented both liver and kidney. However, disk-shaped structuring element approach supports with 70% accuracy. This research recommends the disk function based on the experimental result.

Erode image - Erode the filled image so as to leave just the liver. Each image was eroded using a disk of size 20 to erode with. Create morphological structuring element.

Erodes the grayscale, binary, or packed binary image, returning the eroded image. The argument se is a structuring element object or an array of structuring element objects returned.

If a binary image is logical and the structuring element is flat, performs binary erosion; otherwise it performs grayscale erosion. If structuring element is an array of structuring element objects, performs multiple erosions of the input image, using each structuring element in succession.

Multiplied with original CT abdominal Image, Modified regional maxima super imposed on the original image.

2.2. Tumour Extraction

Automatic tumour extraction also a challenging task, due to variety of difficulties such as tumour shape variations, low contrast between tumour tissue and normal liver tissue, different tumour imaging characteristics at different CT scanning phases.

Hong. J.S, et al. (2001) proposed a CAD system based on Fuzzy C Means Clustering for liver tumour extraction with an accuracy of 91% using features like area, circularity and minimum distance from the liver boundary to tumour and Bayes classifier for classifying normal and abnormal slice. Also, Lee.C.C, et al. (2003) identified liver region by using the fuzzy descriptors and fuzzy rules constructed using the features like location, distance, intensity, area, compactness and elongated-ness from CT abdominal images.

From the liver, tumour region is segmented using, FCM clustering technique. FCM minimizes the object function through the iterative optimization of the membership function based on the similarity between the data and the centre of a cluster. FCM varies the threshold between clusters through an iterative process. As a result, the threshold is determined appropriate for every slice and the tumour region can be successfully extracted.

The pixels of the input image are divided into three clusters. The first cluster includes pixels in the background (low intensity). The second cluster includes pixels in the tumour region (medium intensity) and the third cluster includes pixels in the liver region other than tumour (high intensity). The tumour region is outputted for further analysis.

2.2.1. Otsu's method

The graythresh function uses the Otsu's method, which chooses the threshold to minimize the intraclass variance of the black and white pixels.

2.2.2. Outline the Liver in original Image

The Liver region would be highlighted through draw a skeleton on the segmented liver potion. The outline is shaped by the bwperim function. Imoverlay function also does the same process but it won't support to 3D images that's why unable to apply this function. Also, Segout is reassigned as the cropped image and then the outline places on the cropped image.

2.2.3. Texture Feature Extraction

Texture feature is a commonly use characteristics in medical image interpretation, also applicable to a variety of image processing problems. However, John.E.K et al, (1999) stated that, the tissues are expected to have consistent and homogeneous textures along with the series of slices. Therefore, texture information can be practiced to categorize among different organ's tissues. Also, gray level co-occurrence matrices estimate the properties of images related to second-order statistics. The Gray level co-occurrence matrices are known as a widely used approach for texture

analysis, Kurani. A.S. et al. (2004) recommended the GLCM techniques for better feature extraction.

3. EXPERIMENT

The approach has been experimented with CT abdomen image and the expected result was archived. The experiment results as shown below:
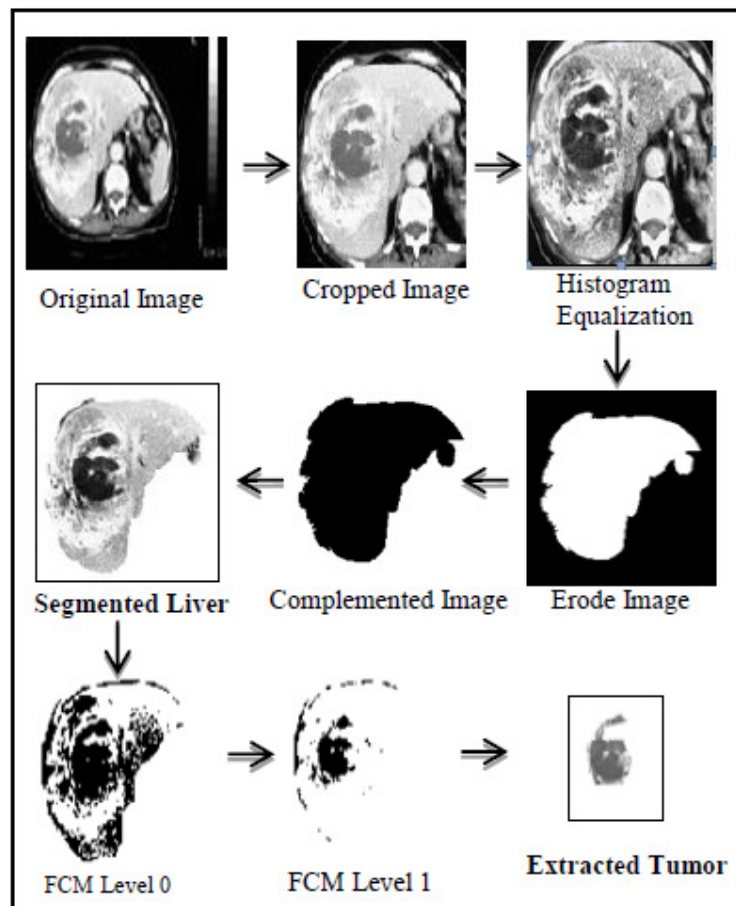
Figure 2: Experiment Result

4. EVALUATION

Each sub modules are experimented separately with 100 samples and the experiment result received as follows: the pre-processing stage, Change the size, contrast of the Image given 96% accuracy and Main experiment of the research; liver segmentation from the inputted CT abdomen image successfully resulted with 90% accuracy, likewise, another major task, extract the tumour region from segmented liver image achieved with 92% accuracy, Finally Extract the value of mean, standard, homogeneity, entropy, energy, contrast, correlation also resulted as expected with 94% accuracy level.

The performance and accuracy of end product evaluated with the support of radiologists, such as accuracy, predictability, usability, functionality, user interface and user friendliness. Additionally, the concept and technology of the product are evaluated by the computer technical experts.

Finally, the most important factor of a medical product, 'accurately' assessed with 100 CT abdomen images gathered from ten different patients, and received 90% of accuracy. The bellows formula practiced to figure out the accuracy level.

$$Accuracy = \frac{Total\ No\ of\ Correctly\ Segmented\ Image}{Total\ No\ of\ Tested\ Image} * 100$$
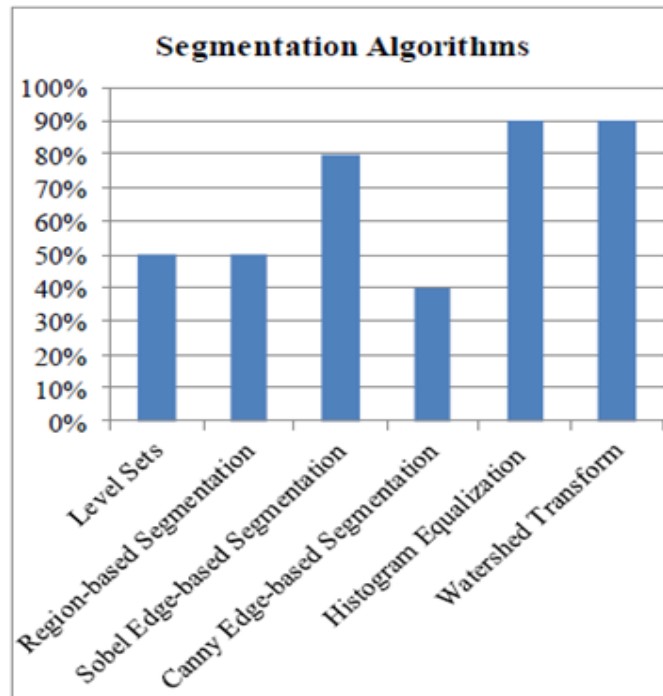
Figure 3: Evaluation Result

According to the experiment and evaluation result, out of these above technologies Sobel Edge detection, Histogram Equalization, Watershed Transform methods are recommended by the author as part of the process of automatic liver segmentation from CT abdomen images. Further, Region-based segmentation appropriate for semi-automatic approach and Level set algorithm works as semi-automatic; it will detect the liver when the user manually clicks on the liver area. However it's segmented the liver with some other organs.

5. CONCLUSION

In this research, the liver region automatically segments from CT abdominal images, using the anatomical knowledge of the liver, adaptive threshold decision based on intensity information and morphological processing in watershed method. Tumour region extracts by using Fuzzy C Means Clustering (FCM). Gray Level Co-occurrence Matrix practice for extract the texture features. All these technologies and algorithms are well examined and critically evaluated.

6. RECOMMENDATION

Recommend to expand this research up to classify the tumour category and compute the size of the tumour in the future. It might help to reduce the radiologist's work load.

REFERENCES

[1]   Abrahams, P., 2002. The Atlas of the Human Body. 2nd ed. San diego, California, USA: Bright Star Publishing Plc.

[2]   Hiransakolwong.N., Windyga.P.S., Hua.K.A., and Khanh.V., 2003. Segmentation of ultrasound liver images: an automatic approach. [Online] Available at: http://www.computer.org/portal/web/csdl/doi/10.1109/ICME. 2003.1220982 [Accessed 10 Dec 2012].

[3]   Hong.J.S., Kaneko.T., Sekiguchi.R., and Houmpark.K.,(2001). Automatic Liver Tumor Detection from CT. IEICE Trans. Inf.& Syst, E84-D(6), pp. 741-748.

[4]   John.E.K., Newman. F.D., Johnson.T.K., and Kirch. D.L., 1999. Abdominal Organ Segmentation Using Texture Transforms and a Hopfield Neural Network. IEEE Transactions on Medical Imaging, 18(7), pp. 640-648.

[5]   Kurani AS, Xu DH, Furst J, Raicu DS., 2004. Co-occurrence Matrices for Volumetric Data. Hawaii, USA, s.n.

[6]   Lee.C.C, Chung.P.C., and Tsai.H.M., 2003. Identifying Abdominal organs from CT image series using a Multimodule Contextual Neural network and Spatial Fuzzy rules. IEEE Transactions on Information Technology in Biomedicine, 7(3), pp. 208-217.

[7]   Maini.R and Sobel.J.S., 2006. Performance Evaluation of Prewitt Edge Detector for Noisy Images. GVIP Journal, 6(3).

[8]   Mala.K., Sadasivam.V., and Alagappan.S., "Neural Network based Texture Analysis of Liver Tumour from Computed Tomography Images," World Academy of Science, Engineering and Technology International Journal of Medical, Health, Biomedical, Bioengineering and Pharmaceutical Engineering Vol:2, No:1, 2008.

[9]   Radiological Society of North America, Inc., 2013. RadiologyInfo.org. [Online] Available at: http://www.radiologyinfo.org/en/about/index.cfm?pg=abt_co pyrt [Accessed 16 Mar 2013].

[10] Yu-qian.Z., Wei-hua.G., Zhen-cheng.C., Jing-tian.T., Ling-yun.L., 2005. Medical Images Edge Detection Based on Mathematical Morphology. IEEE - Engineering in Medicine and Biology Society, p. 6492 – 6495.

[11] Zayane.O., Jouini1.B., and Mahjoub.M.A., 2011. Automatic liver segmentation method in CT images. Canadian Journal on Image Processing & Computer Vision, 2(8).

AUTHOR

Thayalini Prakash,
BSc (Hons) Software Engineering, MBA, MBCS
t.piragash@gmail.com

INTENTIONAL BLANK

LEAN LEVEL OF AN ORGANIZATION ASSESSED BASED ON FUZZY LOGIC

A. Abreu[1] and J. M. F. Calado[2]

[1,2]Mechanical Engineering Department, ISEL - Instituto Superior de Engenharia de Lisboa, IPL – Polytechnic Institute of Lisbon Rua Conselheiro Emídio Navarro, 1, 1959-007 Lisboa, Portugal
[1]CTS - Uninova – Instituto de Desenvolvimento de Novas Tecnologias
[2]IDMEC/LAETA, Instituto Superior Técnico – Universidade de Lisboa

ABSTRACT

To determine the lean level of an organization a methodology was developed. It was based on a qualitative assessment approach, including quantitative basis, whose development was supported using fuzzy logic. Recourse to the use of fuzzy logic is justified by its ability to cope with uncertainty and imprecision on the input data, as well as, could be applied to the analysis of qualitative variables of a system, turning them into quantitative values. A major advantage of the developed approach is that it can be adjusted to any organization regardless of their nature, size, strategy and market positioning. Furthermore, the proposed methodology allows the systematically identification of constraint factors existing in an organization and, thus, provide the necessary information to the manager to develop a holistic plan for continuous improvement. To assess the robustness of the proposed approach, the methodology was applied to a maintenance and manufacturing aeronautical organization.

KEYWORDS

Data-driven decision making; Fuzzy systems in business and economy; Management of competences and knowledge; Business analytics; Lean organization.

1. INTRODUCTION

Currently, markets are increasingly globalized and competitive, being constantly changing and evolving. It is in this context that companies to survive are seeking instruments to ensure their productivity gains and competitive advantages, allowing an effective and efficient management of competences based on knowledge supported by data-driven decision approaches. So many companies adopt lean thinking or lean philosophy as a survival strategy. However, according to Bashin and Burcher [1], more than 90% of companies that have been applying lean tools and methodologies show shortcomings in the evaluation of their improved performance. The causes cited for this gap in the evaluation of performance improvements resulting from the lean approach implementation, are largely due to a lack of understanding of the concept of lean performance and appropriate models to monitor, evaluate and compare the evolution of "lean level" during the corresponding implementation process [2, 3].

The lack of a clear understanding about what is lean performance and its evaluation is one of the reasons for lean programs implementation have failed. In other words, it is not possible to manage the lean level of an organization without measuring its performance. According to Pakdil and

Leonard [4], although there are several different methods of measuring the various perspectives of lean production, in literature there is no holistic assessment approach to determine the level of implementation of lean thinking in organizations. We can find in the literature several definitions for the term "lean level" of an organization. For example, Wan and Chen [5] defines the "lean level" as the performance level of the stream value compared to perfection, or according to Bayou and De Korvin [6], the "lean level" is the measure of the implementation of lean practices. Thus, one of the major challenges facing this area, it is related with the development of models to assess and validate the effectiveness and efficiency of lean thinking implementation in organizations.

As a general criticism of lean assessment methods described in the literature, we can see that each method of evaluation focuses only on a specific lean dimension and not on its entirety [6]. On the other hand, while some methods focus on the perceptions of employees, using a qualitative approach [7]; others use various performance metrics, creating a quantitative assessment [2, 5, 6]. However, none of the existing studies use qualitative and quantitative approaches simultaneously [4]. According to some authors, lean assessment methods can be categorized into four groups: Value Stream Mapping (VSM), Qualitative Assessment Tools, Performance Indicators and Benchmarking [3, 5].

Currently most organizations use qualitative evaluation methods based on questionnaires or a group of metrics used simultaneously to determine the level of application/implementation of the methodologies and lean tools. The challenge of using performance indicators and metrics concerned with the assessment of the lean level of an organization, it is the ability to define a set of indicators including all dimensions of the lean approach [8]. Furthermore, the synthesis of a set of indicators in a single lean metric is also in itself a challenge due to the different measurement units [9].

Furthermore, it is worth to mention that the number of studies in literature on leanness assessment is low when compared to that in the area of lean implementation. However, the approach proposed in this paper follows the trend of lean thinking assessment literature, which is getting transformed from process-level monitoring to enterprise-level monitoring [14]. The recently published material about leanness assessment revealed that future studies in this domain would fall into two major categories, namely manufacturing leanness assessment and service leanness assessment. Thus, the framework of the proposed approach has been developed with the aim to cope with both scenarios; manufacturing and service enterprises.

In this context, this paper presents a model based on fuzzy logic that aims to determine the lean level of an organization, facing the challenges mentioned above and trying to overcome the corresponding difficulties, which could be seen as a modelling and decision making tool for complex systems.

Hence, the paper is structured as follows: Section 2 presents a detailed description of the lean assessment approach proposed in this paper; to assess the robustness of the proposed method, on Section 3 is described its application to a case study and a critical analysis of the achieved results is provided; Section 4 includes some concluding remarks.

2. LEAN ASSESSEMENT MODEL

The proposed model aims to permit an assessment of lean practices, determining the lean level of an organization and to identifying the main constraints. Accordingly, the model developed utilizes the concept of fuzzy logic using triangular membership functions, to integrate both performance evaluation strands, either quantitative or qualitative in a single index, as well as to be a model able to cope with ambiguity and uncertainty of human evaluation. Thus, the model comprises the following elements:

- Model Structure - Definition of dimensions, criteria and attributes;

- Definition of linguistic variables and membership functions;

- Indicators of lean performance of an organization - Construction of fuzzy indicators to determine the lean level of an organization and to identify the main constraints.

2.1. Model Structure

The model architecture consists of three levels of granularity that are called, dimensions, criteria and attributes, as shown in Figure 1. At the first level, it was defined three dimensions of analysis – "Customers"; "Suppliers"; and "Organization". The second level comprises thirteen criteria and in the third level are defined one hundred of attributes.

Table 1 shows the attributes defined for the criterion "5S and Visual Management". The identification of dimensions' criteria and attributes were based on the literature reviewed. Each of the elements corresponds to an indicator of lean performance, from which the lean level of the organization will be achieved.
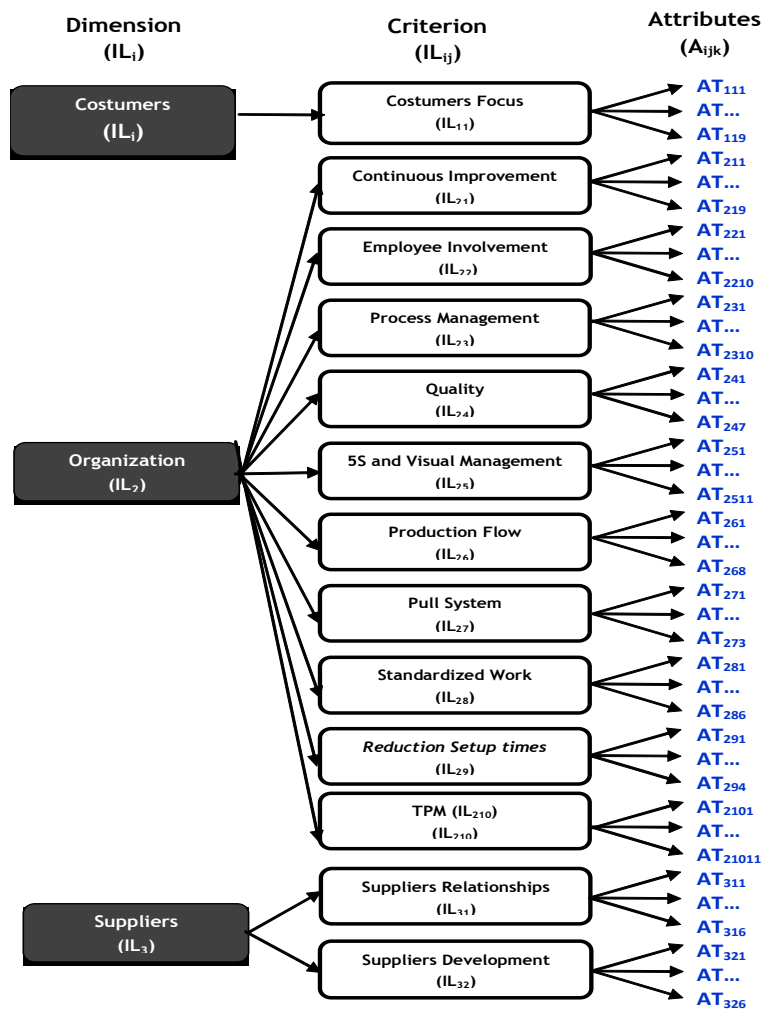

Figure 1. The model structure.

2.2. Fuzzy Sets and Membership Functions

Imprecision of the human systems is due to the imperfection of knowledge that human receives (observation) from the external world. Imperfection leads to a doubt about the value of a variable, a decision to be taken or a conclusion to be drawn for the actual system. Fuzzy logic deals with uncertainty and imprecision, and is an efficient tool for solving problems where knowledge uncertainty may occur. Imprecise and uncertain values are usually expressed by means of linguistic terms, especially when they have been provided by or for a human being, However, the ad-hoc use of linguistic terms and the corresponding membership functions is always criticized in applications where fuzzy logic is used [10]. Thus, for the sake of convenience, rather than making our own definition of linguistic terms, the adoption of linguistic terms and the corresponding membership functions was chosen from the literature [10, 11, 12, 13].

In general, it is suggested that the linguistic terms to represent the behaviour of a linguistic variable do not exceed nine terms, which represent the discrimination limits of human perception [10]. Based on the literature in the field of fuzzy logic [10, 11, 12, 13] the following linguistic terms or fuzzy sets {Excellent (E), Very Good (VG), Good (G), Satisfies (S), Satisfies Little (SL), Insufficient (I) and Weak (W)} were adopted to characterize the performance rating and it has been selected the linguistic terms {Very High (VH), High (H), Moderately High (MH), Medium (M), Moderately Low (ML), Low (L) and Very Low (VL)} to characterize the weighting factors, as illustrated in Table 2. The corresponding membership functions have been defined using triangular functions represented by 3-tuples (a, b, c), with parameters a < b < c and b representing the middle point.

Defined the fuzzy sets and the corresponding membership functions, one can now define the relative importance of each element (size, criterion and attribute), based on the strategy and policy of the organization, trend of competition, technological development, knowledge and experience of specialists [10].

Table 1. 5S Visual Management Attributes.

Dimension	Criterion	Attributes
Organization	5S and Visual Management	AT_{251} - The working environment is clean, organized and safe. AT_{252} - Products / materials used are identified and a visual supervision exists. AT_{253} -Tools are organized and can be managed based on a visual system. AT_{254} -Visual devices are used to inform the workload distribution and the production scheduling. AT_{255} - Andon panels are used to inform the working stations that are stopped or who need help. AT_{256} - The process flow is well-defined, and it is clear. AT_{257} - Periodic audits are taken place to assess 5S system and corrective actions are implemented whenever necessary. AT_{258} - Audit evaluation to the 5S's system is made public and posted. AT_{259} -The maintenance plan has well defined the periodicity to clean equipment and tools. AT_{2510} - Information boards in a visible place with updated information are used. AT_{251} -Safety signs are used for prevention of industrial accidents.

Table 2. Fuzzy Sets and Membership Functions.

Performance Rating (*A*)		Weighting Factor (*W*)	
Fuzzy Set	*Membership Function*	*Fuzzy Set*	*Membership Function*
E	(8.5; 9.5; 10)	VH	(0.85; 0.95; 1)
VG	(7; 8; 9)	H	(0.7; 0.8; 0.9)
G	(5; 6.5; 8)	MH	(0.5; 0.65; 0.8)
S	(3; 5; 7)	M	(0.3; 0.5; 0.7)
SL	(2; 3.5; 5)	ML	(0.2; 0.35; 0.5)
I	(1; 2; 3)	L	(0.1; 0.2; 0.3)
W	(0; 0.5; 1.5)	VL	(0; 0.05; 0.15)

2.3. Performance Indicators of Lean Level

This subchapter presents a detailed description of the performance metrics used to assess the lean level of an organization under the approach proposed in this paper. Thus, the following Performance Indicators (all of them being fuzzy variables) have been considered and used in the case study presented below:

- Aggregated Lean Index for each criterion (LI_{ij}) - According to the definition of weighted average the Aggregated Lean Index, LI_{ij}, can be calculated through W_{ijk} and A_{ijk} variables, representing, respectively, the fuzzy weighting factors associated with each attribute (n) and the fuzzy performance ratings, by using the equation (1):

$$LI_{ij} = \frac{\sum_{k=1}^{n}(W_{ijk} x A_{ijk})}{\sum_{k=1}^{n} W_{ijk}}$$

(1)

- Aggregated Lean Index of each dimension (LI_i) - Obtained the Aggregated Indexes for each criterion, now there is a need to integrate the values of the various criterions (*m*) in a single index, associated with a dimension, by using the equation (2):

$$LI_i = \frac{\sum_{j=1}^{m}(W_{ij} x LI_{ij})}{\sum_{j=1}^{m} W_{ij}}$$

(2)

Where W_{ij} is the fuzzy weighting factor associated with each criterion and LI_{ij} is the aggregated fuzzy index associated also with each criterion.

- Performance Lean Index (*PLI*) – Obtained the LI_i, then the Performance Lean Index can be calculated using the equation (3). The *PLI* is a holistic fuzzy lean index consolidating in a single index the evaluations and the weighting factors. Thus, the *PLI* represents the global lean level of an organization, where W_i represents a fuzzy weighting factor and LI_i stands for the aggregated lean index associated with each dimension (*l*).

$$PLI = \frac{\sum_{i=1}^{l}(W_i x LI_i)}{\sum_{i=1}^{l} W_i}$$

(3)

- Lean Level of an Organization (*LLO*) – Evaluated the *PLI*, now the corresponding fuzzy value can be associated with a linguistic variable with a membership function equal or close to the membership function associated to *PLI*. There are several methods to associate the membership function achieved to characterize the *PLI* with a pre-defined linguistic variable. However, it is recommended the use of the Euclidean distance method, since it is the most intuitive perception of human proximity [12]. The Euclidean distance method consists into determine the Euclidean distance between the

obtained membership function and each pre-defined membership functions associated with each linguistic variable. Being the lean level (*LL*) characterized by fuzzy sets with triangular membership functions, represented by 3-tuples (*a*, *b*, *c*), then, the Euclidean distance between the triangular membership function associated with the fuzzy set *PLI* and each membership function associated with the fuzzy sets pre-defined to characterize the fuzzy variable *LL*, can be calculated using the equation (4):

$$d(PLI, LL_i) =$$

$$= \sqrt{\frac{1}{3}[(a_2 - a_1)^2 + (b_2 - b_1)^2 + (c_2 - c_1)^2]} \qquad (4)$$

With the aim to characterize the behaviour of the fuzzy variable *LL*, it was used and defined the fuzzy sets and the corresponding membership functions presented in Table 3.

To identify the main constraints to improve the organization's lean level, it is proposed the fuzzy Importance-Performance Index (*IPI*) [10]. According to this index, all the attributes that are classified with a high weighting factor (W_{ijk}) and then evaluated having low performance (A_{ijk}), are classified as a critical constraint to improvement.

Thus, in the *IPI* calculation process cannot be used the values assigned to the weighting factors W_{ijk}, but their complementary, $[(1, 1, 1) – W_{ijk})]$, in order to not mask the results. For example, if an attribute is classified with a high W_{ijk} (then, the value of $[(1,1,1) – W_{ijk}]$) will be low) and has a low performance evaluation A_{ijk}, then such an attribute is considered a critical constraint and IPI_{ijk} will take a low value. For each attribute *ijk*, the fuzzy Importance-Performance Index (*IPI*) will be define as follows:

$$IPI = W'_{ijk} \times A_{ijk} \qquad (5)$$

where,

$$W'_{ijk} = (1, 1, 1) – W_{ijk} \qquad (6)$$

and, W_{ijk} stands for a fuzzy weighting factor of each lean attribute.

For two triangular fuzzy numbers the subtraction, addition and multiplication operations are defined as follows:

- Fuzzy number subtraction

$$A_1 - A_2 = (a_1, b_1, c_1) - (a_2, b_2, c_2) = (a_1 - c_2, b_1 - b_2, c_1 - a_2) \qquad (7)$$

- Fuzzy number addition

$$A_1 + A_2 = (a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2) \qquad (8)$$

- Fuzzy number multiplication

$$A_1 \times A_2 = (a_1, b_1, c_1) \times (a_2, b_2, c_2) = (a_1 \times a_2, b_1 \times b_2, c_1 \times c_2) \qquad (9)$$

Calculated the IPI_{ijk} there is now the need to classify it. In this work, it was used the Chen and Hwang's left-and-right fuzzy ranking method, since it not only preserves the sort order, but also considers the absolute location of each fuzzy set [13]. In such a method to defuzify a fuzzy set, the maximum and minimum functions are given as follows:

Table 3. Lean Linguistic Terms - Fuzzy Sets and Membership Functions.

Lean linguistic terms	
Fuzzy sets	*Membership functions*
Extremely Lean (EL)	(7; 8.5; 10)
Very Lean (VL)	(5.5; 7; 8.5)
Lean (L)	(3.5; 5; 6.5)
Reasonably Lean (RL)	(1.5; 3; 4.5)
Little Lean (LL)	(0; 1.5; 3)

$$f_{max} = \begin{cases} x & 0 \leq x \leq 10 \\ 0 & Otherwise \end{cases} \tag{10}$$

$$f_{min} = \begin{cases} 1-x & 0 \leq x \leq 10 \\ 0 & Otherwise \end{cases} \tag{11}$$

According to the above-mentioned method and considering a triangular membership function associated with the characterization of *IPI* and defined as, $f_{IPI}: R \rightarrow [0, 10]$, the left and right indexes are evaluated as follows:

$$U_L(IPI_{ijk}) = sup_x[f_{IPI}(x) \cap f_{min}(x)] \tag{12}$$

$$U_R(IPI_{ijk}) = sup_x[f_{IPI}(x) \cap f_{max}(x)] \tag{13}$$

Then, the total index, which will be a crisp value being given as follows:

$$U_T(IPI_{ijk}) = \frac{U_R + 10 + U_L}{2} \tag{14}$$

3. CASE STUDY – APPLICATION OF THE PROPOSED METHOD

The approach proposed in this paper was applied to an organization concerned with aeronautical maintenance and manufacturing. However, before proceeding to the implementation of the proposed methodology it was carried out a training session to ensure that the evaluators were familiar with the concepts of what is meant by a lean organization to ensure adjusted results to reality. According to the literature, before proceeding to the implementation of the methodology to assess the lean level of an organization it is important to build at early stage a "consensus" with the evaluators on the object that will be subject to evaluation [11]. Defined the linguistic variables and their membership functions and assigned the relative importance of each element, follows the implementation phase of evaluation of the lean organizational performance. The fuzzy sets used to characterize the weighting factors (*w*) have been obtained conducting a Delphy study including a set of several experts in the field of Lean, Quality, Innovation, Project Management, Management, Marketing and Logistics.

Applying equation (1) to the values obtained in the performance evaluation of the organization the values of LI_{ij} are calculated. The LI_{ij} value corresponds to the aggregate index for each of the criterions. Calculated the value for the various LI_{ij} and applying now the equation (2), the values for each dimension LI_i, were obtained. The LI_i value corresponds to the aggregate index for each of the dimensions considered in the proposed approach. The obtained aggregate indices are described in Table 4.

Once obtained the values for the LI_i, then, the *PLI* can be determined applying equation (3), being in the case under study *PLI* = (3.88; 5.50; 7.10). Afterwards, as described in the last section, the determined membership function for *PLI* should be associated with a membership function of one

of the linguistic variables (fuzzy sets) pre-defined to characterize the organization's lean level and described in Table 3. Hence, using the equation (4) and as depicted in Figure 2, the following Euclidean distances between the membership function achieved for *PLI* and each of the membership functions associated with each fuzzy set used to characterize the LLO, have been obtained: *D(PLI, EL)* = 3.01; *D(PLI, VL)* = 1.51; *D(PLI, L)* = 0.50; *D(PLI, RL)* = 2.50; *D(PLI, LL)* = 4.00. Thus, determining the minimum value taken by *D* can be said that the organization's lean level is "Lean", which means that the organization is in an intermediate state of lean performance.

To identify the main constraints to lean improvement, using equation (5) it is possible to calculate the *IPI* for all attributes that were evaluated. For example, the *IPI* for the attribute AT_{251} - the work environment is clean, organized and safe, is calculated as follows:

$$IPI_{251} = [(1; 1; 1) - (0.7; 0.8; 0.9)] \times (3; 5; 7) \tag{15}$$

$$IPI_{251} = (2.1; 1; 0.3) \tag{16}$$

The fuzzy value obtained for the IPI_{251} should now be transformed into a crisp value. Then, through the defuzification method described in the last section, using equation (12), (13) and (14), the quoted crisp value is determined as follows:

$$U_R(IPI_{251}) = 1.89 \tag{17}$$

$$U_L(IPI_{251}) = 9.07 \tag{18}$$

Table 4. Lean Performance Indicators.

IL_i	IL_{ij}
Costumers (4.14; 5.71; 7.27)	Costumers Focus (4.14; 5.71; 7.27)
Organization (3.58; 5.13; 6.67)	Continuous Improvement (3.21; 4.94; 6.65)
	Employee Involvement (3.83; 5.48; 7.11)
	Process Management (4.75; 5.71; 6.73)
	Quality (2.75; 4.30; 5.84)
	5S and Visual Management (3.59; 5.29; 6.93)
	Production Flow (3.86; 5.48; 6.98)
	Pull System (3.71; 5.54; 7.36)
	Standardized Work (3.33; 4.98; 6.58)
	Setup Reduction Times (2.93; 4.78; 6.58)
	TPM (3.49; 4.65; 5.81)
Suppliers (4.15; 5.85; 7.50)	Suppliers Relationship (4.18; 6.03; 7.75)
	Suppliers Development (4.12; 5.68; 7.25)
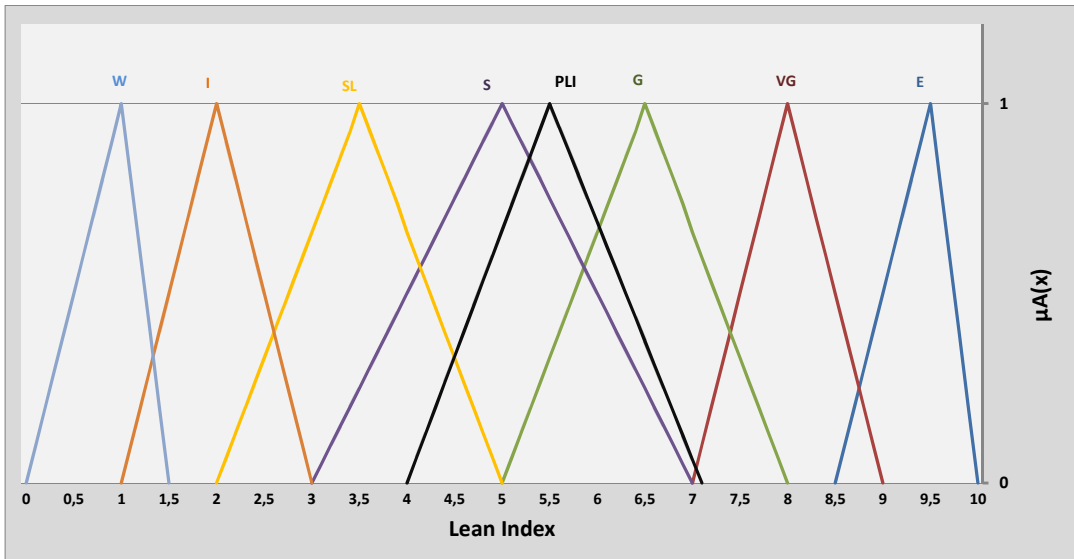
Figure 2. Membership functions of fuzzy sets used to characterize LLO and membership function associated with *PLI*.

$$U_T(IPI_{251}) = \frac{1.892 + 10 - 9.065}{2} = 1.41 \tag{19}$$

Figure 3 illustrates graphically the method used to estimate $U_R(IPI_{251})$ and $U_L(IPI_{251})$.

As mentioned in the Pareto principle, resources should be used to improve the critical constraints [10], and thus based on the literature, the value of 0.8 was established as the threshold to identify the critical constraints that need to be improved. Thus, since the value obtained was 1.41, corresponds to a non-critical constraint, being the critical constraints, all attributes whose value is less than or equal to 0.8. Figure 4 illustrates the 11 critical constraints identified in the organization.
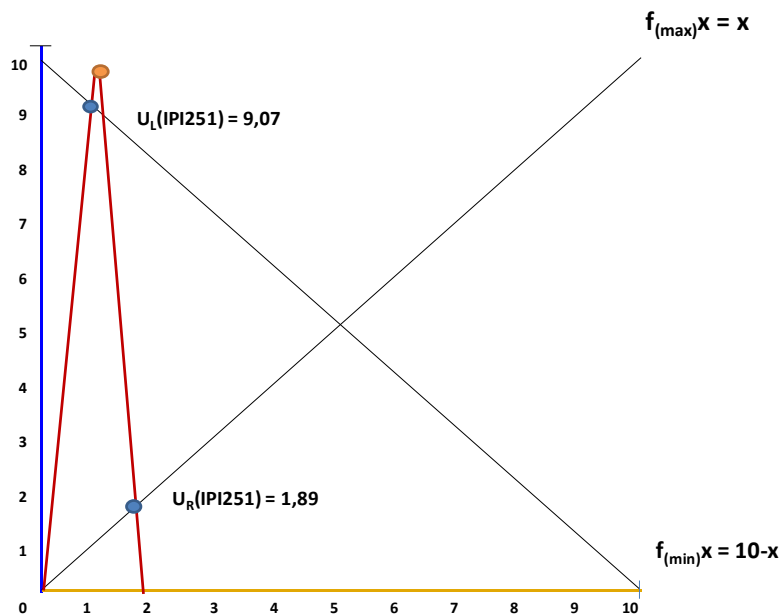
Figure 3. Graphical representation to estimate $U_R(IPI_{251})$ and $U_L(IPI_{251})$.

U_T (IDID$_{ijk}$)	0,27	0,44	0,61	0,62	0,71
Attribute (AT$_{ijk}$)	AT$_{243}$	AT$_{217}$	AT$_{117}$	AT$_{268}$	AT$_{115}$
		AT$_{227}$	AT$_{118}$	AT$_{210}$	AT$_{228}$
			AT$_{211}$		
			AT$_{219}$		

Figure 4. Critical constraints.

The representation of the results obtained in radar graph as shown in Figure 5, can simultaneously analyse the current performance level of the various criteria. Moreover, this type of representation allows benchmarking with other organizations. Thus, the membership function associated with each fuzzy aggregate Lean Index, LI_{ij}, should be transformed into a crisp value by using the defuzification method mentioned in the last section, which is based on equation (12), (13) and (14). Then, the values obtained for each criterion are represented in Figure 5.
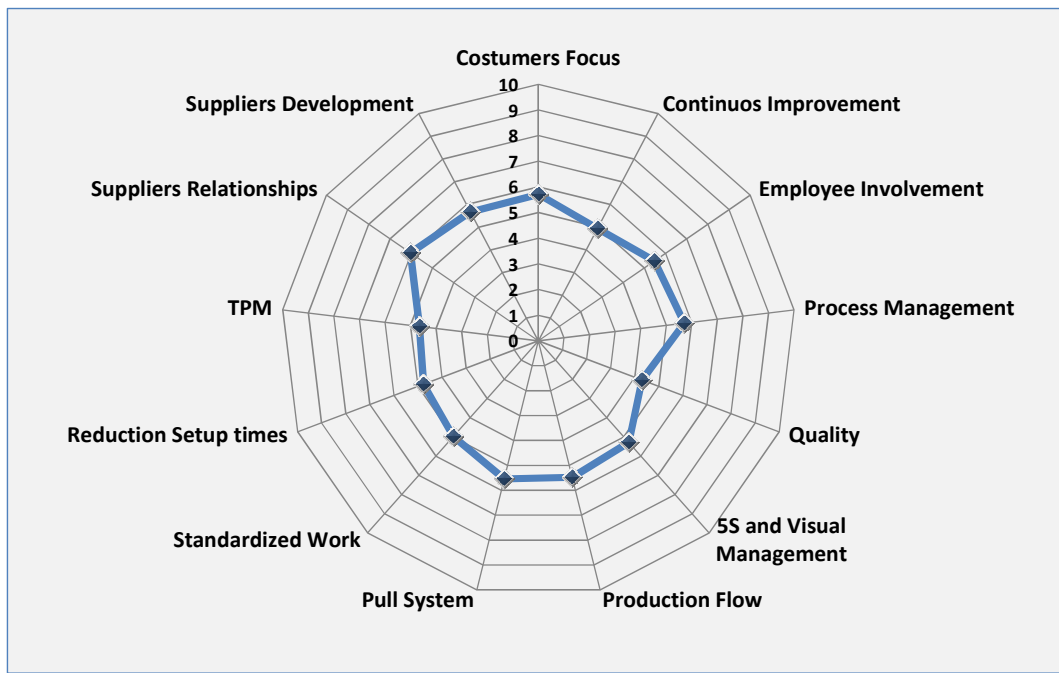
Figure 5. Fuzzy aggregate lean index for each criterion.

The values closer to the periphery represent better performance while values closer to the centre correspond to a worse performance. For instance, considering the fuzzy aggregate Lean Index, LI_{25}, associated with the criterion "*5S and Visual Management*", the obtained corresponding value is as follows: $U_T(IL_{25})$=5.24.

Aiming to obtain a graphical representation of the performance value associated with each dimension, the membership functions associated with each fuzzy aggregate lean index related to each dimension, were transformed into crisp values following the methodology previously described. In Figure 6 is represented the achieved crisp values associated with each aggregate lean index, LI_i, related to each dimension. For instance, applying the equations (9), (10) and (11) the crisp value obtained for the aggregate lean index LI_2, which corresponds to the dimension "Organization", is as follows: $U_T(LI_{25})$=5.11.
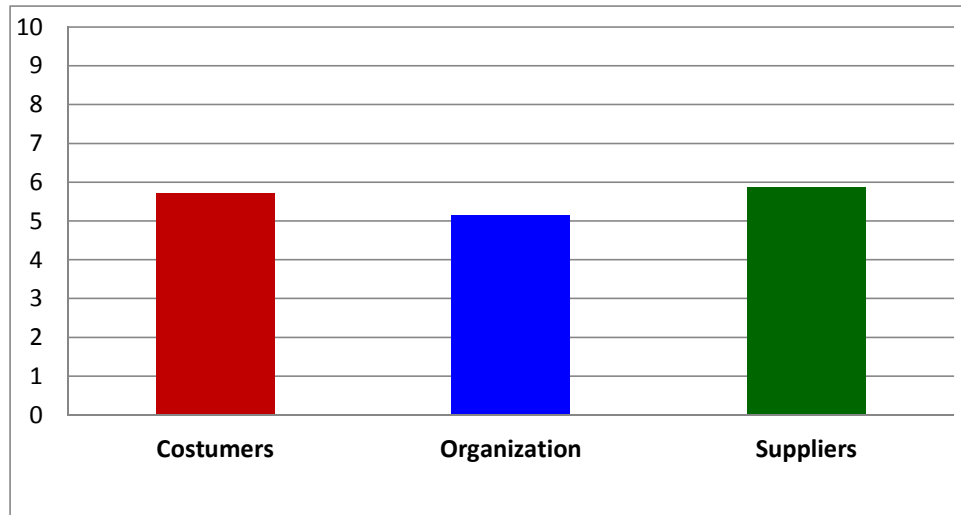
Figure 6. Aggregate lean index for each dimension.

3. CONCLUSIONS

Organizations should make use of simultaneous approaches either of perception and measurement in order to guide their efforts to implement lean thinking more efficiently. It was in this sense that the present model was developed using a qualitative evaluation approach, including quantitative basis, supported on fuzzy logic, since it can handle the uncertainty and inaccuracy of input data, and is also applicable on the analysis of qualitative variables of a system, turning them into quantitative values. A major advantage of the developed approach, when compared with other approaches reported in the literature, it is that it can be adjusted to any type of organization regardless of its nature, size, strategy and market positioning. Moreover, the proposed model makes possible to identify systematically the constraints factors existing in the organization concerned with its lean level enhancement and, thus, provide the necessary information for the management to develop a holistic plan for continuous improvement. Furthermore, another advantage of the framework adopted to develop the organizations' lean level assessment methodology presented above, when compared with other reported approaches, it is its ability to cope with the specificities of any kind of organization, being either a manufacturing company or a services enterprise.

The development of a framework based on fuzzy set theory was motivated in large measure by the need for a methodology able to cope with humanistic systems; that is, with systems in which human judgement behaviour and emotions play a dominant role. Viewed in this perspective, this work takes advantage of the main fuzzy logic capabilities to perform the analysis of systems whose behaviour is based on people's skills and knowledge in management control and organization analysis. However, the application of fuzzy logic as a tool to support the organization assessment introduces some limitations. The membership functions of the linguistic variables (fuzzy sets) depend on the perception of the evaluator. Thus, the evaluator should be an experienced person with skills in continuous improvement or lean thinking in order to realize the importance of the model elements. The contribution of this work aims to provide a rational framework for assessing imprecise phenomena such as the case of lean assessment.

The successful results obtained with the proposed approach using a real industrial scenario, demonstrates the level of maturity of the methodology developed and allows us to envisage its

application not only in research work but also in the monitoring of the implementation of lean thinking in any public or private organization.

REFERENCES

[1]   Bashin, S. and Burcher, P. (2006). Lean viewed as a philosophy. Journal of Manufacturing Technology Management, Vol. 17, Issue 1, pp. 56-72.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2]   Behrouzi, F. and Wong, K.Y. (2011). Lean performance evaluation of manufacturing systems: A dynamic and innovative approach. Procedia Computer Science, Vol. 3, pp. 388-395.K. Elissa, "Title of paper if known," unpublished.

[3]   Amin, M.A. (2013). A Systematic approach for selecting lean strategies and assessing leanness in manufacturing organizations'. Ph.D. Thesis, Queensland University of Technology, Australia.

[4]   Pakdil, F. and Leonard, K. (2014). Criteria for a lean organisation: development of a lean assessment tool. International Journal of Production Research, Vol. 52, Issue 15, pp. 4587-4607.

[5]   Wan, H. and Chen, F. (2008). A leanness measure of manufacturing systems for quantifying impacts of lean initiatives. International Journal of Production Research, Vol. 46, Issue 23, pp. 6567-6584.

[6]   Bayou, M.E. and De Korvin, A. (2008). Measuring the leanness of manufacturing systems - A case study of Ford Motor Company and General Motors. Journal of Engineering and Technology Management, Vol. 25, Issue 4, pp. 287-304.

[7]   Fullerton, R. and Wempe, W. (2009). Lean Manufacturing, Non-financial Performance Measures, and Financial Performance. International Journal of Operations and Production Management, Vol. 29, Issue 3, pp. 214–240.

[8]   Baker, P. (2008). The Role, Design and Operation of Distribution Centres in Agile Supply Chains. Ph.D. Thesis, School of Management, Cranfield University, England.

[9]   Mahfouz, A. (2011). An Integrated Framework to Assess Leanness Performance in Distribution Centres. Ph.D. Thesis, Dublin Institute of Technology, England.

[10]   Lin, C.-T., Chiub, H. and Tseng, Y.-H. (2006). Agility evaluation using fuzzy logic. International Journal of Production Economics, Vol. 101, Issue 2, pp. 353-368.

[11]   Zanjirchi, S.M., Tooranlo, H.S. and Nejad, L.Z. (2010). Measuring Organizational Leanness Using Fuzzy Approach. Proceedings of the 2010 International Conference on Industrial Engineering and Operations Management, Dhaka, Bangladesh, pp. 144-156.

[12]   Guesgen, H.W. and Albrecht, J. (2000). Imprecise reasoning in geographic information systems. Fuzzy Sets and Systems, Vol. 113, Issue 1, pp. 121–131.

[13]   Chen, S.J. and Hwang, C.L. (1992). Fuzzy Multiple Attribute Decision Making Methods and Application. Lecture Notes in Economics and Mathematical Systems, Vol. 375, Springer Berlin Heidelberg.

[14]   Narayanamurthy, G. and Gurumurthy, A. (2016). Leanness assessment: a literature review. International Journal of Operations and Production Management, Vol. 36, Issue 10, pp. 1115-1160.

AUTHORS

António Abreu, before joining the academic world in 1998, he had an industrial career since 1992 in manufacturing industries with management positions. He concluded his PhD in 2007 in Industrial Engineering at the New University of Lisbon and he is currently professor of Industrial Engineering in the Polytechnic Institute of Lisbon (ISEL– Instituto Superior de Engenharia de Lisboa), where he now holds assistant professor position.

He is member of several national and international associations, e.g. he is co-founder of SOCOLNET, member of the ISO/TC 258 and INSTICC .

As researcher, he has been involved in several European research projects such as: VOmap, Thinkcreative and ECOLEAD. He has been involved in the organization and program committees of several national and international conferences with particular reference to PRO-VE, , MCPL, BASYS. His main research is in collaborative networked organisations, Logistics, project management, open-Innovation and lean management area.

João M. F. Calado, received his degree (5 years undergraduate course) from Instituto Superior Técnico, Technical University of Lisbon, in Electrical and Computing Engineering and the Ph.D. from The City University, London, United Kingdom, in Control Engineering, in 1986 and 1996 respectively. He joined the Maritime Machinery Department of Nautical School Infante D. Henrique, Lisbon, Portugal, in 1986, as an Assistant and was promoted to Assistant Professor, in 1991. Since 1998, he has been with the Mechanical Engineering Department of ISEL – Instituto Superior de Engenharia de Lisboa, Polytechnic Institute of Lisbon, Lisbon, Portugal, as Associate Professor being promoted to Full Professor in 2009. He is Fellow Member of the Engineers Portuguese Association, IEEE Senior Member, Member of IFAC – TC SAFEPROCESS, Member of APCA, Member of SPR and Member of Socolnet. His research and development field covers fault tolerant control, intelligent control systems, mobile robotics, rehabilitation robotics, modelling and control of manufacturing processes, multi agent systems and collaborative approaches.

INTENTIONAL BLANK

AN INTERVAL TYPE-2 FUZZY LOGIC-BASED FRAMEWORK FOR CALL ADMISSION CONTROL IN 4G MOBILE NETWORKS

Uduak Umoh [1], Daniel Asuquo[2] and Imoh Eyoh[3]

[1,2]Department of Computer Science, University of Uyo,
Akwa Ibom State, Nigeria
[3]ASAP Research Group, University of Nottingham, Nottingham,
United Kingdom

ABSTRACT

This paper presents a technique to control based on interval type-2 fuzzy logic system (IT2FLS) of Mamdani fuzzy inference, employed to model connection admission control in Fourth Generation (4G) Networks in order to improve quality of service (QoS). The appropriate parameter selection to achieve connection admission control is also considered based on major system parameters like latency, packet loss, load, signal strength and user mobility. We explore the use of Karnik-Mendel (KM) and Wu-Mendel (WM) approaches in our proposed system. We also implement a T1FLS connection admission control for guaranteed QoS in 4G mobile networks for comparison purposes. The empirical comparison is made on the designed system using 4G network admission control synthetic datasets. Analysis of our results reveal that the presence of additional degrees of freedom in IT2FLS-WM controller tend to reduce the root mean square error (RMSE) of the model compared to IT2FLS-KM and fuzzy type-1 approaches.

KEYWORDS

Interval type-2 fuzzy logic; Admission control system; 4G Mobile Networks; Computational complexity

1. INTRODUCTION

Due to emerging needs for multimedia applications, a variety of access technologies such as third generation (3G), beyond 3G (B3G), and 4G networks are developed and deployed to complement 2G networks and satisfy demands for mobile services and internet access. 4G communication networks strive to seamlessly integrate various existing wireless communication technologies with the goal of replacing the entire core of cellular networks with a single worldwide cellular network. It provides capabilities defined by International Telecommunication Union (ITU) in Internet Mobile Telephony (IMT) Advanced [1]. 4G network is believed to be the fastest network technology following the path set and commercially deployed by its wireless siblings, evolved to offer a mobile environment with high data rate up to 450 Mbps and efficient quality of service (QoS) for real-time applications [2].

The increasing demand for mobile multimedia applications along with the increasing population of advance mobile devices seeking best connections anywhere and anytime comes with the challenge of providing efficient mechanisms for seamless handover among heterogeneous networks to meet specific QoS requirements. Consequently, choosing the best network to accept a new connection request without disrupting the service quality of ongoing connections becomes difficult [3] [4] [5]. Furthermore, as 4G networks are associated with much uncertainty and imprecision due to escalating number of access points, constant change in propagation channels, network load sudden variations and random mobility of users [6] [7], there is need to develop a framework that ensures fair admission control and efficient service delivery to all categories of call requests.

A Connection Admission Control (CAC) is an important decision making technique aimed at providing required QoS by restricting access to the network resources [8]. According to [3] and [9], maintaining QoS (e.g. signal quality, packet delay, jitter, loss rate, call blocking and dropping thresholds, etc.) is necessary for efficient admission control in mobile multimedia networks. Based on network load conditions for a requested connection type, the admission controller can decide to either accept or block the new request depending on the available network resources to meet the QoS requirements for the new connection without violating the QoS of already accepted requests, otherwise it is rejected. Several methods have been used to improve QoS across 4G networks. These methods include Markov models, queuing models, and expert systems, etc. In recent years, conventional fuzzy logic otherwise called type-1 fuzzy logic systems, arewidely used to improve the capability of existing CAC methods in mobile networks. This is due to its ability to process information using linguistic variables and making decision with imprecise, vague, ambiguous, uncertain data [12] [13].

Type-1 fuzzy logic systems (T1FLSs) have achieved great success in many different real world applications including wireless sensor networks, ATM networks, wireless cellular networks, congestion control[14] [15] [16] [17] [18] [19] [20] [21]. Despite the popularity of T1FLS, research has shown that there are difficulties in the ability of T1FLSs to model and minimize the effect of uncertainties because they provide a hard decision boundary [22] [23]. To solve this problem, type-2 fuzzy logic controllers are introduced. Type-2 fuzzy systems [24] are extensions of type-1 fuzzy systems, characterized by membership functions that are themselves fuzzy with soft decision boundaries. T2FLSs provide additional design degrees of freedom, which can be very useful when such systems are used in situations where lots of uncertainties are present. Both the T1FLS and T2FLS consist of the same four components, which are: a fuzzification unit, a rule base, a fuzzy inference engine, and a defuzzification unit. In addition, T2FLs possess type-reducer which converts T1FS output into crisp value. Recently, type-2 FLSs have been applied as a useful technique to handle all forms of uncertainties both in classification, prediction and control and the results have been promising and very encouraging [25] [26] [27] [28] [29] [30] [31] [32].

Despite the advantages offered by T2FLSs, there is the problem of computational complexity due to type-reduction computation, especially when there are many MFs and the rule base is large. To reduce the computational burden while preserving the advantages of IT2FLCs, a special case of type-2 fuzzy system called the interval type-2 fuzzy system is used [33]. IT2FLSs are widely applied in various areas because of their abilities to simplify T2FLCs [34] [35] [36]. Typically, an IT2FLS comprises five components namely, a fuzzification unit, a rule base, a fuzzy inference engine, type-reduction and defuzzificztion units. An iterative Karnik-Mendel (KM) algorithm is explored to perform type-reduction process. An extended version of type-1 defuzzification operation technique is applied on T2FSs case of the IT2FLS to obtain a T1FS at the output. The T1F set so obtained is a type-reduced set which is a collection of the outputs of all of the embedded T1-FLSs [25]. However, Karnik-Mendel (KM) algorithm is computationally complex, time-consuming with computational overhead which can reduce the real-time performance of the

IT2-FLS and also limit their application in industrial embedded controllers. To overcome the limitations of IT2FLS in order to speed up a T2FLC, Wu and Mendel uncertainty bounds (UB) technique is employed to approximate the type-reduced set instead of using KM algorithm [37][23]. This approach is believed to reduce the computation cost of the type-reduction and the memory required for the IT2FLS implementation.

In this paper, an IT2FL connection admission control framework for guaranteed QoS in 4G network is proposed. The admission decisions are made based on system parameters like latency, packet loss, load, signal strength, and user mobility. The study employs two approaches; K-M algorithm to obtain the type-reduced sets, and Wu-Mendel uncertainty bound approach for approximation of type-reduced set to estimate the uncertainty and crisp output of an IT2FLC. Experimental results indicate that approximation of the type-reduced set using Wu-Mendel method can eliminate type-reduction computational complexity. Also, computations associated with interval type-2 fuzzy systems provide a more accurate result than T1FLS, with practical results in connection admission control in 4G networks. The results further indicate that, our system is able to maximize the network resource utilization by reserving resources only when needed and within the expected residence time interval. In addition, the system ensures that QoS is maintained by deciding whether a connection should be accepted or rejected thereby improving customer's quality of experience and loyalty.

2. AN OVERVIEW OF INTERVAL TYPE-2 FUZZY LOGIC

2.1. Interval Type-2 Fuzzy Sets

According to standard background material about interval type-2 fuzzy sets taken from [38], an interval type-2 fuzzy set (IT2FS), Ã is characterized as:

$$\tilde{A} = \left\{ \left((x, u), \mu_{\tilde{A}}(x, u) \right) \middle| \forall x \in X, \forall u \in J_x \subseteq [0, 1] \right\} \tag{1}$$

where x, the *primary variable*, has domain X; $u \in U$, the *secondary variable*, has domain J_x at each $x \in X$; J_x is called the primary membership of x and the secondary grades of Ã all equal 1 [39]. Uncertainty about Ã is conveyed by the union of all the primary memberships, which is called the *footprint of uncertainty* (FOU) of *A* as shown in Fig1.

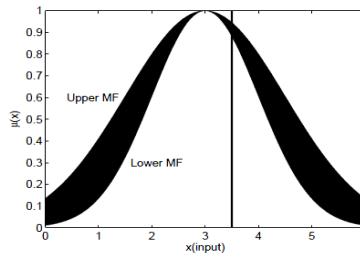$$\mu_{\tilde{A}}(x, u) = 1, FOU(\tilde{A}) = \bigcup_{\forall x \in X} J_x = \{(x, u) : u \in Jx \subseteq [0, 1]\} \tag{2}$$

Fig 1: Interval Type-2 Fuzzy set [27]

The *upper membership function* (UMF) and *lower membership function* (LMF) of Ã are two type-1 MFs that bound the FOU, i. e.

$$UMF = \bar{\mu}_{\tilde{A}}(x) \equiv \overline{FOU(\tilde{A})} \quad \forall x \in X \tag{3}$$

$$LMF = \underline{\mu}_{\tilde{A}}(x) \equiv \underline{FOU\ (\tilde{A})}\ \forall x \in X \tag{4}$$

$$J_x = \{(x, u) : u \in [\underline{\mu}_{\tilde{A}}(x), \overline{\mu}_{\tilde{A}}(x)]\} \tag{5}$$

where J_x is an interval set. We can apply set theory operations of union, intersection and complement to easily compute for IT2 FSs

2.2. Interval Type-2 Fuzzy Logic Systems (IT2FLS)

Figure 2 represents an IT2FLS, which is a FLS that uses at least one IT2FS, is characterized by five components: a rule-base, a fuzzification unit, an inference-engine unit, type-reduction and defuzzification units - that are inter-connected.
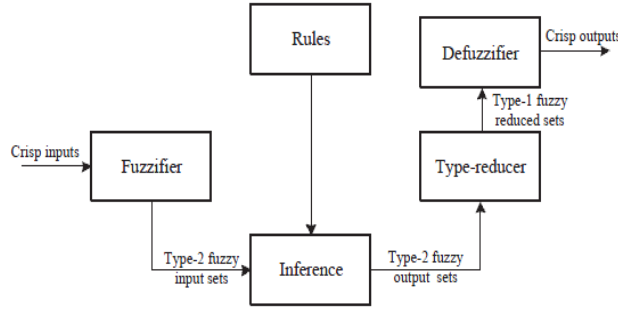

Fig. 2: Architecture of type-2 fuzzy system [27].

The type-2 fuzzy logic architecture updates a type-1 fuzzy logic system by adding the type reduction component. The IT2FLS is a mapping from crisp inputs to crisp outputs and this mapping can be expressed quantitatively as $Y = f(x)$. The fuzzification process maps a crisp input vector into type-1 or IT2FSs using singleton, triangular, trapezoidal or Gaussian fuzzifier. Input IT2-FSs then activate the inference engine and the rule base to produce output IT2 FSs. A type-reduction unit combines the output sets and then performs a centroid calculation which produces an interval T1FS (type-reduced set). The type-reduced set is then processed by the defuzzification unit to produce crisp outputs. In type-2 fuzzy logic, rules may be provided by experts or can be extracted from numerical data which can be expressed as a collection of IF–THEN statements. An IT2FLS can be with *m* inputs and *n* outputs or *m* inputs and *one* output. The later have the if-then rules specified as in (6).

$$IF\ x_i\ is\ \tilde{D}_i^l\ AND, \dots, AND\ x_m\ is\ \tilde{D}_m^l\ THEN\ y\ is\ \tilde{E}^l \tag{6}$$

Where x_i, $i = 1, \dots, m$ are the antecedents, y is the consequent of the *lth* rule of IT2FLS. The $\tilde{D}^i$'s are the MFs $\mu_{\tilde{D}_i^l}(x_i)$ of the antecedent part assigned of the *i*th input x_i, The E^l is the MFs $\mu_{\tilde{E}_j^l}(y)$ of the consequent part assigned to the output y_j.

The result of the input and antecedent operations contained in the firing set produces an interval type-1 set as shown in (7) [26].

$$F^i(x') = [\underline{f'}(x'), \overline{f'}(x')] \equiv [\underline{f'}, \overline{f'}] \tag{7}$$

where $F^i(x')$ is the antecedent of rule *i* and $\mu_{F1}^i(x')$ is the degree of membership of *x* in F. $\overline{\mu}_{\tilde{f}^i}(x)$ and $\underline{\mu}_{\tilde{f}^i}(x)$ are upper and lower MFs of $\mu_{\tilde{f}^i}$, $i = 1$ to *m* respectively.

The inference engine combines the fired rules and gives a mapping from input to output in IT2FSs. The combined output fuzzy set, $\mu_{\tilde{E}_j^i}(y_j)$, is obtained by combining the fired output consequent sets by taking the union of the *ith rule* fired output consequent sets.

2.3. Interval Type-2 Fuzzy Logic Systems (IT2FLS

From the standard background material on type-reduction and defuzzification in an IT2FLS taken from [38], five different Type-reduction (TR) techniques are defined, where the *type-reduced set* gives an interval of uncertainty for the output of an IT2FLS. The more uncertainties in an IT2FLS, the more uncertainties about its MFs, the larger the type-reduced set, and vice-versa. Although, computing the centroid of a general T2FS is complex; for an IT2FS, an exact iterative method of type-reduction is performed to compute the centroid of *an IT2FS* which is a T1FS. IT2FS are characterized by their left- and right-end points required to compute the centroid of an IT2FS [23][40][25].

Center-of-sets, centroid, center-of-sums, and height type-reduction can all be expressed in [27][29] as

$$Y_{TR}(x') = [y_l(x'), y_r(x')] \equiv [y_l, y_r] = \int_{y^1 \in [y_l^1, y_r^1]} \cdots \int_{y^1 \in [y_l^N, y_r^N]} \int_{f^1 \in [\underline{f}^1, \overline{f}^1]} \cdot \int_{f^N \in [\underline{f}^N, \overline{f}^N]} 1/$$

$$\frac{\sum_{i=1}^N f^i y^i}{\sum_{i=1}^N f^i} \tag{8}$$

TR center-of-sets (COS) are mostly used where y_l^i and y_r^i are the left and right end points of the centroid of the consequent of the *i*th rule while $\underline{f}^i$ and $\overline{f}^i$ are the lower and upper firing degrees of the *i*th rule and *N* is the number of fired rules.

KM Algorithms in [41] are employed for computing the end-points exactly and are presented in (9) and (10) respectively;

$$y_r = \frac{\sum_{i=1}^N f_r^i y_r^i}{\sum_{i=1}^N f_r^i} \tag{9}$$

$$y_l = \frac{\sum_{i=1}^N f_l^i y_l^i}{\sum_{i=1}^N f_l^i} \tag{10}$$

Defuzzification of the interval set is performed using the average of y_{lk} *and* y_{rk}, and the defuzzified crisp output for each output *k* is achieved;

$$Y_k(X) = \frac{y_{lk} + y_{rk}}{2} \tag{11}$$

2.4. An IT2FLS Using Wu-Mendel Uncertainty Bounds

The Type-reduction is computationally intensive, time-consuming and associated with output uncertainty for a real-time application of an IT2FLS. However, to overcome the limitations of IT2FLS in order to speed up a T2FLC, Wu-Mendel uncertainty bounds technique is employed to approximate the type-reduced set. The inner- and outer-bound sets (called minimax uncertainty bounds) are provided for the type-reduced set to estimate the output uncertainty of IT2FLS and directly perform defuzzification to obtain output under certain conditions [23] [37].

These uncertainty bounds are $\underline{y}_l(x'), \overline{y}_l(x'), \underline{y}_r(x'), \overline{y}_r(x')$ as expressed in details in [37], where $\underline{y}_l(x') \leq y_l(x') \leq \overline{y}_l(x')$ and $\underline{y}_r(x') \leq y_r(x') \leq \overline{y}_r(x')$

The type-reduction sets are approximated without having to perform TR and also defuzzify directly to obtain the output in (12) and (13) [37] as follows:

$$[y_l(x), y_r(x)] \approx [(\underline{y}_l(x) + \overline{y}_l(x))/2, (\underline{y}_r(x) + \overline{y}_r(x))/2] \qquad (12)$$

The output of IT2FLS is given as;

$$y(x) = \frac{1}{2}[y_l(x), y_r(x)] = \frac{1}{2}[(\underline{y}_l(x) + \overline{y}_l(x))/2 + (\underline{y}_r(x) + \overline{y}_r(x))/2] \qquad (13)$$

3. PROPOSED INTERVAL TYPE-2 FUZZY LOGIC FRAMEWORK FOR CALL ADMISSION CONTROL IN 4G NETWORKS

The In this paper, a 4G connection admission control framework is proposed using interval type-2 fuzzy logic technique in order to improve QoS. The choice of this technique lies in its ability to handle uncertainty associated with variables used in connection admission decision more effectively compared to type-1 fuzzy logic model. Connection admission factor (CAF) is determined for effective decision on call admission into the network and for proper management of network's resources based on the impact of these indictors (variables) – latency, packet loss, load, signal strength, and user mobility. The general structure of an IT2FLS for CAC in 4G networks is presented in Figure 3. The Model of the Proposed IT2FL-AC is shown in Figure 4.
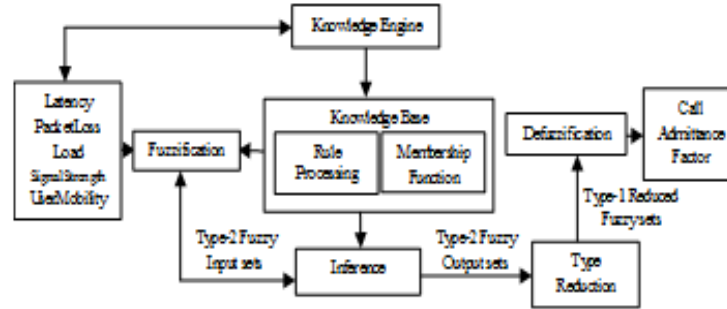
Fig. 3: Type-2 Fuzzy logic model for call admission control

In Figure 3, there are five inputs *latency (LA)*, *Packet Loss (PL)*, *Signal Strength (SS)*, *Load (LD)*, and *User Mobility (UM)* obtained from the knowledge engine and one output, *Call Admittance Factor (CAF)* for determining the degree of acceptability or otherwise of call request. General T2FLSs are computationally complex [42]. However, T2FLC is simplified using IT2FLS. In this paper, IT2FLS as discussed is employed for controlling call admission parameters.

In *layer one*, fuzzy linguistic variables (input parameters) are defined as *LA*, *PL*, *SS, LD,* and *UM*. The linguistic terms for each of *LA*, *PL*, and *UM* are Low (L), Medium (M), and High (H). *LD* has Very Low (VL), Low (L), High (H) and Very High (VH) as linguistic terms while Weak (W), Moderate (M), and Strong (S) are the linguistic terms for *SS*. Their MF plots in MATLAB are as shown in figures 9(a) – (e). The output parameter – CAF is described using four linguistic terms which are *Poor (P), Fair (F), Good (G,) and Excellent (E)*, as shown in Figure 4.The MF limits are selected based on input parameters and applied for reducing footprint of uncertainties. The MFs of these fuzzy sets contain five inputs and one output. These inputs are converted and

fuzzified into input interval type-2 fuzzy sets, and then are mapped to the linguistic labels of fuzzy sets to determine their degree of membership.

Fig. 4: The Model of the Proposed IT2FLCAC- adapted from [43]

This work considers IT2 Gaussian MFs with uncertain width (deviation) because it is suitable for highly dynamic random networks such as 4G.

$$f(x) = e^{\frac{-1}{2}\left(\frac{x-c}{\sigma}\right)^2}, \sigma \in [\sigma_1, \sigma_2] \text{ and } c \in [c_1, c_2] \tag{14}$$

That is $\sigma \in [\sigma_1, \sigma_2]$ with upper and lower membership functions defined as follows:

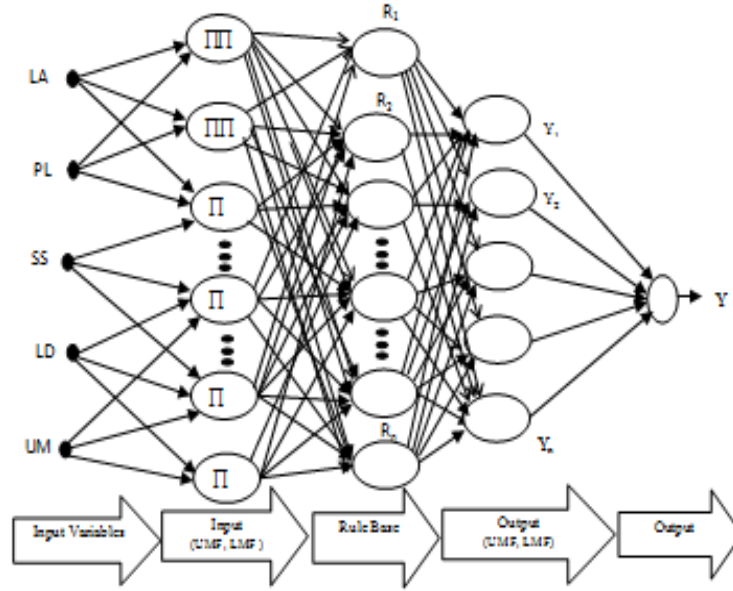$$\bar{\mu}_{\tilde{A}_{im}}(x_i) = \exp\left(-\frac{x_i - c_{im}}{2\bar{\sigma}_{2,im}^2}\right), \ \bar{\mu}_{\tilde{A}}(x) = N(c, \sigma_2; x) \tag{15}$$

$$\underline{\mu}_{\tilde{A}_{im}}(x_i) = \exp\left(-\frac{x_i - c_{im}}{2\underline{\sigma}_{1,im}^2}\right), \ \underline{\mu}_{\tilde{A}}(x) = N(c, \sigma_1; x) \tag{16}$$

Where c is the center (mean) of the MF, σ is the width (standard deviation) of the MF and x is the input vector. The variables $\bar{\sigma}_{2,im}$ and $\underline{\sigma}_{1,im}$ are premise parameters that define the degree of membership of each element to the fuzzy set Ã and FOUs of the IT2IFS. The detail description is found in [33] [23]. MFs are defined and evaluated for all the input and output linguistic variables. IT2F sets are explored in the antecedents' parts and each MF of the antecedent part is represented using an upper and a lower MFs, denoted by $\bar{\mu}_{\tilde{A}}(x)$ and $\underline{\mu}_{\tilde{A}}(x)$ as described in [33]. Each node output indicates the lower and upper interval.

In *layer two*, the fuzzy rules are defined based on (6). One example is expressed as: IF *Latency* is *High* and *Packet Loss is Moderate* and *Load is High* and *Signal Strength* is *Strong* and *User Mobility is Low THEN CAF is FAIR* = [0.32, 0.29]. 243 rules were defined in the rule base for the IT2 FLC based on human expert opinion. For simplicity, parts of the rules are presented in Table 1. In the IT2FLS, the rule base part are enclosed with five antecedents *(LA, PL, SS, LD, UM)* which divide the input space into a set of fuzzy regions and one consequent (CAF) part which

describes the system behavior in those regions. Each MF of the antecedent part is represented by an upper and a lower membership function

In *layer three*, the inference engine combines fired rules, maps input IT2 fuzzy sets and output IT2 fuzzy sets by computing unions and intersections of type-2 sets, as well as compositions of type-2 relations. The main problem is to determine the effect of input parameters in the antecedent part such that a concise representation of the system's behavior is produced in the consequent part, i.e. network connection admission. This paper uses Mamdani fuzzy inference engine to calculate the firing strengths of the *i*th rule illustrated in (7).

Layer Four: In this layer, type reducer maps IT2FS into a T1FS by combining the fuzzy output sets (IT1FS). In our paper, IT2FLC-AC employs center-of-sets type-reduction [44], and applies the iterative Karnik-Mendel (KM) procedures illustrated in section 4 of this paper, to calculate correct values of type-reduced sets. IT1FS is determined by its two end points, y_l and y_r in (9) and (10).

Layer five: Defuzzification is performed in this layer by mapping the T1FS into a crisp number by computing the interval output of this layer for each node present in this layer respectively. The final output of T2FLS-AC, which is a numeric value, is obtained by averaging the output of the resultant effect of the four embedded T1FLS using (10).

However, it is observed that K-M type-reduction scheme shows a major bottleneck using an interval type-2 FLS in real-time practices. We employ Wu-Mendel uncertainty bounds approximation method illustrated in section 5 of this work, to estimate the type-reduced sets and then determine the output of the FLS directly in to eliminate type-reduction.

Next, we present our model experiment and discussion of simulation results. We use the root mean square error (RMSE) performance criterion for our experiments which is defined as:

$$RMSE = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y^x - y)^2} \qquad (17)$$

Where y^x is the desired output, y is our model output and N is the number of data items.

4. MODEL EXPERIMENT RESULTS

In this paper, IT2FL controller using KM type-reduction method and the IT2FL controller using the Wu-Mendel UB method are applied to a non-linear system control problem in 4G mobile networks where 200 datasets are generated based on the variables; *latency*, *Packet Loss*, *Signal Strength, Load,* and *User Mobility* which are used as inputs and *call admittance factor* is the desired output. For each input in this study, Gaussian membership functions with fixed mean and uncertain standard deviation are used. An IT2FLS-AC and T1FLS-AC are implemented for comparison purposes. Fuzzy logic toolbox in Matlab 7.5.0 is used for the input and output membership functions plots as presented in Figures 5(a)-(f) respectively. The results of applying different approaches to the admission control in 4G networks to guarantee efficient QoS are shown in Table1 and graphs are presented in Figures (6) to (8) respectively. The result of RMSE performance criterion for our experiment is presented in Table 2.
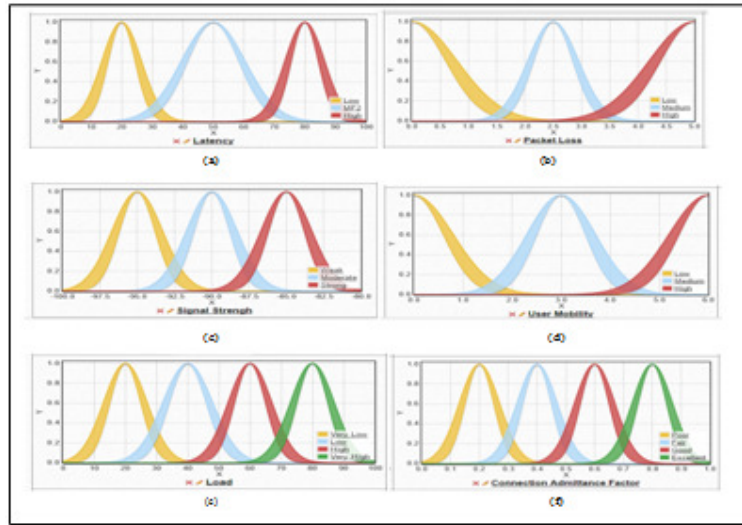
Fig. 5: (a) Latency (b) Packet Loss (c) Load   (d) Signal Strength (e) User Mobility (input IT2 Membership Functions for) and (f) Output membership functions (CAF)

Table 1: Experimental Results

|								IT2FL		T1FL
S/N	Latency	Packet Loss	Load	Signal Strength	User Mobility	Yl	Yr	KM	WU	IT1FL
1	23.39761925	4.782493591	34.14649963	-86.58191681	4.16469574	0.651729187	0.609048401	0.630388794	0.630167788	0.52
2	59.13171005	4.835350037	29.49345016	-93.16853333	2.212117672	0.99995877	0.992286656	0.996122713	0.996431759	0.65
3	8.009558678	4.997141838	40.46202469	-81.70938873	1.075722814	0.650119839	0.550421062	0.60027045	0.60407055	0.5
4	28.88267708	1.556679249	0.618451834	-98.71507263	2.57207346	0.814729847	0.787889404	0.801309625	0.80132129	0.75
5	57.68119049	3.718532085	96.13624573	-86.05348969	3.419070244	1	0.987392868	0.993696434	0.996129886	0.7
6	36.49825287	0.467535853	84.23316956	-99.67602539	3.332528591	0.999999834	0.899342281	0.949671058	0.949671055	0.75
7	16.43228531	1.770384908	4.708766937	-91.43685913	0.983432651	0.978162667	0.208230975	0.593196821	0.617159698	0.48
8	91.47351074	3.671760082	76.3494873	-98.97769928	0.544688702	0.624114712	0.821757072	0.722935892	0.733975238	0.7
9	29.72520638	0.575915277	99.39528656	-96.62104797	5.489224434	1	0.896624423	0.949812211	0.949812211	0.7
10	37.83773804	4.140957155	46.00809097	-97.79297638	4.743180275	0.999248616	0.393988832	0.696618724	0.702996027	0.55
11	73.30070496	0.570019484	19.82002258	-84.14083862	1.904493213	0.309896523	0.285087653	0.297492088	0.293975965	0.09
12	90.50460815	1.187733412	48.80061722	-81.58362579	3.851906776	0.659964457	0.645077075	0.652520766	0.652539482	0.8
13	35.31845856	0.796303749	55.58693314	-91.94580841	2.347836256	0.901271068	0.200206576	0.550738822	0.57220729	0.5
14	25.81006813	2.981541395	35.22211456	-99.78913116	3.002118587	0.667908269	0.608371366	0.638139818	0.638556624	0.6
15	86.09112549	4.168234825	85.61044312	-98.93075562	5.994147778	0.999999691	0.898933886	0.949466788	0.949511194	0.72
16	44.31048584	4.547613144	66.90149689	-84.54164886	4.623449326	0.99923982	0.999148899	0.99919436	0.999193708	0.75
17	57.17311478	4.864745617	57.4464798	-88.15919495	0.09990406	0.999997491	0.997864367	0.998930929	0.99901652	0.74
18	48.1325798	2.806750536	97.74352264	-84.34715271	3.428855419	0.999939181	0.201135766	0.600537473	0.601496962	0.65
19	8.453929901	3.228743553	57.91474152	-85.3899765	4.550435066	0.650325384	0.600365801	0.625345592	0.625345593	0.43
20	93.65468597	4.439779758	47.34951782	-98.01423645	1.359944701	0.610046116	0.792653241	0.701349679	0.70554719	0.5
21	92.99415588	2.921215534	77.52400208	-86.62914276	0.583048224	0.999352784	0.884940483	0.942146633	0.943375959	0.72

IT2FL RESULT New 2
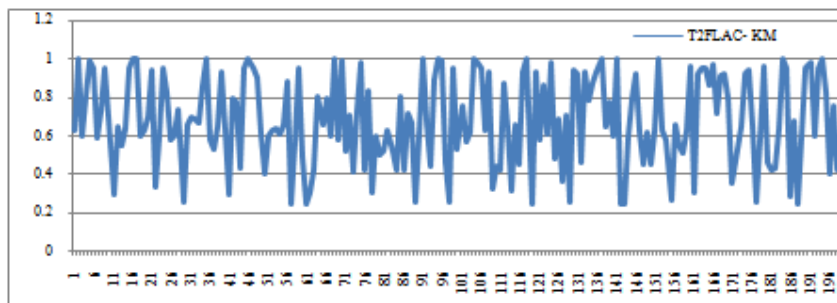
Fig. 6: Graph of the result of Interval Type-2 Fuzzy Logic Admission Control using KM approach
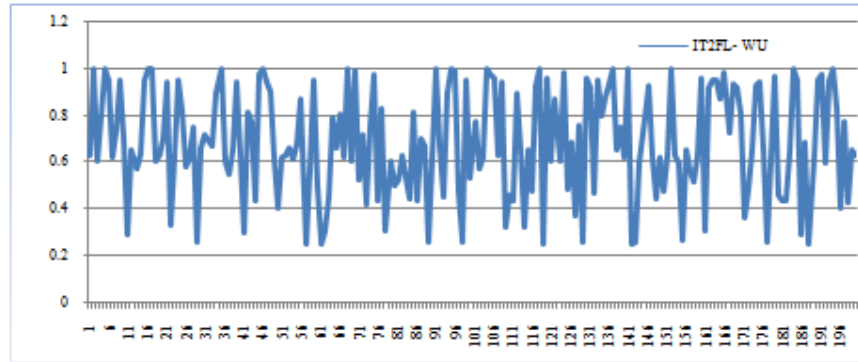
Fig. 7: Graph of the result of Interval Type-2 Fuzzy Logic Admission Control using WU approach
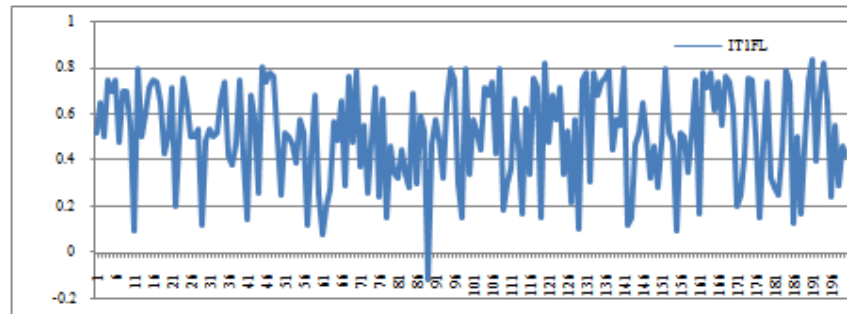
Fig. 8: Graph of the result of Interval Type-1 Fuzzy Logic Admission Control

Table 2: Comparison of IT2FLS-KM, IT2FLS-UM and ITIFLS in Admission Control in 4G Networks

Models	Training/Chk	Mean	Standard Deviation	Root Mean Square Error (RMSE)
IT1FLAC	400/200	0.5123	58.6776	0.0456
IT2FLAC-KM	400/200	0.6789	51.5483	0.0021
IT2FLAC-WM	400/200	0.6876	48.2197	0.0016

The results of applying different approaches to the connection admission control problem are as listed in Table 1 and in Figures (6) to (8) indicate that generally, IT2FLS using Wu-Mendel method outperforms Karnik-Mendel on the same set of input parameters. For example, with 35% low latency, 1% low packet loss, 56% low load, -91.9 signal strength and 2% moderate user mobility, 57% good CAF is achieved using WU approach as against 55% good CAF with Km method. However, it is also observed that approximately 100% optimal value in terms of QoS demands and overall network performance is achieved using both approaches with 44% medium latency, 5% high packet loss, 67% high load, -85% strong signal strength and 5% high user mobility. RMSE performance measure applied in the work, as shown in Table 2 after training. IT2FLS using WM give 0.0016 RMSE, outperforms IT2FLS using KM with 0.0021 RMSE, because the lower the error, the better the performance of the technique. We also implement a T1FLS for connection admission control in 4G Networks in order to comparatively evaluate the performance of the IT2FLS-AC with the T1FL model, where results indicate that IT2FLS-AC outperforms T1FLS because of the extra degrees of freedom offered by the FOUs of the IT2FLSs. The overall result shows a 1.62% improvement of IT2FLS with WM over IT2FLS KM and

87.07% over T1FLS. This indicates that there is a significant performance improvement of IT2FLS over T1FLS on system control.

4. CONCLUSION

In this study, an IT2FLS approach to control is presented. The IT2FLS can accommodate more imprecision thereby modelling imperfect and imprecise knowledge better than some T1FLS. The main problem is to determine the effect of input parameters in the antecedent part such that a concise representation of the systems behavior is produced in the consequent part, i.e. network connection admission. The key point in this design is the use of IT2FL to model the level of uncertainty of every element in each set. In future, we intend to learn the parameters of the IT2FLS using Gaussian membership function with uncertain mean and also to train IT2FLS using hybrid approach of neural networks and particle swarm optimization and to apply on network connection admission control datasets for more effective guarantee of QoS.

REFERENCES

[1]   M. E. Dien, A. A. Youssif, A. Z. Ghalwash "Energy Efficient and QoS Aware Framework for Video Transmission over Wireless Sensor Networks". Wireless Sensor Network, 2016, vol. 8, pp 25-36.

[2]   R. Sepúlveda, O. Ross, J. Qui˜nones-Rivera, and E. Quiroz "WLAN Cell Handoff Latency Abatement Using an FPGA Fuzzy Logic Algorithm Implementation. Hindawi Publishing Corporation Advances in Fuzzy Systems. Vol, 2012, Article ID 219602, 1-10 s doi:10.1155/2012/219602

[3]   S. Kumar, K. Kumar and K. Pandey "A Comparative Study of Call Admission Control in Mobile Multimedia Networks using Soft Computing. International Journal of Computer Applications (0975 – 8887) Vol. 107 Issue 16, pp 1-7, 2014.

[4]   P. Metre, K. Radhika, Gowrishankar "Survey of Soft Computing Techniques for Joint Radio Resource Management", 978-1-4673-1520, IEEE 2012.

[5]   P. Payaswini, D.H. Manjaiah "Challenges and issues in 4G – Networks Mobility Management". International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue5–May 2013, 1247-1251, 2013.

[6]   A. A. Atayero and M. K. Luka 'Applications of Soft Computing in Mobile and Wireless Communications". International Journal of Computer Applications (0975 – 8887), vol. 45 No. 22, pp 48-55, 2012.

[7]   I. F. Akyildiz, D. M. Gutierrez-Estevez, E. C. Reyes "The evolution to 4G cellular systems". LTE Advanced Physical Communication, vol. 3 pp 217–244, 2010.

[8]   A. Shukla, Super-Fast 4G Wireless Service Launching in South Korea. Asia-Pacific Buisness and Technology Report, 2011.

[9]   G. Mahesh, S. Yeshwanth, U. V. Manikantan "Survey on Soft Computing based Call Admission Control in Wireless Networks". International Journal of Computer Science and Information Technologies, Vol. 5 No. 3, pp 3176 – 3180, 2014.

[10]   A. M. Miyim, M. Ismail, R. Nordin and M. T. Ismail "Regressive Prediction Approach to Vertical Handover in Fourth Generation Wireless Networks". J. ICT Res. Appl., vol. 8, No. 1, pp 31-48, 2014.

[11]   L. A. Zadeh "Fuzzy Sets". Information and Control, vol. 8, pp 338–353, 1965.

[12]   O. Castillo, P. Melin "Type-2fuzzylogic: theory and application". Studfuzz, vol. 223, pp. 29–43, 2008.

[13]   E. H. Mamdani and S. Assilian "An experiment in linguistic synthesis with a fuzzy logic controller". International Journal of Man–Machine Studies, vol. 7, no.1, pp. 1-13, 1975.

[14]   M. V. Ramkumar, A. D. Mihovska, N. R. Prasad and R. Prasad "Fuzzy-Logic Based Call Admission Control for A Heterogeneous Radio Environment". International Jornal of Research in Computer Science, vol. 3, Issue 4, 2016.

[15]   M. P. Selvi and S. Sendhilnathan "Fuzzy Based Mobility Management in 4G Wireless Networks". Brazilian   Archives   of   Biology   and   Technology.   vol.   59   no.   spe2,   2016, http://dx.doi.org/10.1590/1678-4324-2016161047.

[16]   G. U. Mali "Fuzzy Based Vertical Handoff Decision Controller for Future Networks". International Journal of Advanced Engineering, Management and Science (IJAEMS) vol. 3, no.1, 111-119, Jan-2017.

[17]   R. Abbasi, A. Bidgoli and M. Abbasi, "A New Fuzzy Algorithm For Improving Quality of Service In Real Time Wireless Sensor Networks". International Journal Of Advanced Smart Sensor Network Systems (IJASSN), vol. 2, no. 2, pp 1-14, 2012.

[18]   A. Dogman, R. Saatchi, and S. Al-Khayatt, "Quality of Service Evaluation using a Combination of Fuzzy C-Means and Regression Model". World Academy of Science, Engineering and Technology vol. 6, pp. 562-571, 2012.

[19]   J. Ye, X. Shen, and J. Mark, "Call admission control in wideband CDMA cellular networks by using fuzzy logic". IEEE Trans. Mobile Comput., vol. 4, no. 2, pp. 129-141, 2005.

[20]   C. Sonmez, O. Incel, S. Isik, M. Donmez and C. Ersoy, "Fuzzy-based congestion control for wireless multimedia sensor networks". Sonmezet al. EURASIP Journal on Wireless Communications and Networking, no. 63, pp 1-17, 2014.

[21]   Y. Bazaz1, S.   Kumar and S. Anand, "Congestion Control Mechanism using Fuzzy Logic".International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) vol. 2, no. 2, pp. 313-319, 2013.

[22]   H. Hagras "Type-2 flcs: A new generation of fuzzy controllers".IEEE Computational Intelligence Magazine, vol. 2, no. 1, 30–43, 2007.

[23]   J. M. Mendel, Uncertain Rule-Based Fuzzy Logic Systems: Introduction and New Directions, Prentice-Hall, Upper Saddle River, NJ, 2001.

[24]   L. A. Zadeh, "The concept of a linguistic variable and its application to approximate reasoning—1," Inf. Sci., vol. 8, pp. 199–249, 1975.

[25]   N. N. Karnik and J. M. Mendel, "Centroid of a type-2 fuzzy set," Information Sciences, vol. 132, pp. 195-220, 2001.

[26]   D. R.Wu and W. W. Tan "Computationally efficient type-reduction strategies for a type-2 fuzzy logic controller", in FUZZ-IEEE, Reno, USA pp. 353-358, , May, 2005.

[27]   Wu, Dongrui (2005), Design and analysis of Type-2 Fuzzy Logic Systems. A Master's Thesis, Department Of Electrical Aad Computer Engineering, National University of Singapore 2005

[28]   J. M. Mendel, "Fuzzy sets for words: a new beginning," in Proceedings of the 12th IEEE International conference on Fuzzy Systems, pp. 37–42, Los Angeles, Calif, USA, May 2003.

[29] D. Wu and J. M. Mendel, "A vector similarity measure for linguistic approximation: interval type-2 and type-1 fuzzy sets," Information Sciences, vol. 178, no. 2, pp. 381–402, 2008.

[30] H.M. Fayek , I.Elamvazuthi N.Perumal , B.Venkatesh (2014). A controller based on OptimalType-2 FuzzyLogic:Systematic design, optimization and real-time implementation. ISA Transactions, vol. 53, pp. 1583–1591, 2014.

[31] Q. Ren, M. Balazinski and Luc Baron "Type-2 TSK Fuzzy Logic System and its Type-1 Counterpart". International Journal of Computer Applications (0975 – 8887) vol. 20. no.6, pp. 8-14, April 2011.

[32] R. Sarojinee, V. Gupta, M. K. Jha and M. F. Qureshi "Development of Interval Type-2 Fuzzy Logic Controller for Polymer Extruder Melt Temperature Control". International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 2, February 2015, 593-605.

[33] Q Liang, N. N. Karnik "Connection Admission Control in ATM Networks Using Survey-Based Type-2 Fuzzy Logic Systems'. IEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, vol. 30, no. 3., pp. 329-340, August 2000.

[34] S. Shukla, M. Jha, M. F. and Qureshi "An Interval Type-2 Fuzzy Logic Approach for Induction Motors Stator Condition Monitoring". IJISET - International Journal of Innovative Science, Engineering & Technology, vol. 1 no. 5, 96-112, July 2014.

[35] M. Khosla, R. K. Sarin and M. Uddin "Design of an Analog CMOS Based Interval Type-2 Fuzzy Logic Controller Chip". International Journal of Artificial Intelligence and Expert Systems, vol. 2, no. 4, 169-186, 2011.

[36] E. A. Jammeh, M. Fleury, C. Wagner, H. Hagras, and M. Ghanbari, "Interval type-2 fuzzy logic congestion control for video streaming

[37] H. Wu and J. M. Mendel "Uncertainty Bounds and Their Use in the Design of Interval Type-2 Fuzzy Logic Systems". IEEE Transactions on Fuzzy Systems, vol. 10, no. 5, 622-640, 2011.

[38] J. Mendel, H. Hagras and R. John Standard Background Material About Interval Type-2 Fuzzy Logic Systems. "Unpublished".

[39] J. Mendel and R. John, "Type-2 fuzzy sets made simple," IEEE Transactions on Fuzzy Systems, vol. 10, no. 2, pp. 117–127, 2002.

[40] N. N. Karnik, J. M. Mendel and Q. Liang, "Type-2 fuzzy logic systems," IEEE Trans on Fuzzy Systems, vol. 7, pp. 643-658, Dec. 1999.

[41] J. M. Mendel and F. Liu, "Super-exponential convergence of the Karnik-Mendel algorithms for computing the centroid of an interval type-2 fuzzy set," accepted for publication in IEEE Trans on Fuzzy Systems, 2006.

[42] Hani Hagras, (2009), "General Type-2 Fuzzy Logic Systems to Enable Better Uncertainty Handling for Real World Application". The University of Essex, England, UK.

[43] U. A. Umoh and U. G. Inyang 'A Fuzzy-Neural Intelligent Trading Model for Stock Price Prediction". IJCSI International Journal of Computer Science Issues, vol. 12, no. 3, pp. 36-44, May 2015.

[44] O. Castillo and P. Melin, Recent Advances in Interval Type-2 Fuzzy Systems vol. 1. USA: Springer, 2012.

AUTHORS

Umoh U. A. had received her Doctor of Philosophy (PhD) degree in Soft Computing from University of Port Harcourt, Rivers State, Nigeria in the year 2012, Master's degree in Database Management System from University of Port Harcourt, Rivers State, Nigeria in the year 2006 and Bachelor's degree from University of Uyo, Akwa Ibom State, Nigeria in 2007. She is currently working as a Senior Lecturer, in the University of Uyo in the Department of Computer Science. She has published several articles in her areas in reputable national and international journals and has written some quality books in Computer discipline. Her area of interest include; Soft Computing (Fuzzy System, Neural network, Hybrid models), Database System, Data Communications, etc. She is a member of Nigerian Computer Society (NCS), Member, Computer Professionals Registration Council of Nigeria (CPN), member, Nigerian Women in Information Technology (NWIT), member, Organization for Women in Science in Developing World (OWSD), member, Universal Association of Computer and Electronics Engineers (UACEE), member, Soft Computing Research Group (SCRS), member, Internet Society (ISOC), etc.

Daniel Asuquo graduated from the University of Calabar, Nigeria, in 2002 with a B.Sc. degree in Computer Science. In 2007, he received a M.Sc. degree in Computer Science from the University of Ibadan, Nigeria and in 2015, he received a Ph.D degree in Computer Science from the University of Port Harcourt, Nigeria. He is a Lecturer I in the department of Computer Science, University of Uyo, Nigeria. His special fields of interest include mobile computing, wireless communications and computer networks as well as web technology. He is an associate member and member of Nigeria Computer Society and Computer Professionals Registration Council of Nigeria, respectively.

DETECTING AND LOCATING PLAGIARISM OF MUSIC MELODIES BY PATH EXPLORATION OVER A BINARY MASK

Mu-Syuan Sie, Cheng-Chin Chiang, Hsiu-Chun Yang and Yi-Le Liu

Department of ComputerScience and Information Engineering
National Dong Hwa University, Taiwan

ABSTRACT

To the best of our knowledge, the issues of automatic detection of music plagiarism have never been addressed before. This paper presents the design of an Automatic Music Melody Plagiarism Detection (AMMPD) method to detect and locate the possible plagiarism in music melodies. The key contribution of the work is an algorithm proposed to address the challenging issues encountered in the AMMPD problem, including (1) the inexact matching of noisy and inaccurate pitches of music audio and (2) the fast detection and positioning of similar subsegments between suspicious music audio. The major novelty of the proposed method is that we address the above two issues in temporal domain by means of a novel path finding approach on a binarized 2-D bit mask in spatial domain. In fact, the proposed AMMPD method can not only identify the similar pieces inside two suspicious music melodies, but also retrieve music audio of similar melodies from a music database given a humming or singing query. Experiments have been conducted to assess the overall performance and examine the effects of various parameters introduced in the proposed method.

KEYWORDS

Music Melody Plagiarism, Music Melody Retrieval, Subsequence Matching, Warping Time Series Join

1. INTRODUCTION

No matter how the modern life changes, music appreciation is always one of the easy and affordable ways to slacken the strain of our daily lives. Nowadays, common users can acquire musical contents easily anywhere and anytime with the Internet. The large demands from the vast number of music-goers have been driving the fast growth of the market of music production, inspiring potential music composers plunging into the realm of music creation. To fit the general tastes of worldwide audience and meet the high production rate requested by music production companies, composers often habitually take some existing popular music pieces as the inspiring sources for faster composition. Occasionally, composers may intentionally or unintentionally mimic some pieces of melodies from others' work, thus may causing the illegal plagiarism of music arts. We all are aware of that illegal piracy of musical intellectual properties can severely obstruct the development of music creation and marketing business. Finding the plagiarized pieces among the fast-growing number of music contents is not trivial. Manual examination costs very high in both time and human power. To prevent the music plagiarism and to keep the prosperous production of the legal music arts, an efficient way to detect automatically the piracy among created music contents becomes highly desirable.

One major challenge of AMMPD is that the plagiarised pieces can appear at any place in a music melody. Exhaustive searching by matching all subsegments of two suspicious music melodies is very time consuming. Additionally, the AMMPD may also suffers from the problem of inexact matching due to some tonal variations on the plagiarized melody pieces. Hence, the AMMPD demands an efficient and effective solution to locate similar melody pieces in two music melodies. The objective of our work presented in this paper is to propose such a solution for developing an AMMPD system.

2. RELATED WORK

According to our literature survey, we have not found any related study on the issues of AMMPD. Most prior arts that have been published are applications relating to retrieval of musical contents. For example, the query by singing/humming (QBSH) are one of the typical topics [1, 2, 3]. The problem of QBSH is different from that of AMMPD. One major difference is that the query input in the QBSH has a clear pair of end points (both the starting point and the ending point) for matching with the partial pieces of each music content in the database. However, for the problem of AMMPD, since we are not aware of where the plagiarised pieces may appear in both the query input and a database content, detecting and locating the plagiarised pieces are thus more cumbersome. Particularly, the possible existence of multiple plagiarised pieces inside two suspicious melodies further complicates the problem.

To address the QBSH problem, the Dynamic Time Warping (DTW) [4] algorithm is a common way to do the nonlinear sequence matching. Athitsos et al. [5] proposed a DTW-based method for approximate subsequence matching of time series. Their method is applicable only to the matching between the whole query input an subsequences of a sequence in the database. For the AMMPD problem that requires intensive subsequence matching between the query input and the database sequence, their method is not feasible. Some methods underlain by the longest common subsequences algorithm [6] are also not suitable because they deal with only noisy-free sequences. That is, the matching between subsequences must be exact matching, instead of the inexact matching required by the tonal features of music audio. Lin et al. [7] presented a method using the rough longest common subsequence algorithm to address the music retrieval problem which is similar to the QBSH. Not aiming at the problem of music processing, Chen et al. proposed a warp time series join (WTSJ) algorithm to find the similar subsegments between two motion sequences as the best part for fusing the two sequences. Though the WTSJ algorithm can locate similar pieces in two motion sequences, the algorithm may suffer from some problems, such as poor alignment and over-segmentation of similar pieces, due to the weak capability in handling noisy elements in sequences.

In this paper, we address the issues of AMMPD by a 2-D spatial-domain approach, rather than the 1-D temporal-domain approach that underlies the methods mentioned above. The proposed method tackles the subsequence matching problem for AMMPD by the path exploration method over a binary mask, which incorporates some image-based techniques, such as gap filling, block partitioning, connected path finding, and polyline approximation of distorted paths. Some tricky designs have been incorporated in the proposed method to handle the noisy pitch features of music audio. The proposed method can not only locate all possible plagiarised subsegments in two suspicious melodies, but also retrieve music contents that contain the melody pieces similar to the input query of a music clip. Hence, the proposed method is feasible for both the AMMPD problem and the QBSH problem.

3. THE PROPOSED METHOD

3.1. Overview

Fig. 1 shows the process flow of the proposed AMMPD method. Given two suspicious music melodies, the pitch extraction module extracts the pitch vectors, $Q = [q(1), q(2), ..., q(F_1)]$ and $D = [d(1), d(2), ..., d(F_2)]$, of the two melodies by a pitch tracking method. Since the two pitch vectors may contain some noisy pitch elements, we smoothen them by applying the median filter of the window size m. From the two smoothed pitch vectors, the pairwise distances between the pitch elements in the pitch vectors are calculated to derive a local distance matrix. By setting a threshold ε, we binarized this local distance matrix as a binary 2-D mask M where an entry $M(i, j) = 1$ indicates a possible correspondence between the pitch pair $(q(i), d(j))$ in the two melodies Q and D. In contrast, an entry of 0 on the mask M means a dissimilar pitch pair in the two melodies. Hence, a rectangular block containing contiguous entries of 1's on M actually identifies preliminarily a potential similar subsegments in the two sequences. One important task for the subsequent processing is to partition the mask into several rectangular blocks that reveals the potential plagiarised subsegments. To avoid the over-partitioning of the mask due to the unexpected pairwise pitch dissimilarity caused by some singular pitch elements, we fill the minor gaps, whose sizes are defined by a parameter g, between blocks before the mask partitioning. After the minor gap filling, the binary mask M is partitioned by finding vertical and horizontal gaps (consecutive entries of 0 along vertical and horizontal directions) between the blocks. Note that the partitioning is repeatedly done on every block until no vertical or horizontal gap appears on the block. After the partitioning, all paths of connected 1-entries inside each block are explored. Meanwhile, the detailed correspondences between the pitch elements along the path are also derived. Afterwards, multiple overlapping paths in each block can be ranked according to the derived detailed correspondences. An explored path may also have some distorted sections that reveal unreasonable many-to-one or one-to-many correspondences between pitch elements. These many-to-one and one-to-many correspondences alone the path can usually be found on the sections that are horizontal/near-horizontal or vertical/near-vertical. Hence, we remove these distorted sections by approximating the path with multiple polylines and removing those polylines that are horizontal/near-horizontal or vertical/near-vertical. Eventually, those paths that are too short to identify plagiarised subsegments are eliminated.

3.2. Pitch Vector Extraction of Music Audio

A digitized music data contains a sequence of audio data sampled at a fixed rate such as 8KHz or 16KHz. The data sequence is then partitioned into frames with each containing a fixed number of samples and overlapping partially with its neighboring frames. Applying the pitch tracking method [8] to each frame, we can estimate the fundamental frequency of the audio samples as the pitch of the frame. Given a fundamental frequency f, the pitch corresponds to a semitone $n = 69 + 12\log_2(f/440)$ which ranges normally over 35~72 for male sounds and 45~83 for female sounds. Therefore, an music audio of F frames can get a pitch vector of F semitones to characterize the tonal feature.

Unfortunately, the estimated fundamental frequency of each frame is not always robust under the disturbance of noisy audio signal. The output pitch vector may contain some noisy semitones which can incur undesired effects on matching music melodies. To reduce the effect of the noisy semitones, we perform the median filtering on the elements of the pitch vector to remove some singular noise pitch elements. However, for some continuous occurrences of noisy pitch elements, other methods is still necessary to remedy the possible side effects. We will present a way in later descriptions of the proposed method.
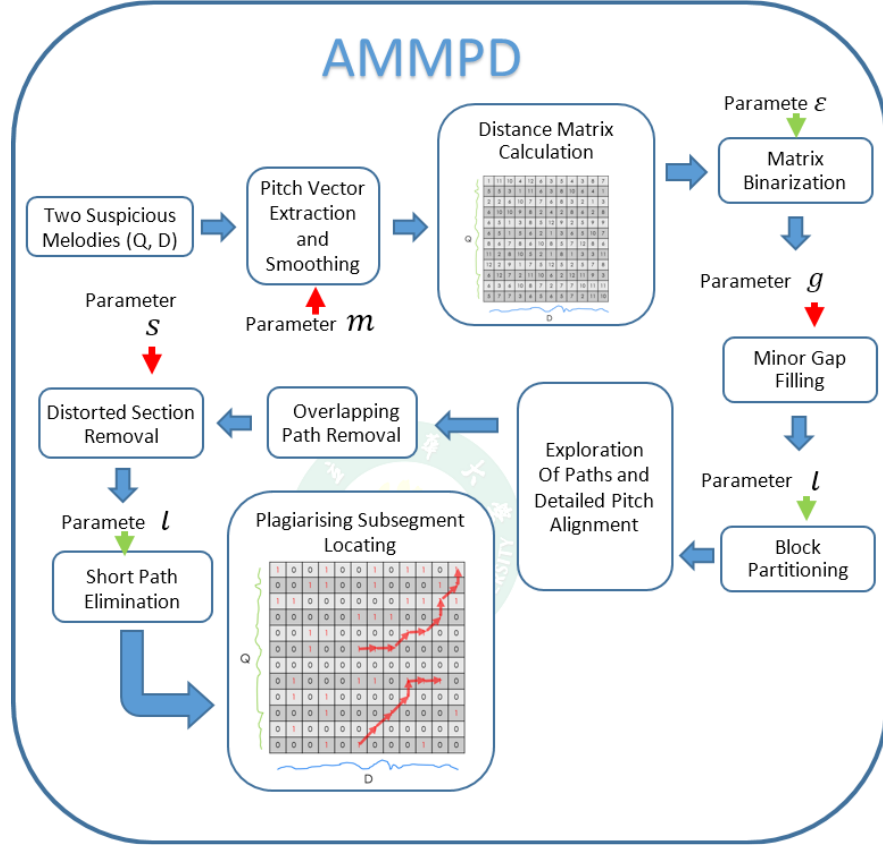
Figure 1: The process flow of the proposed AMMPD method.

3.3. Distance Matrix Calculation and Binarization

Let $Q = [q(1), q(2), ..., q(F_1)]^T$ and $D = [d(1), d(2), ..., d(F_2)]^T$ be the pitch vectors of two suspicious music melodies. Computing the pairwise distances between the pitch elements in the two vectors lead to a 2-D distance matrix $\mathbb{D}(i, j) = |q(i) - d(j)|$ for $1 \leq i \leq F_1$ and $1 \leq j \leq F_2$. The entries in the matrix $\mathbb{D}$ can be quantized into similar indications and dissimilar indications by specifying a distance threshold ε which defines the maximal dissimilarities allowed between the pitch elements of two plagiarised pieces. In other words, we can derive a 2-D binary mask M by

$$M(i, j) = \begin{cases} 1, & if\ \mathbb{D}(i, j) < \varepsilon, \\ 0, & otherwise, \end{cases}$$

where an an entry $M(i, j)$ of 1 indicates a similar pair of pitch elements $(q(i), d(j))$ in the two suspicious melodies. On the contrary, an entry of 0 implies that the pitch elements $q(i)$ and $d(j)$ are too different to be two corresponding pitches in plagiarised pieces. Fig. 2 shows an example of $\mathbb{D}$ and M with the threshold ε of 4.

Figure 2: Given a threshold ε of 4, the 2-D distance matrix $\mathbb{D}$ (the left matrix) and the 2-D binary mask M (the right matrix) derived from two pitch vectors Q and D.
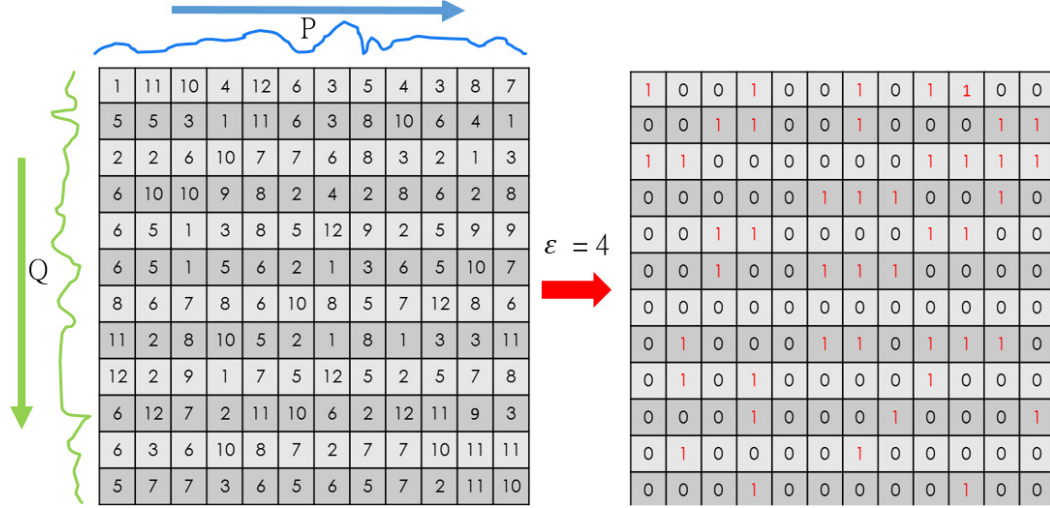
3.4. Minor Gap Filling

On the derived binary mask, we can find some entries of 1 connected as many paths. A path may start from a certain entry $M(i,j)$ and stop at another $M(i',j')$. We denote such a path as $o(u(i,j) \Rightarrow u'(i',j'))$, where u and u' are called nodes. Note that the entry of the mask on a node is always 1. Besides, a node (i,j) can have at most only three possible preceding nodes, i.e., $(i-1,j)$, $(i,j-1)$, $(i-1,j-1)$. For convenience, we also use the notations, $u.i$ and $u.j$, to represent the row index and column index of the node u, respectively. In physical meaning, each path actually corresponds a pair of potential plagiarised subsegments $q(i:i')$ and $d(j:j')$ in the two melodies, respectively. Hence, one important task of the proposed AMMPD method is to explore all potential connected paths over the binary mask M.

Since every path always breaks at an entry of 0 on M, the exploration of the paths can be done by finding rectangular blocks separated by horizontal and vertical gaps formed by 0-entries. However, the separation of rectangular blocks are prone to the gaps formed by some singular nodes (i,j)'s with larger pairwise distances $\mathbb{D}(i,j)$'s incurred from noisy pitch elements. Like the binary mask shown in Fig. 3 (a), the red areas and white areas contain respectively 1-entries and 0-entries. A small gap appearing on the singular node of entry-0 highlighted with the blue circle breaks a path. As a result, the broken path may cut the true plagiarised subsegments, as shown in Fig. 3 (b), into shorter ones.

To avoid the bad break of paths, we perform a gap filling process to bridge the paths separated by the singular nodes. This filling process fills those entries between a node and the nearest node along the horizontal, the vertical, and the diagonal direction according to the following three rules:

- Horizontal Filling: $M(i+k,j) = 1$ for $1 \le k \le k^* - 1 \le g$ if $M(i+k,j) = 0 \wedge M(i+k^*,j) = 1$;

- Vertical Filling: $M(i,j+k) = 1$ for $1 \le k \le k^* - 1 \le g$ if $M(i,j+k) = 0 \wedge M(i,j+k^*) = 1$;

- Diagonal Filling: $M(i+k,j+k) = 1$ for $1 \le k \le k^* - 1 \le g$ if $M(i+k,j+k) = 0 \wedge M(i+k^*,j+k^*) = 1$;

Note that the parameter g is set as the largest gap width allowed for the gap filling. The gaps with the width larger than g will not be filled. Taking the case in Fig. 3 (a) as an example, the resultant path explored after the gap filling is the one shown in Fig. 3 (b).
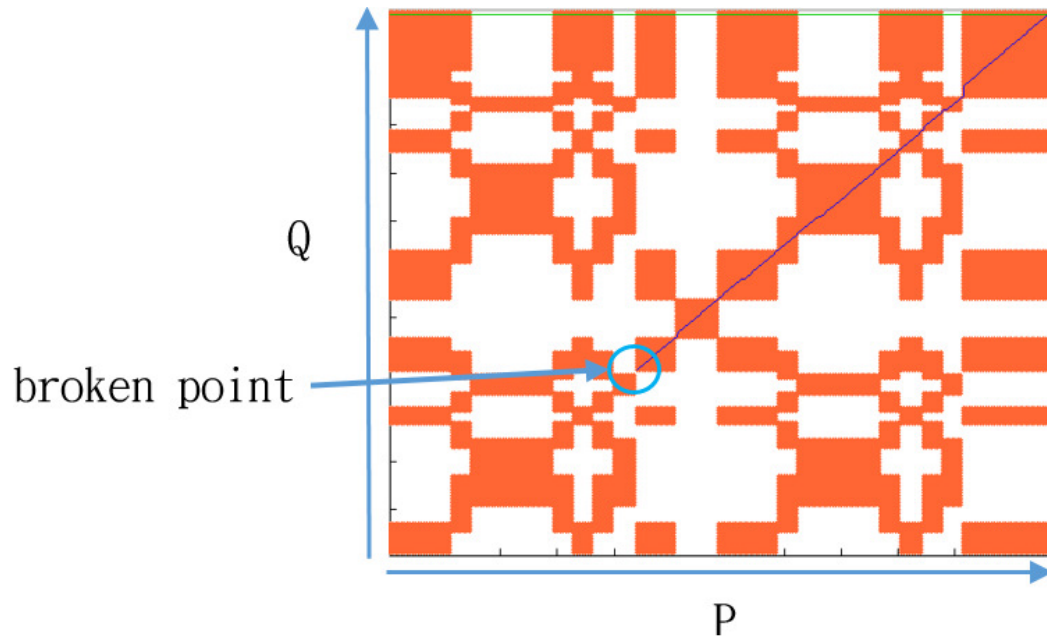
(a) the bad break point cuts a path into a shorter one.
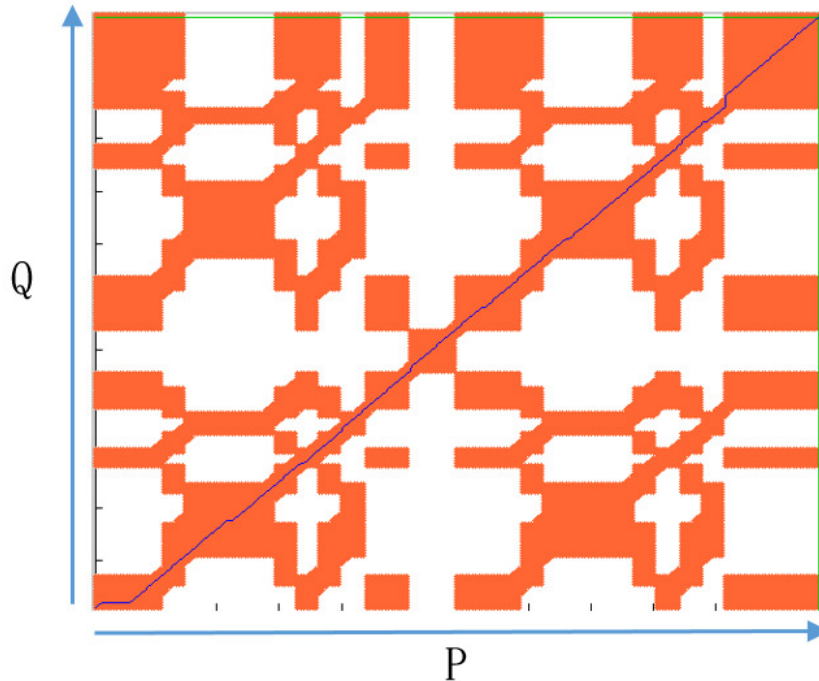
(b) the longer path formed in the block without the bad break point.

Figure 3: Improper partitioning of blocks of caused by noisy pitch elements.

3.5. Block Partitioning

Some paths of connected 1-entries are not long enough to identify a pair of plagiarized subsegments in two melodies. To fast remove these paths before exploring the connected nodes in them, we exploit a recursive block partitioning procedure on the binary mask to extract all potential rectangular blocks that enclose the paths. If the size of a block is too small, then all paths inside the block can be ignored directly with having to explore the connected nodes along them. The steps of the recursive block partitioning procedure $Partition()$ are listed in Procedure 1. The blocks on the mask M can be derived by making a call to $Partition(1, F_1, 1, F_2)$, where F_1 and F_2 are the height and width of M, respectively.

In the set of blocks obtained from the partitioning procedure, any block B can be discarded if $width(B) < l$ or $height(B) < l$, where l specifies the smallest length of any plagiarised subsegment. This would save the efforts to explore all connected nodes along the paths inside the block B.

Procedure 1 $Partition(b, t, l, r)$

Input: the rectangular block B corresponding to $M(bottom = b, top = t, left = l, right = r)$, where $l < r \wedge b < t$.
Output: a set of disjoint subblocks ($\mathbb{B}$) inside the block B

1: Compute the sum of each row in M covered by the block B by $S_R(i) = \sum\limits_{j=l}^{r} M(i, j)$, for $b \le i \le t$

2: Compute the sum of each column in M covered by the block B by $S_C(j) = \sum\limits_{j=b}^{t} M(i, j)$, for $l \le j \le r$

3: Set $G_R = \{i | S_R(i) = 0\} = \{g_r(1), g_r(2), \ldots, g_r(N)\}$, where $g_r(i) < g_r(i + 1)$ for $i = 1, 2, \ldots, N - 1$.
4: Set $G_C = \{j | S_C(j) = 0\} = \{g_c(1), g_c(2), \ldots, g_c(M)\}$, where $g_c(j) < g_c(j + 1)$ for $j = 1, 2, \ldots, M - 1$.
5: **if** $M = 1 \wedge N = 1$ **then return** $\mathbb{B} = \{B\}$
6: **else**
7:     **for** each $i = 1, \ldots, N - 1$ **do**
8:         **for** each $j = 1, \ldots, M - 1$ **do**
9:             $b \leftarrow g_r(i)$
10:             $t \leftarrow g_r(i + 1)$
11:             $l \leftarrow g_c(j)$
12:             $r \leftarrow g_c(j + 1)$
13:             $\mathbb{B} \leftarrow \mathbb{B} \bigcup Partition(b, t, l, r)$.

3.6. Path Exploration by Finding Detailed Alignment of Pitch Elements

Once the blocks inside the binary mask are available, the paths inside each block need to be explored. A path is a sequence of connected nodes. The starting node (i, j) is an open node that has no preceding nodes, i.e., $M(i - 1, j) = M(i, j - 1) = M(i - 1, j - 1) = 0$. In contrast, the stopping node (i, j) of a path is a close node that has no succeeding nodes, i.e., $M(i + 1, j) = M(i, j + 1) = M(i + 1. j + 1) = 0$. Any node that is neither an open node nor a close node is an intermediate node. Hence, all nodes in a block actually form a directed acyclic graph (DAG). Every node corresponds to a graph node. A graph node (i, j) connects only to its preceding nodes $(i - 1, j)$, $(i, j - 1)$, and $(i - 1, j - 1)$ if the three nodes of 1-entries do exist (nodes do not exist for 0-entries). With the constructed DAG, all paths from an open node (u_o) to a close node (u_c) can be found by the procedure $Explore(u_o, u_c)$ listed in Procedure 2. Some notations are introduced in the procedure. First, $predecessor(u)$ and $successor(u)$ mean the direct succeeding nodes and the direct preceding nodes of a node u, respectively. The notation $c(u \triangleright u')$ denotes a connection connecting the two nodes u and u'. The operator $c \oplus o$ denotes the concatenation of a connection c and a path o. To explore all paths inside a block, we just need to find all open nodes and close nodes and then make a call to the procedure $Explore(u_o, u_c)$ for each pair of open node u_o and close node u_c.

There might exist relations of dominance among the paths explored by the $Explore()$ procedure. A path $o(u \Rightarrow v)$ dominates another path $o'(u' \Rightarrow v')$ if $(u.i <= u'.i) \wedge (u.j <= u'.j) \wedge (v.i > v'.i) \wedge (v.j > v'.j)$. The physical meaning of the dominance is that the plagiarised subsegment implied by the path o contains that implied by the path o'. In case that a path o dominates another path o' in the set of explored paths, then o' is removed from the path set because it is redundant.

Procedure 2 $Explore(u_0, u_1)$

Input: a node u_0 and a node u_1 in the same block.

Output: a set of paths (O) starting from u_0 and stopping at u_1.

1: **if** $u_0 \in predecessor(u_1)$ **then**
2:     **return** $O' = \{o(u_0 \Rightarrow u_1)\}$
3: **else if** $(u_o.i > u_1.i) \vee (u_0.j > u_1.j) \vee (successor(u_0) = \phi)$ **then**
4:     **return** $O' = \phi$
5: **for** $u \in successor(u_0)$ **do**
6:     $O' \leftarrow Explorer(u, u_1)$
7: $O = \phi$
8: **for** $o \in O'$ **do**
9:     $O \leftarrow O \bigcup \{c(u_0 \rhd u) \oplus o\}$

3.7. Overlapping Path Removal

After removing all dominated paths from the set of explored paths, some paths may overlap with others. The overlapping paths may share some connected nodes, but do not dominate each other. As shown in Fig. 4, three paths share a large portion of the paths. However, these three paths identify three different pairs of plagiarized subsegments in the two melodies. Similarly, the three pairs of plagiarized subsegments also have a large part in common and thus may cause redundant detection of plagiarism. One reasonable action is to choose the best one among them. To do this, we need to define a criterion for assessing the goodness of a path. As every explored path contains a sequence of connected nodes $u(i, j)$, with each meaning a corresponding pair of pitch elements $(q(i), d(j))$. Along the path, every two neighboring nodes must be a node u and a successor node of the node u. Hence, a path can consist of three kinds of connections for any two neighboring nodes, including vertical, horizontal, and diagonal node connections. A vertical node connection $(i - 1, j) \rhd (i, j)$ implies a two-to-one correspondence of pitch elements, i.e., $\{q(i - 1), q(i)\} \rightarrow \{d(j)\}$. A vertical node connection $(i, j - 1) \rhd (i, j)$ implies a one-to-two correspondence of pitch elements, i.e., $\{q(i)\} \rightarrow \{d(j - 1), d(j)\}$. A diagonal node connection $(i - 1, j - 1) \rhd (i, j)$ implies a one-to-one correspondence, i.e., $\{q(i - 1)\} \rightarrow \{d(j - 1)\}$ and $\{q(i)\} \rightarrow \{d(j)\}$. Obviously, the one-to-one correspondence gives a better explanation to the correspondence between elements of plagiarised subsegments. Therefore, a feasible index to assess the goodness of a path o the number of diagonal node connections, say $Diag(o)$, along the path. Based on the criterion, $Diag(o)$, the procedure to remove those overlapping paths with lower values of $Diag(o)$ is designed as the $RemoveOverlappingPaths(O, l)$ listed in Procedure 3.

Procedure 3 $RemoveOverlappingPaths(O, l)$

Input: the set of paths (O) in a block; the lower bound on the length (l) of the overlapping part between two overlapping paths

Output: the paths O' which contains no overlapping paths

   for $o(u \Rightarrow v) \in O$ **do**
       for $o'(u' \Rightarrow v') \in O \wedge o' \neq o$ **do**
           if $Overlap(o, o') \geq l$ **then**
               if $Diag(o) > Diag(o')$ **then**
                   $O \leftarrow O - \{o'\}$
               else
                   $O \leftarrow O - \{o\}$
   return O
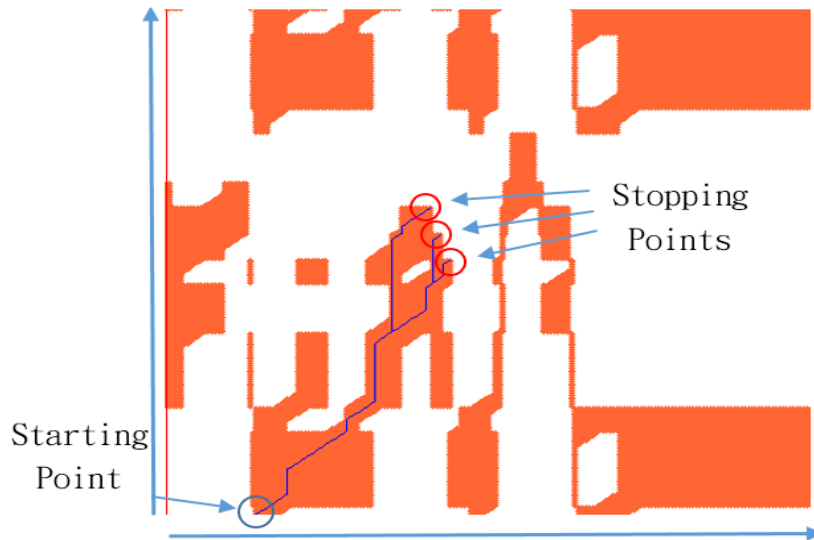
Figure 4: Example cases of overlapped paths.

3.8. Removal of Distorted Sections in Eligible Paths

Every path that remains after the overlapping path removal is an eligible path for identifying plagiarised subsegments between the two suspicious melodies. However, there may still exist one kind of oddness on the path. Taking Fig. 5 as an example, we can see that some nodes have one-to-many or many-to-one correspondences, as highlighted with blue circles. These one-to-many correspondences or many-to-one correspondences would cause longer sections of vertical node connections or horizontal node connections inside the path. We refer to this kind of sections as distorted sections which may not be appropriate to identify the pieces in plagiarised subsegments. Namely, we should remove these distorted sections from a path to prevent false detection of plagiarised pieces.
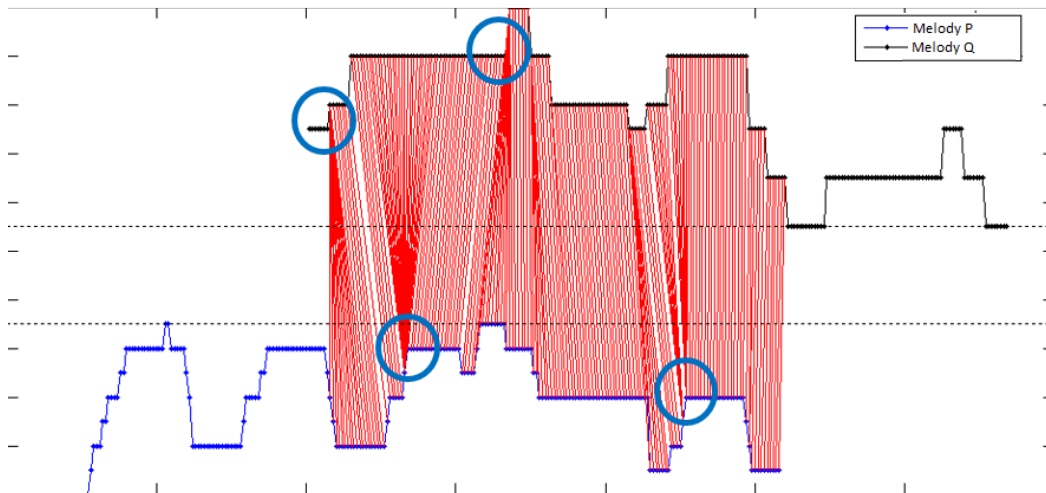
Figure 5: The alignment of the pitch elements between two melodies may contain unreasonable one-to-many and many-to-one correspondences.

As shown in Fig. 6(a), a long path may comprise several horizontal and vertical sections highlighted with circles. The distorted sections in blue circles are longer, while those in red circles are shorter. For the path illustrated in Fig.6(a), the true section corresponding to the

plagiarised subsegments in the two melodies is the section enclosed by the large blue rectangle. To extract the non-distorted sections from an eligible path, our method first approximates the path with a polyline. Afterwards, the horizontal/vertical and near-horizontal/near-vertical segments in the polyline are removed. In doing so, a segment $\bar{o}$ in the polyline is removed if $|slope(\bar{o}) - 1| > \delta$, where $slope(\bar{o})$ is the slope of the segment $\bar{o}$ and δ is the threshold specified for the removal. Fig. 6(b) shows the result after applying the method to the path in Fig. 6(a). The result demonstrates that this method works fine to extract the desired non-distorted section from the path.

(a)   The path with distorted sections

(b) The segmented paths after removing distorted sections
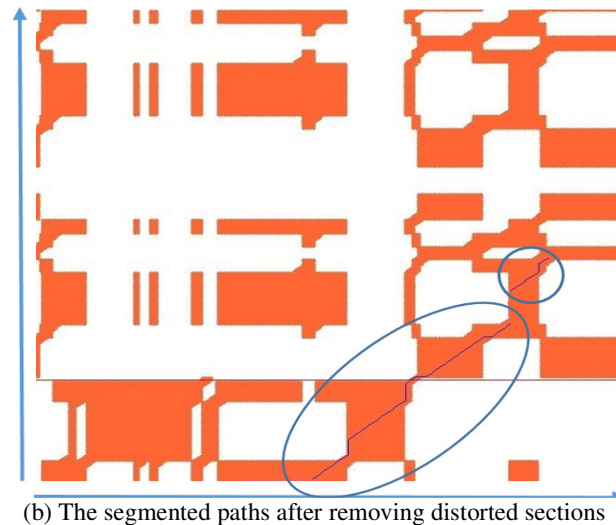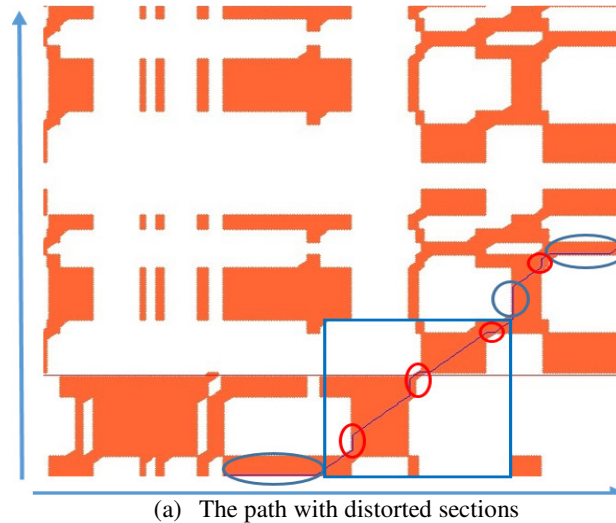
Figure 6: Examples of distorted sections in a path.

After removing the distorted sections in a path, some paths may become shorter and even dominated by others. These paths should be purged, too. According to the specified parameter l in block partitioning, we discard those paths with the lengths smaller than l. Additionally, as done at the end of path exploration, the path dominated by others are also discarded.

4. EXPERIMENTAL RESULTS

4.1. Data Set and Types of Experiments

Several experiments are conducted to evaluate the performance of the proposed method. We use the MIR-QBSH data set created by Chang et al [9] for the experiments. The data set contains 48 ground-truth MIDI files and 4431 singing/humming clips from about 195 subjects. Since the songs in the data set does not contain the plagiarising pieces, we randomly partition the 48 MIDIs into 16 groups, with each having three. Then, the three MIDIs in each group are concatenated as on MIDI to get 16 concatenated MIDI songs. Besides, we also randomly compose 100 concatenated voiced songs from 300 signing/humming clips which enclose all melodies of the 48 MIDIs sung/hummed by at least 6 different subjects. Each concatenated voiced song also has three different signing/humming clips. Three types of experiments are conducted on the composed data set. Type A experiments use one concatenated voiced MIDI song as the input and search the possible plagiarising pieces in all concatenated voiced songs of the database. Type B experiments use one single MIDI song (not a concatenated MIDI song) as the input and search the possible plagiarism in all concatenated voiced songs of the database. Finally, Type C experiments use a single MIDI song as the input and search the similar single signing/humming clips. The indices for performance evaluation are the precision rate and the recall rate. A correct detection of a plagiarising subsegment requires that the following condition hold true for the detected subsegment d and the true plagiarising subsegments in two melodies a and b:

$$\left(\frac{len(d \cap a)}{len(a)} \geq \frac{1}{3}\right) \wedge \left(\frac{len(d \cap b)}{len(b)} \geq \frac{1}{3}\right),$$

where $len(s)$ denotes the length of a subsegment s.

4.2. Overall Performance Evaluation

The performance of the proposed method is evaluated from the results of the three types of experiments. Table 1 lists the averaged precision rate and recall rate for these three types of experiments. The achieved precision rate is about 84% and the recall rate is about 63%. Because of the inaccuracy of pitch extraction, the recall rates are much lower than the precision rates. The noisy pitch vectors can cause the mismatch of many subsegments with similar melodies in suspicious music audio. The median filtering and block gap filling proposed in the method seem take only minor effect in handling the noisy pitch features. Particularly, the query input, which is a MIDI clip, and the database targets, which are humming/singing clips, are different audio source which reveal different audio characteristics. Moreover, as the pitch of a humming/singing clip varies with different subjects, the pitch vectors extracted from the audio clips of the same melody still may differ significantly for different subjects.

Table 1. The overall precision rates and recall rates for the three types of experiments. X_p and X_r denote respectively the precision rate and the recall rate of Type X experiments.

A_p(%)	A_r(%)	B_p(%)	B_r(%)	C_p(%)	C_r(%)
82	64	83	63	87	63

4.3. Examining the Effects of Different Parameters

There are some parameters introduced in the proposed method, including

- ε: the upper bound on the pairwise distances of pitch elements in two suspicious melodies;

- l: the lower bound on the length of an eligible candidate path for locating the plagiarising subsegments in two melodies;

- g: the parameter defining the upper bound on the minor gaps to be filled between blocks on the binary mask M;

- δ: the slope parameter used for removing the distorted sections along an eligible path.

In the following, the effects of these parameters are examined and discussed with the experimental results.

4.3.1. The Effect of ε

The parameter ε affects mainly the number of blocks formed on the binary mask M. Table 2 shows the precision rates and recall rates corresponding to the different settings of ε, i.e., ε=0, 1, and 2. All other parameters are set as m=5, l=150, g=3, and δ=0.4. The extremal case of $\varepsilon = 0$ causes that two suspicious melodies are detected as plagiarism only when they are exactly identical. The results show that a higher setting can increase the recall rate because it allows larger pitch differences between two plagiarising subsegments. However, loosened condition of plagiarism may also increases the number of false alarms and thus decreases the precision rate.

Table 2: The precision rates and recall rates for different setting of ε. X_p and X_r denote respectively the precision rate and the recall rate of Type X experiments.

ε	A_p(%)	A_r(%)	B_p(%)	B_r(%)	C_p(%)	C_r(%)
0	100	0	100	0	100	0
1	82	64	83	63	87	63
2	27	80	31	79	35	79

4.3.2. The Effect of l

The parameter l specifies at least how long a true plagiarisinig subsegement must be. We test l with the different values 120, 130, 140, 150, and 160. Note that a length of 150 pitch elements is about 150*0.032 (=4.8) seconds. Table 3 lists the precision rates and recall rates for these different settings. The larger the l, the longer the plagiarising subsegments must be. Therefore, some shorter plagiarising subsegments are more likely to be missed and the recall rate tends to decrease. On the other hand, some shorter false alarms can be avoided and thus the precision rate tends to increase.

Table 3: The precision rates and recall rates for different setting of l.

l	A_p(%)	A_r(%)	B_p(%)	B_r(%)	C_p(%)	C_r(%)
120	33	76	36	76	41	76
130	51	74	54	73	59	72
140	67	69	70	69	74	69
150	82	64	83	63	87	63
160	89	60	90	59	92	59

4.3.3. The Effect of g

The parameter g defines the upper bound on the minor gaps between blocks on the binary mask M. To prevent the binary mask being over-partitioned into many small blocks, the proposed method fills the minor gaps between blocks. A larger value of g causes more blocks connected through the gap filling process, thus usually resulting in more detected plagiarising subsegments. Though the increased detection of plagiarism improves the recall rate, the precision rate may decrease due to the increased number of false alarms. The precision rates and the recall rates for different settings of g are shown in Table 4. The results show that an appropriate value for the parameter g ranges between 3 and 5.

Table 4: The precision rates and recall rates for different setting of g.

g	$A_p(\%)$	$A_r(\%)$	$B_p(\%)$	$B_r(\%)$	$C_p(\%)$	$C_r(\%)$
0	88	38	88	38	90	38
1	85	49	86	49	89	49
2	84	54	86	54	89	54
3	82	64	83	63	87	63
4	79	69	80	69	86	69
5	72	74	74	73	81	73
6	66	76	70	75	77	74
7	59	76	63	75	71	75

4.3.4 The Effect of δ

The parameter δ specifies the deviation of the slope of a path from a 45° diagonal line. A large deviation indicate that the path is a distorted path which contains improper alignment of pitch elements and should be discarded. Hence we experiment the proposed method with the settings of δ ranging between 0.1 and 0.8. The smaller the δ is, the better element correspondences an eligible path may derive, meaning that a better precision rate we may achieve. However, the side effect is that some true plagiarising subsegments with slightly distorted correspondences may be missed. Table 5 shows the precision rates and recall rates for the different settings of δ.

Table 5: The precision rates and recall rates for different setting of δ.

δ	$A_p(\%)$	$A_r(\%)$	$B_p(\%)$	$B_r(\%)$	$C_p(\%)$	$C_r(\%)$
0.1	89	41	88	41	89	41
0.2	88	53	88	53	89	53
0.3	86	60	87	59	90	59
0.4	82	64	83	63	87	63
0.5	74	65	76	65	80	64
0.6	65	67	69	66	73	65
0.7	52	69	57	67	63	66
0.8	36	70	41	68	49	67

3. CONCLUDING REMARKS

The paper presents a novel method to address the problem of AMMPD. The novelty originates from the tackling of the challenging issues of detecting and locating plagiarised subsegments between two suspicious music melodies through an image-based approach in spatial domain. The proposed method performs mainly the path exploration over a 2-D binary mask. The key contribution of the proposed method is a feasible solution to the two major issues in AMMPD, including (1) the inexact matching of noisy and inaccurate pitches of music audio and (2) the fast detection and positioning of similar subsegments between suspicious music audio. In fact, the proposed method is applicable to not only the applications of AMMPD, but also the applications of querying by humming/singing (QBSH).

REFERENCES

[1] Chung-Che Wang, Jyh-Shing Roger Jang, and Wennen Wang, "An improved query by singing/humming systemusing melody and lyrics information.," in ISMIR. Citeseer, 2010, pp. 45–50.

[2] Hung-Ming Yu, Wei-Ho Tsai, and Hsin-Min Wang, "A query-by-singing system for retrieving karaoke music,"IEEE Transactions on multimedia, vol. 10, no. 8, pp. 1626–1637, 2008.

[3] Yunjing Wang, "Similarity matching method for music melody retrieval," Journal of Multimedia, vol. 8, no. 4, pp.386–393, 2013.

[4] Donald J Berndt and James Clifford, "Using dynamic time warping to find patterns in time series." in KDDworkshop. Seattle, WA, 1994, vol. 10, pp. 359–370.

[5] Vassilis Athitsos, Panagiotis Papapetrou, Michalis Potamias, George Kollios, and Dimitrios Gunopulos, "Approximate embedding-based subsequence matching of time series," in Proceedings of the 2008 ACM SIGMOD International Conference on Management of data. ACM, 2008, pp. 365–378.

[6] Mike Paterson and Vlado Danˇcˊık, "Longest common subsequences," in International Symposium on MathematicalFoundations of Computer Science. Springer, 1994, pp. 127–142.

[7] Hwei-Jen Lin, Hung-Hsuan Wu, and Chun-Wei Wang, "Music matching based on rough longest common subsequence.," J. Inf. Sci. Eng., vol. 27, no. 1, pp. 95–110, 2011.

[8] Li Hui, Bei-qian Dai, and Lu Wei, "A pitch detection algorithm based on amdf and acf," in 2006 IEEE InternationalConference on Acoustics Speech and Signal Processing Proceedings. IEEE, 2006, vol. 1, pp. I–I.

[9] Roger Chang, "MIR-QBSH dataset," http://mirlab.org/dataSet/public/.

AUTHORS

Cheng-Chin Chiang received his Ph.D. degree in the Department of Computer Science and Information Engineering from National Chiao Tung University in Taiwan in 1993. He is now a professor at the Department of Computer Science and Information Engineering in National Dong Hwa University. His research interests include neural networks, pattern recognition, machine learning, multimedia processing and analysis, and virtual reality and augmented reality.

Mu-Syuan Sie received his Master degree in the Department of Computer Science and Information Engineering from National Dong Hwa University in Taiwan in 2015. He is now a multimedia system software engineer in MediaTek Inc. His research interests include human-machine interactions, machine learning, pattern recognition, and multimedia retrieval.

Hsiu-Chun Yangis pursuing his Master degree in the Department of Computer Science and Information Engineering from National Dong Hwa University. His research interests include machine learning, pattern recognition, and musical informationprocessing and retrieval.

Yi-Le Liuis pursuing his Master degree in the Department of Computer Science and Information Engineering from National Dong Hwa University. His research interests include machine learning, neural networks, pattern recognition, and content-based image retrieval.

INTENTIONAL BLANK

PD-FUZZY CONTROL OF SINGLE LOWER LIMB EXOSKELETON FOR HEMIPLEGIA MOBILITY

Abdullah K Alshatti[1] and M. O. Tokhi[2]

[1]Department of Automatic Control and System Engineering,
University of Sheffield, United Kingdom
[2] School of Engineering, London South Bank University, United Kingdom

ABSTRACT

This paper presents studies in the design and control of single leg exoskeleton for hemiplegia mobility in simulation environment. The exoskeleton is designed to support the affected side of the hemiplegia patient while the other leg functions normally. Hip, knee and ankle joints for both humanoid leg and exoskeleton of the affected side are controlled using PD-Fuzzy control to obtain the required natural torque to allow the exoskeleton to compensate for the deficiency in affected leg to achieve normal symmetric gait. The controller is implemented in MATLAB, and the system behaviour observed in Visual Nastran 4D (VN4D) during simulation. Simulation results show that the exoskeleton can support the humanoid with the required augmentation using the proposed design and control.

KEYWORDS

Assistive robotics, Fuzzy logic control, Hemiplegia mobility.

1. INTRODUCTION

The human locomotion process depends on collaboration between the neuromuscular and musculoskeletal systems for achieving symmetric gait cycle, and any condition of injury, illness or disease will affect the nature of human walking pattern [1]. Human walking disorder can be related to different types of physical conditions such as limb amputation, paralysis, disability and injury. Human walking disorder can result in reduced ability in performing daily life activities due to reduced functionality of muscles as in elderly people or due to medical or physical conditions in general. In order to provide better quality of life for people who experience gait disorder so as to perform their usual daily tasks, attempts have been made to develop various solutions to assist and support their locomotion. According to the world health organization, worldwide 250,000 to 500,000 suffer from spinal cord injury every year. Spinal cord injury (SCI) symptoms may include loss of full or partial body limb control and sensory functions, and one of the essential measures to improve SCI medical care and rehabilitation services is to provide assistive devices to enable SCI patients to perform their daily life activities, but only 5-15 % of people who live in low and middle-income countries can afford assistive devices [2]. Providing innovative solutions to people with mobility disorder becomes an interesting area for researchers. By utilising control algorithms, sensory systems and appropriate motors, assistive robotics can be one of the cutting-edge solutions to deliver the right amount of support needed to assist people with mobility disorder.

This paper initially presents a brief background about exoskeleton applications. Then the approach for design and control of humanoid and exoskeleton model is described. Simulation results are then presented, discussed and conclusion are drawn. The work presented in this paper builds up on previous work of the authors [3].

2. BACKGROUND

Exoskeletons can be categorised into two main types, namely assistive exoskeletons and rehabilitation exoskeletons and the design mechanisms vary based on application, such as full or partial body and lower or upper extremity. The current exoskeleton designs include three types, namely performance exoskeletons, rehabilitation exoskeletons and assistive exoskeletons [4]. Performance exoskeletons are developed for supplementation of human physical ability to perform tasks such as lifting heavy weight, rehabilitation exoskeletons are developed to help people who suffer from neurological injury to retrieve their mobility and assistive exoskeletons are developed to benefit people with mobility disorders to perform daily tasks. Research in exoskeleton systems has intensified in the late 20th century and researchers have reported various novel models of wearable robotics, and exoskeleton has become a research focus in the field of robotics [5].

Exoskeletons and active orthosis are currently considered as viable human physical assistance and support devices. In the last few years several efforts have been made to integrate robotics technology to human body in order to improve human physical abilities for better performance and one of these efforts is the exoskeleton, also referred to as active orthosis. Late 1960s, "Hardiman" considered one of the earliest full body exoskeleton developed by General Electric in cooperation with Cornell University to augment wearer strength. "Hardiman" was hydraulically power-driven machine with 30 DOF [6]. Berkeley lower extremity exoskeleton (BLEEX) is one of the first autonomous load carrying exoskeletons with seven DOF in each leg with actuated joint supporting hip, knee and ankle while three DOF are unactuated on ankle and hip [7]. Exoskeletons are also considered in the medical field especially for rehabilitation and gait disorder enhancement. Berkeley Bionic designed assistive exoskeleton (eLEGS) to support lower limbs of paralyzed patients to stand up and walk by actuating hip and knee joints and with the ankle actuated by passive spring, using finite state machine to differentiate between the four states in stride cycle to obtain the walking movement [8]. Cyberdyne launched the HAL (hybrid assistive leg) series of exoskeletons. HAL-5 has been designed to physically strengthen healthy people and assist people with gait disorder to perform their daily tasks, where the assistive strategy determined by using controller based on activity of the hip and knee (flexion/extension) actuators and recording walking pattern of the operator. EMG, GRF, potentiometer, gyroscope and accelerometer sensors are used to feed the controller with the essential data [9].

Exoskeleton robotic developments are still considered by researchers as challenge with many technological issues. Lightweight, energy consumption and exoskeleton design aspects are essential to the operator adaptability and functionality, but more sensors and actuation used in the exoskeleton device will lead to more operating complexity and high power consumption [10]. In addition, the cost of available commercial exoskeletons is too high. Therefore, one of the challenges and motivations in exoskeleton developments is to make them cheaper and affordable by considering the technology selection and exoskeleton design.

3. SYSTEM MODEL

The exoskeleton and humanoid model presented in this paper consists of different joint motors, links, exoskeleton frame and the controller. With such complexity of the system, modelling and design method using finite element analysis (FEA) has been selected to analysis how the

exoskeleton reacts to various forces, disturbances as well as different controllers. The software facilities used to design the humanoid model and exoskeleton model comprise Solid Works and Visual Nastran 4D software. MATLAB software is used to develop the controller and simulation of the whole system model by integrating Visual Nastran 4D with MATLAB Simulink. The humanoid model with exoskeleton on the right leg was used to replicate real human movements by using torque as input and orientation as output representing hip and knee joints positions by using Visual Nastran 4D meter and control features.

3.1. Humanoid

The humanoid model shown in Figure 1 is designed to simulate human body characteristics such as width, height and weight, and replicate human physical appearance and movements according to the anthropometric data given in [11]. The humanoid model represents 75 Kg in weight and 1.7 m in height. Humanoid parts and limbs were designed in Solid Works then exported and assembled in Visual Nastran software. The assembly of the humanoid design is based on different aspects such as degree of freedom, type of joint and axes of rotation. Each body segment is connected by choosing the appropriate joint constraints to activate and control the humanoid motion during the simulation. The humanoid joints are designed to perform motion in the sagittal plane while other axes are locked.
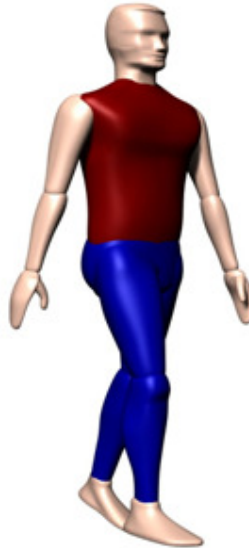
Figure 1. Humanoid model

3.2. Exoskeleton

Passive orthosis is widely used to support human movement due to lightweight, compact fitting and easy to operate compared to active orthosis or exoskeletons, but exoskeleton can support human with extra mechanical power to augment their ability to perform daily tasks. The concept of the exoskeleton design in this research is based on supporting people with hemiplegia paralysis to restore gait disorder. The exoskeleton shown in Figure 2 is designed to fit the right side of wearer lower limb and actuate hip, knee and ankle joints. The exoskeleton structure was designed in Solid Works then exported and assembled in Visual Nastran 4D using body tools. Hip, knee and ankle joints of the exoskeleton were set to be parallel in position with humanoid hip, knee and ankle joints and rotate in the sagittal plane (Y axis). Revolute motors are used to actuate the exoskeleton hip and knee joints during the simulation process.
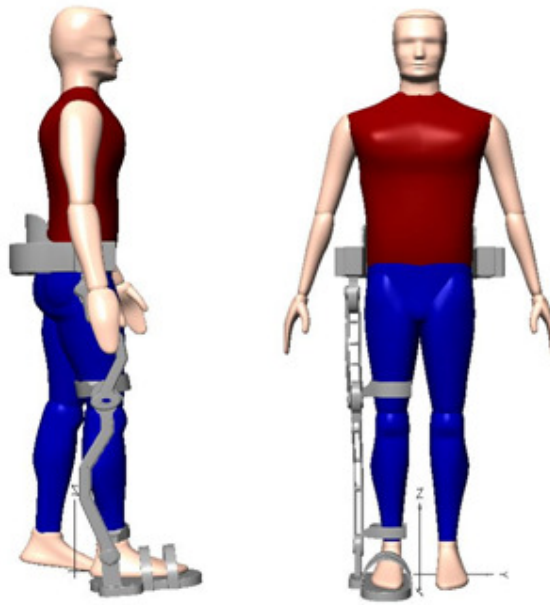
Figure 2. Humanoid and exoskeleton

The mechanical structure of lower limb exoskeleton should follow the characteristics of human lower limb biomechanics such as type of motion, range of motion (RoM), and degree of freedoms (DoF). Table 1 shows the biomechanical properties of human lower limb joints [12], [13]. The exoskeleton joints are controlled according to the biomechanical properties of human lower limb during complete gait cycle to achieve the desired position of each joint.

Table 1. Biomechanical properties of human lower limb joints

Joints	DoF	Motion	RoM(deg)
Hip	1		140 (Flexion)/15 (extension)
Knee	1		120-140 (Flexion)/0-10 (extension)
Ankle	1		40-50 (Flexion)/20 (extension)

3.3. Controller

Human intelligent control system is more advanced than recently developed control systems, therefore it is difficult to design a control system that can match human functions. Furthermore, the level of force generated by human muscles depends on the condition and physical ability of each individual. In case of people with paralysis, muscles may include involuntary strong signals that influence the behaviour of controllers based on biological signals to provide motion support [14]. The control strategy adopted to control the humanoid and exoskeleton is to use predefined trajectory to achieve motion support during walking, based on the trajectory data of human walking provided by clinical gait analysis (CGA) [15].

PD-Fuzzy logic control is considered in this work to control the humanoid and exoskeleton. Fuzzy control is one of the solutions to handle complicated and nonlinear systems when it is difficult to configure an accurate dynamic model, The main advantage of fuzzy systems theory is to approximate system behaviour if the numerical relations of such a system do not exist [16]. Figure 3 shows the fuzzy logic controller. It contains four main blocks: the inputs of the system interpreted in the fuzzification block; the fuzzy-rules block holds information on how to control the system; the appropriate is rule selected and implemented by an interface mechanism block; the fuzzy results are converted into required output signals by the defuzzification block [17].
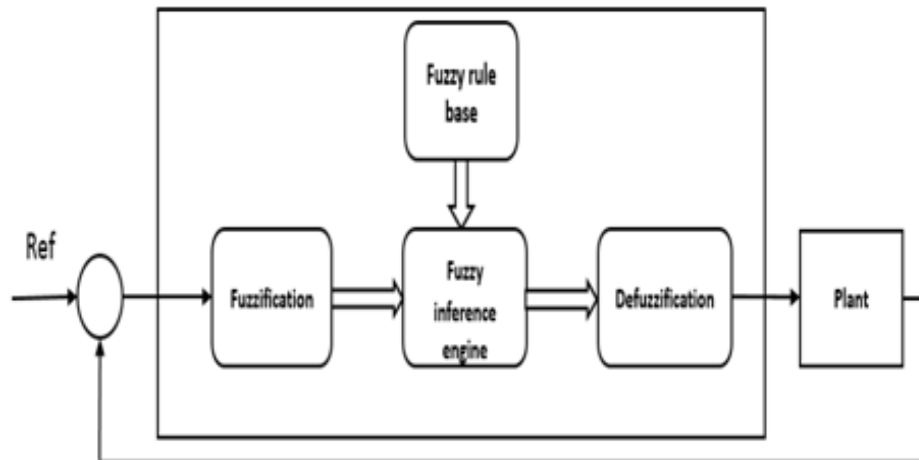
Figure 3. Fuzzy logic control scheme

The fuzzy logic control (FLC) used is based on Mamdani type fuzzy rules with multiple input and single output. The FLC inputs are error (e) and change of error (Δe). Five Gaussian membership functions (MF's) used are shown in Table 2: negative small (NS), negative big (NB), zero (Z), positive small (PS) and positive big (PB). The inputs and outputs defined as a result of 25 rules for each fuzzy controller with 50% overlap between the MF's. Inputs and output are normalised to the range of [-1,+1] as shown in Figure 4. Fuzzy rules are developed to minimise the error and change of error of each input variable.
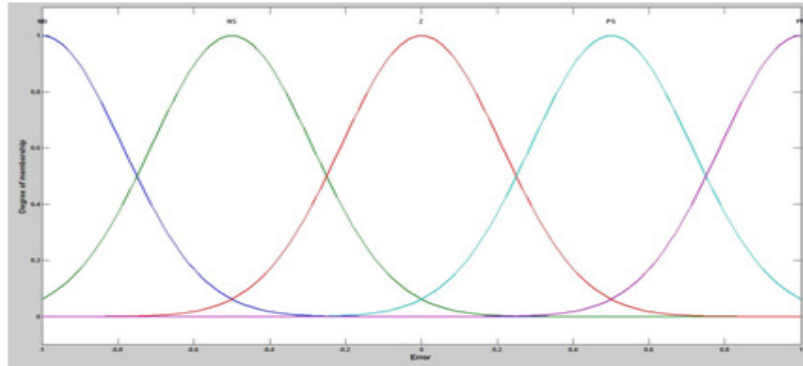
Figure 4. Gaussian membership functions

Table 2. Fuzzy rules

e/Δe	NS	NB	Z	PS	PB
NS	PB	PB	PS	Z	NS
NB	PB	PB	PB	PS	Z
Z	PS	PB	Z	NS	NB
PS	Z	PS	NS	NB	NB
PB	NS	Z	NB	NB	NB
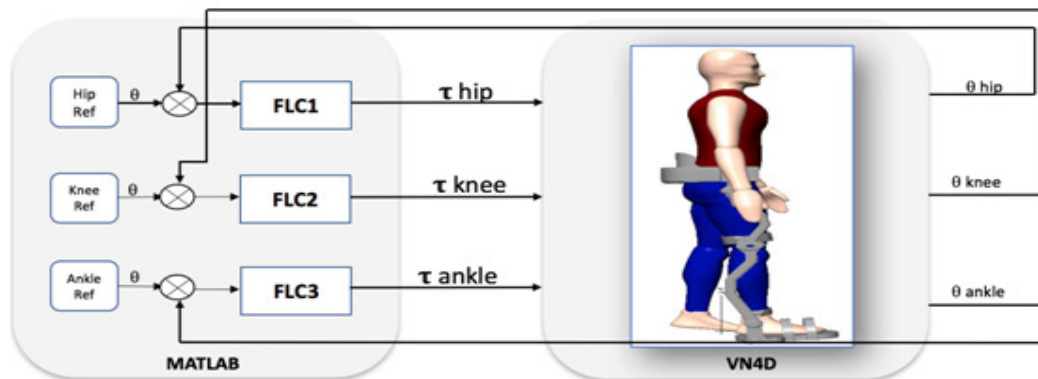
Figure 5. Control system structure

Figure 5 shows the control structure for the exoskeleton and humanoid developed in MATLAB Simulink. The VN4D environment is linked with the controller by adding VN plant from the Simulink library. Three PD-Fuzzy logic controllers shown in Figure 6 (FLC1, FLC2 and FLC3) are used to regulate the input torque (τ) of the right lower limb joints hip, knee and ankle of the humanoid and exoskeleton respectively. The output is formed as orientation (degree) which represents the actual position of each joint, the output is fed back and compared with the reference to determine the error between the actual and the desired position.

The aim of this study is to provide the desired external support by using lower extremity exoskeleton on the affected side to restore natural gait in hemiplegia. Woolley [1] has reported that hemiplegic patients require more metabolic energy cost by 50% to 67% compared to normal human while walking at the same speed. A comparison between the torque profiles of hemiplegia and normal human gait cycle of GCA data case was obtained in previous work presented in [3]. The comparison shows that in the hemiplegic case, the torque is on average 25% to 30% below

that of normal human while walking. Consequently, it was assumed that the exoskeleton will provide the hemiplegia patient with 30% of the torque as compensation to restore the gait and the additional 70% is the natural torque generated by the patient. Based on this assumption, the output torque of the controller was divided between the humanoid and exoskeleton as shown in Figure 6.
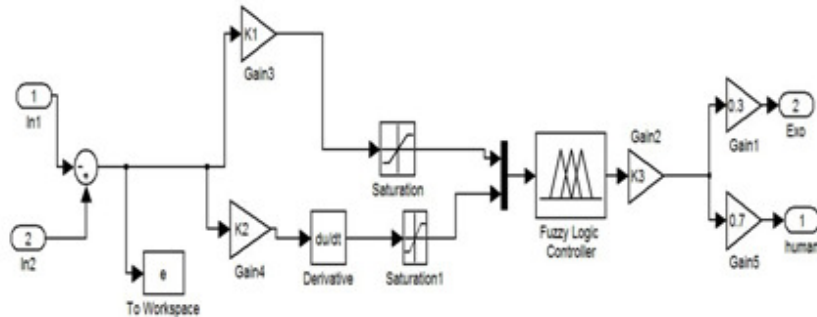
Figure 6. Fuzzy logic controller block (FLC)

4. SIMULATION RESULTS

The simulation results shown in Figures 7, 8 and 9 represent the trajectory tracking of humanoid and exoskeleton right joints. Since the left leg of the humanoid is considered as normal, orientation reference is provided to actuate each joint from the left leg to achieve symmetric walking cycle during simulation. The output of each controller represents the orientation of the exoskeleton and humanoid joints during two gait cycles. Figure 7 shows the trajectory tracking of the hip joint position according to the reference and the error during the simulation. It is noted that the PD-Fuzzy controller was able to minimise the error during two gait cycles and achieve smooth tracking. The knee tracking trajectory in Figure 8, shows that the position of humanoid and exoskeleton deviated from the reference at the highest point of the orientation (swing phase of the gait cycle), due to coupling between the humanoid and exoskeleton. Figure 9 shows the trajectory tracking of the ankle joints. It is noted that the ankle joint had more fluctuation and deviation from the reference. The humanoid and exoskeleton feet were not coupled as well as compared to other parts, due to the design mechanism between the exoskeleton foot and the humanoid foot as seen in Figure 2. Therefore, more investigation is needed to enhance the coupling mechanism between the exoskeleton and the humanoid foot.
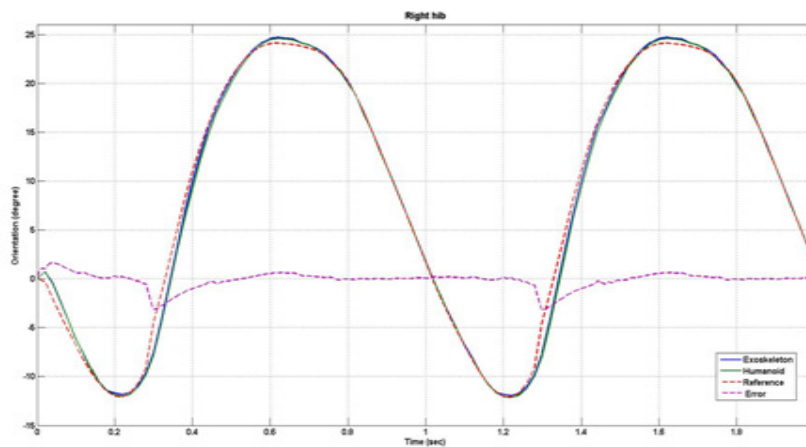
Figure 7. Right hip trajectory tracking
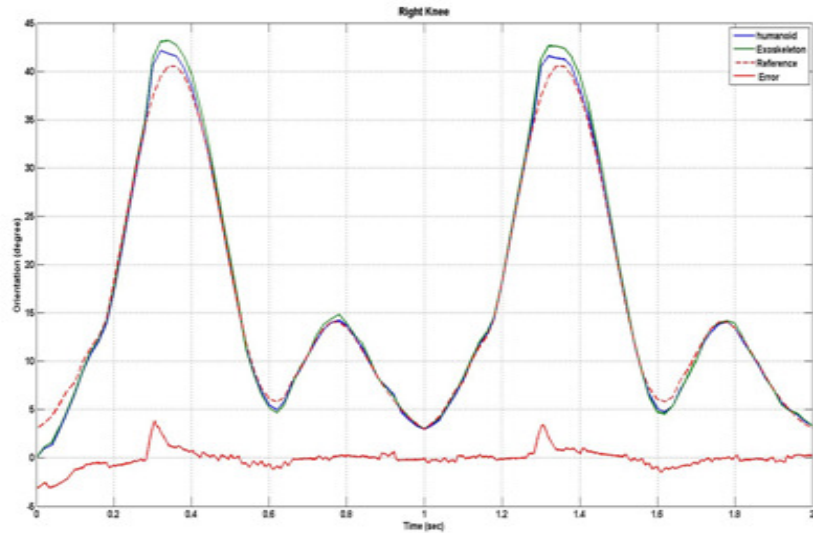
Figure 8. Right knee trajectory tracking
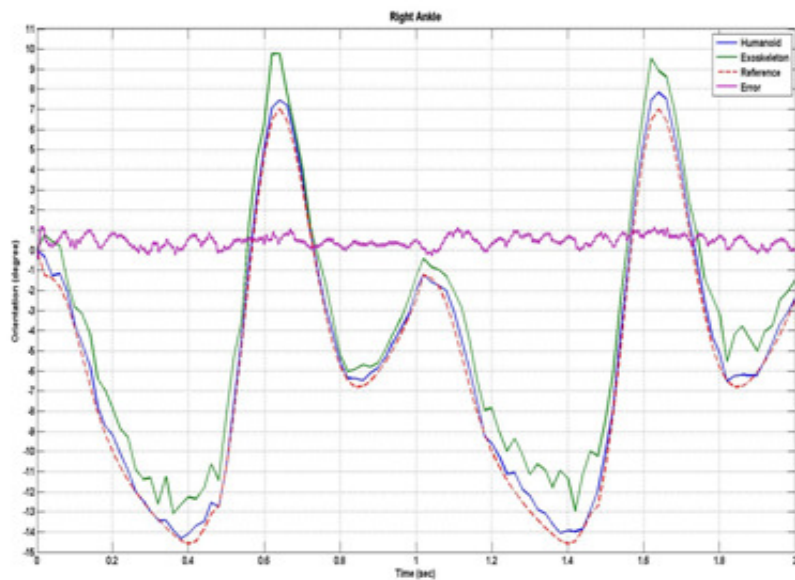
Figure 9. Right ankle trajectory tracking

The investigation carried out constitutes an initial attempt to control the humanoid and exoskeleton to achieve the required support to complete level walking for hemiplegia patient. As noted in the simulation results, the reference signals were not well tracked at some stages of the gait cycle due to the interaction forces generated from the coupled exoskeleton device and humanoid limb. Moreover, the complexity of the system impacted on the response and tracking behaviour during simulation. Therefore, more investigation of the controller approach will be carried out to achieve more robust and stable system performance. The stability of the system will be examined during different locomotion scenarios, such as walking, standing and sitting down. System stability will be examined by applying disturbance forces on humanoid body and the exoskeleton device and the system performance thus achieved will be assessed.

5. CONCLUSIONS

The design and simulation of single leg exoskeleton to support hemiplegia mobility has been presented. The exoskeleton system has been designed to provide 30% of normal leg torque to augment the available 70% leg torque and to naturalise the gait of hemiplegic patient. This has been achieved with PD-Fuzzy control mechanism for the hip, knee and ankle joints. Further investigation will look into enhancing the controller and the exoskeleton design in respect of material, fitting and actuation options.

REFERENCES

[1] S. M. Woolley, "Characteristics of gait in hemiplegia.," Top. Stroke Rehabil., vol. 7, no. 4, pp. 1–18, 2001.

[2] world health organization, "Spinal cord injury," Fact sheet N°384, 2013. [Online]. Available: http://www.who.int/mediacentre/factsheets/fs384/en/.

[3] A. Alshatti, M. O. Tokhi, and G. Alrezage, "Design and control of single leg exoskeleton for hemiplegia mobility," in Advances in Cooperative Robotics : Proceedings of the 19th International Conference on CLAWAR 2016, 2016, pp. 832–839.

[4] V. Grosu, C. R. Guerrero, B. Brackx, S. Grosu, B. Vanderborght, and D. Lefeber, "Instrumenting Complex Exoskeletons for Improved Human-Robot Interaction," Instrumentation & Measurement Magazine, IEEE, no. October, pp. 5–10, 2015.

[5] C.-J. Yang, J.-F. Zhang, Y. Chen, Y.-M. Dong, and Y. Zhang, "A review of exoskeleton-type systems and their key technologies," Proc. Inst. Mech. Eng. Part C J. Mech. Eng. Sci., vol. 222, no. 8, pp. 1599–1612, 2008.

[6] A. M. Dollar and H. Herr, "Lower extremity exoskeletons and active orthoses: Challenges and state-of-the-art," IEEE Trans. Robot., vol. 24, no. 1, pp. 144–158, 2008.

[7] A. B. Zoss, H. Kazerooni, and A. Chu, "Biomechanical Design of the Berkeley Lower Extremity Exoskeletong (BLEEX)," IEEE/ASME Trans. Mechatronics, vol. 11, no. 2, pp. 128–138, 2006.

[8] K. a. Strausser and H. Kazerooni, "The development and testing of a human machine interface for a mobile medical exoskeleton," 2011 IEEE/RSJ Int. Conf. Intell. Robot. Syst., pp. 4911–4916, 2011.

[9] Y. Sankai, "HAL: Hybrid assistive limb based on cybernics," Springer Tracts Adv. Robot., vol. 66, no. STAR, pp. 25–34, 2010.

[10] S. Viteckova, P. Kutilek, and M. Jirina, "Wearable lower limb robotics: A review," Biocybern. Biomed. Eng., vol. 33, no. 2, pp. 96–105, 2013.

[11] D. A. Winter, Biomechanics and motor control of human movement. Hoboken, N.J. : Wiley, c2009, 2009.

[12] K. H. Low, "Robot-assisted gait rehabilitation: From exoskeletons to gait systems," in Defense Science Research Conference and Expo (DSR), 2011, 2011, pp. 1–10.

[13] B. MACKENZIE, "Range of Movement (ROM)," 2004. [Online]. Available:
http://www.brianmac.co.uk/musrom.htm. [Accessed: 21-Apr-2016].

[14] H. Kawamoto, T. Hayashi, T. Sakurai, K. Eguchi, and Y. Sankai, "Development of single leg version of HAL for hemiplegia," Conf Proc IEEE Eng Med Biol Soc, vol. 2009, 2009.

[15] M. A. Kranzl and D. A. Kopf, "65 year old man with hemiplegia, right side," 1997. [Online]. Available: http://www.clinicalgaitanalysis.com.

[16] K. M. Passino and S. Yurkovich, Fuzzy Control. California: Addison Wesley Longman, Inc, 1998.

[17] T. J. Ross, Fuzzy Logic with Engineering Applications, 3rd ed. John Wiley & Sons, 2009.

Experiments on Different Recurrent Neural Networks for English-Hindi Machine Translation

Ruchit Agrawal[1] and Dipti Misra Sharma[2]

[1]Language Technologies Research Center, IIIT Hyderabad
[2]Head, Language Technologies Research Center, IIIT Hyderabad

ABSTRACT

Recurrent Neural Networks are a type of Artificial Neural Networks which are adept at dealing with problems which have a temporal aspect to them. These networks exhibit dynamic properties due to their recurrent connections. Most of the advances in deep learning employ some form of Recurrent Neural Networks for their model architecture. RNN's have proven to be an effective technique in applications like computer vision and natural language processing. In this paper, we demonstrate the effectiveness of RNNs for the task of English to Hindi Machine Translation. We perform experiments using different neural network architectures - employing Gated Recurrent Units, Long Short Term Memory Units and Attention Mechanism and report the results for each architecture. Our results show a substantial increase in translation quality over Rule-Based and Statistical Machine Translation approaches.

KEYWORDS

Machine Translation, Recurrent Neural Networks, LSTMs, GRUs, English-Hindi MT.

1. INTRODUCTION

Deep learning is a rapidly advancing approach to machine learning and has shown promising performance when applied to a variety of tasks like image recognition, speech processing, natural language processing, cognitive modelling and so on. Deep Learning involves using large neural networks for training a model for a specific task. This paper demonstrates the application of deep learning for Machine Translation of English ! Hindi, two linguistically distant and widely spoken languages. The application of deep neural networks to Machine Translation has been demonstrated by (Kalchbrenner and Blunsom, 2013; Sutskever et al., 2014; Cho et al., 2014; Bahdanau et al., 2014) and it has shown promising results for various language pairs.

In this paper, we experiment with different deep learning architectures. These include Gated Recurrent Units (GRUs), Long Short Term Memory Units (LSTMs) and addition of attention mechanism to each of these architectures. We demonstrate that the best performance for English - > Hindi MT is generally obtained using Bi-directional LSTMs with attention mechanism and in

some cases with GRUs with attention mechanism. The Bi-directional LSTMs generally show better performance for compound sentences and larger context windows.

We show manual samples of output translations and provide their evaluation to demonstrate the effectiveness of different architectures.

We describe the motivation behind the choice of RNNs in detail in Section 3. We briefly discuss related work in Section 2, followed by the description of our neural network model in Section 4. The experiments and results are discussed in Section 5. The paper is concluded in Section 6.

2. RELATED WORK

The usage of large neural networks for Natural Language Processing (NLP) tasks was initially proposed by (LeCun et al., 2015) in his feed-forward neural language model. The neural Language Model he proposed is very similar to the current existing Language Models.

The input n-gram is projected into an embedding space for each word and passes to big output layer.
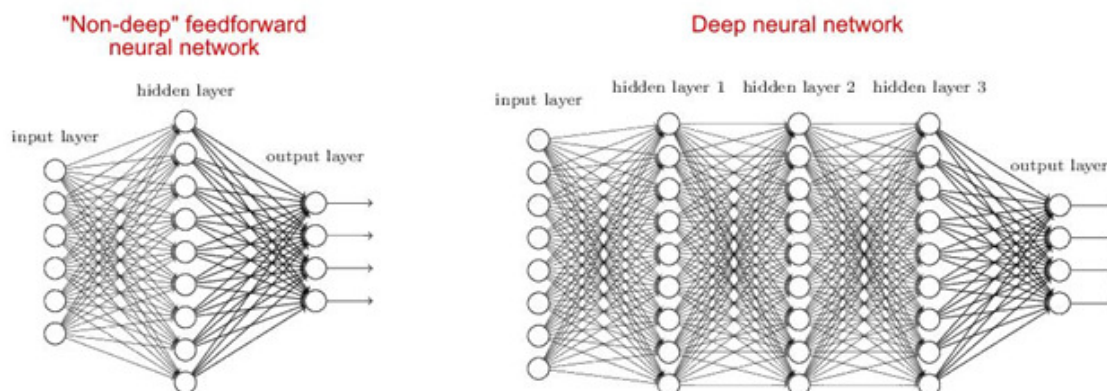
Figure 1: *A comparison of feedforward neural networks with Recurrent Neural Networks*

This novel idea was then used by several researchers who tried to integrate it with Machine Translation systems ((Auli et al., 2013) and (Cho et al., 2014)).

(Sutskever et al., 2014) was a breakthrough for Machine Translation, introducing the "seq2seq" (Sequence to sequence) model which was the first model based completely on neural networks and achieving accuracy comparable to the State-of-the-Art SMT systems. They proposed the usage of a Recurrent Neural Network model with the encoders and decoders comprising of LSTMs or GRUs. They propose running the encoder over the source sentence, producing a hidden state and then running another RNN (decoder) to generate the output one word at a time.

The bottleneck to this approach was that the entire translation is a fixed sized vector. There have been different techniques (like padding) to rectify this issue.

Anusaaraka (Bharati et al., 1994) is an English to Hindi Machine Translation, primarily Rule-based, but employing a parser which uses statistical approaches (De Marneffe et al., 2006).
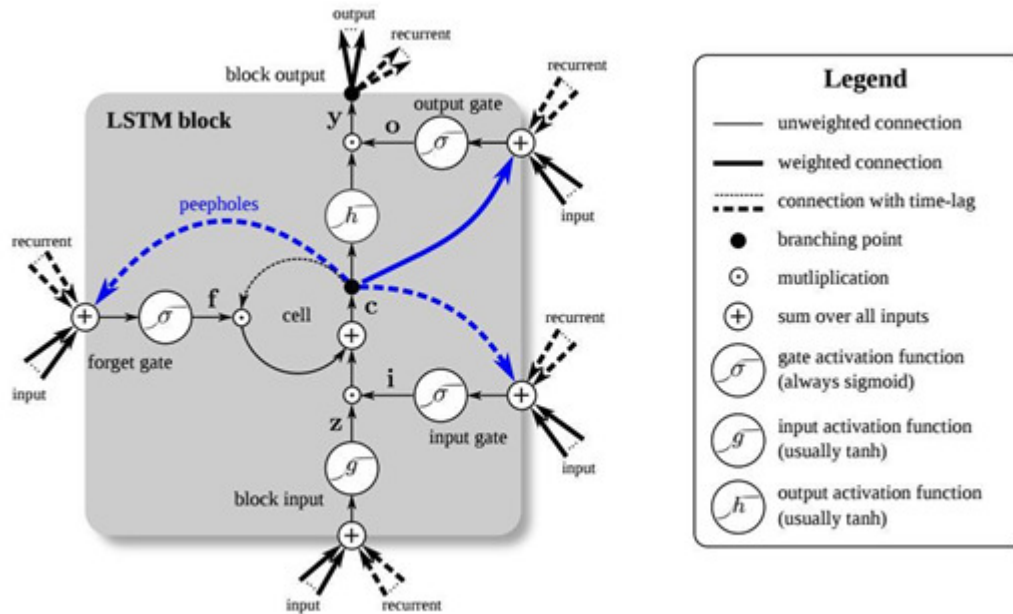
Figure 2: Structure of an LSTM unit

3. MOTIVATION BEHIND USING RECURRENT NEURAL NETWORKS

Traditional Neural Networks have a huge RAM requirement and are not quite feasible in their best settings where they achieve their highest accuracies. Additionally, they are not designed to deal with sequential information. We explain this below :

One important property of machine translation, or any task based on natural languages, is that we deal with variable-length input and output. For example; if the input X=(x_1; x_2; : : : ; x_T) and output Y=(y_1; y_2; : : : ; y_T '); The lengths of the sequences i.e. T and T' are not fixed.

On the other hand, one of the major assumptions in feedforward neural networks is the idea of fixed length, i.e. the size of the input layer is fixed to the length of the input sequence. The other major assumption is the idea of independence - that different training examples (like images) are independent of each other. However, we know of temporal sequences such as sentences or speech, there are short and long temporal dependencies that have to be accounted for.

To deal with these types of variable-length input and output, we need to use a recurrent neural network (RNN). Widely used feed-forward neural networks, such as convolutional neural networks, do not maintain internal state other than the network's own parameters. Whenever a single sample is fed into a feed-forward neural network, the network's internal state, or the activations of the hidden units, is computed from scratch and is not influenced by the state computed from the previous sample. On the other hand, an RNN maintains its internal state while reading a sequence of inputs, which in our case will be a sequence of words, thereby being able to process an input of any length.

Recurrent Neural Networks (RNNs) also address the independence issue - they facilitate the preservation as well as processing of information that has a temporal aspect involved. For example; a sequence of words has an order, and hence a time element inherent in it. A model which takes this into consideration is needed for efficient performance. This is not possible if we employ feed-forward neural networks. Thus, Recurrent Neural Networks can not only learn the local and long term temporal dependencies in the data, but can also accommodate input sequences of variable length.

The RNN's thus help in converting the input sequence to a fixed size feature vector that encodes primarily the information which is crucial for translation from the input sentence, and ignores the irrelevant information. Figure 1 shows a comparison of feed-forward neural networks with recurrent neural networks.

Long Short Term Memory (LSTM) units are a type of RNNs which are very good at preserving information through time-steps over a period of time. Figure 2 shows the structure of an LSTM unit. One key advance in LSTMs in recent years has been the concept of bi-directional encoder and decoder framework. When we employ bidirectional LSTMs, we end up with two hidden states - one in the forward direction and one in the backward direction. This allows the network to learn from the text. Often, even more than two layers are used. Thus there will be multiple layers stacked on top of each other - this is generally only in huge training data conditions. Each one of these has a set of weights inside it, and learns and affects the one above it. The final state represents everything that is in the source words. Bi-directional LSTMs generally work the best specially when complemented with the attention mechanism.

After the encoding process, we are left with a context vector - which is like a snapshot of the entire source sequence and is used further to predict the output. We have a dense layer with softmax similar to a feed-forward neural network, but the difference is that it is time distributed i.e. we have one of these for each time step. The top layer thus has one neuron for every single word in the vocabulary and hence is huge in size in large vocabulary conditions.
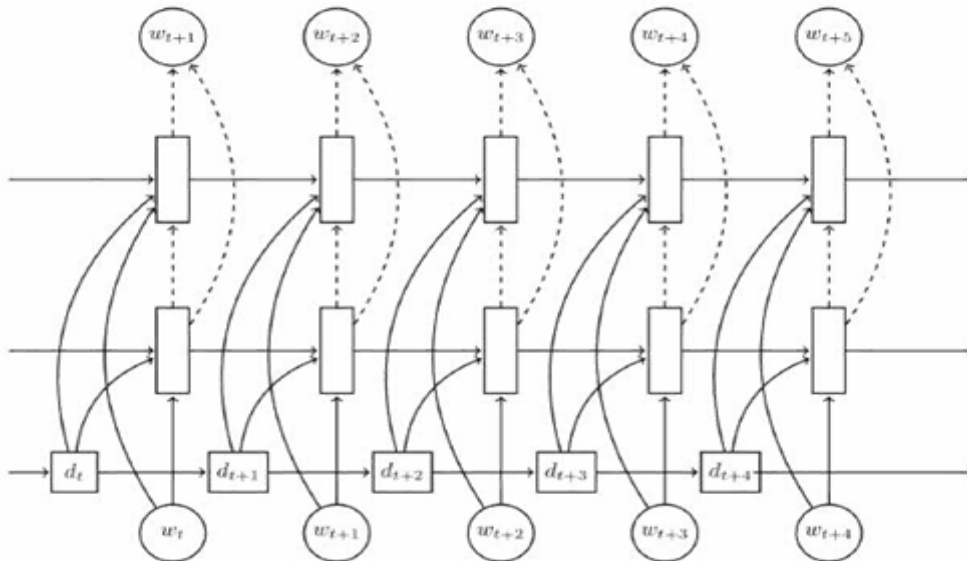
Figure 3: A two-layered LSTM architecture which we employ in our experiments

4. FORMULATION OF OUR MODEL

In order to train the recurrent neural networks, we take the cost function and obtain its derivative with respect to the weight in question. We then move this derivative through the nested layer of computations using the chain rule.

In other words, the output of the previous layer is multiplied by the weight matrix and added to a bias and then passed on to an activation function.

$$y_k = g(W\,\mathbf{y}_{k\ 1} + \mathbf{b}) \tag{1}$$

Table 1: Different Hindi translations corresponding to the English sentence - "Shyam has given the book to Manish." (Due to word order)

	Hindi	Transliteration
Sent : 1	मनीष को श्याम ने किताब दे दी ।	manIRa ko SyAma ne kiwAba xe xI
Sent : 2	श्याम ने मनीष को किताब दे दी ।	SyAma ne manIRa ko kiwAba xe xI

Table 2: Anusaaraka scores on ILCI test data

BLEU	NIST	METEOR	RIBES
6.98	3.68	0.164	0.592

We use a recurrent connection convert the linear unit of feed-forward neural network to a recurrent unit so that now the activity of the unit h_t not only depends on x_t (the input) multiplied by the weight matrix, but also on its activity at the previous timestep. The following equation shows this phenomenon :

$$h^{(t)} = g_h(W_1 x^{(t)} + W_R h^{(t\ 1)} + b_h) \tag{2}$$

Table 3: Two different translations corresponding to the same English sentence - from ILCI test data (Many-to-many mapping between vocabulary)

Test	ताजा साँसेंऔर चमचमाते दाँत आपके व्यिक्त्व को निखारतैं। ह
T l	wAjA sAzseM Ora camacamAwe xAzwa Apake vyakwiwva ko niKArawe hEM
T s	Fresh breath and shining teeth enhance your personality .
LST M	ताजी साँस और चमकदार दाँत आपके व्यिक्त्वंचारम चाँद लगातैं ह
T s	wAjI sAzsa Ora camakaxAra xAzwa Apake vyakwiwva meM cAra cAzxa lagAwe hEM
T l	Fresh breath and shining teeth enhance your personality.

T l : Transliteration, T s : Translation, LST M : Long Short Term Memory, T est : Sentence from ILCI Test data

Table 4: Results - Comparison of metric scores obtained on two-layered and four-layered model at different stages

	Two Layers				Four Layers			
	BLEU	NIST	METEOR	RIBES	BLEU	NIST	METEOR	RIBES
Anusaaraka	6.61	2.51	0.156	0.592	6.72	3.33	0.158	0.567
GRU	15.19	4.45	0.149	0.727	16.41	2.82	0.149	0.64
LST M	15.32	4.42	0.21	0.74	16.85	4.48	0.16	0.69
BiLST M	15.39	4.31	0.228	0.73	17.31	4.62	0.23	0.763
GRU$_{Att}$	16.06	5.37	0.239	0.758	17.45	5.21	0.244	0.775
LST M$_{Att}$	16.76	5.43	0.246	0.760	17.63	5.49	0.251	0.788
BiLST M$_{Att}$	17.91	5.47	0.251	0.78	18.41	5.57	0.274	0.81

GRU : Gated Recurrent Unit
Anusaaraka :Rule-based Machine Translation for English-Hindi
LST M : Long Short Term Memory
Att : Attention Mechanism
BiLST M : Bi-directional LSTM
We use similar nomenclature in all tables hereby.

The second term $W_R h^{(t\ 1)}$ depends on the activity at the previous timestep multiplied by a recurrent weight matrix. We also want to be able to retrieve an output from this unit and this is done by adding a linear operation as described in the following equation :

$$y^{(t)} = g_y(W_y h^{(t)} + b_y) \tag{3}$$

Here, $y^{(t)}$ is a function of $h^{(t)}$ multiplied by weight matrix w and passed through a non-linear activation function. This is the basic element of the recurrent neuron which we use in our RNN architectures.

The process can be visualized as the input sequence being compressed by the RNN into an intermediate representation in the form of a fixed dimensional vector. So, if the vector $h_{t\ 1}$ describes the history of the sequence at timestep t, the new internal state (the updated vector) h_t will be computed by the network, effectively compressing the preceding symbols ($x_1; x_2; : : : ; x_t$ $_1$) as well as the new symbol x_t. The following equation shows this :

$$h_t = \phi\ (x_t, h_{t\ 1})$$

Here, ϕ is a function which takes the new information unit x_t and the hidden state $h_{t\ 1}$ as input. (h_0 can be assumed to be a vector containing zeroes).

Table 5: Evaluating output quality : Different RNN architectures

T est	इसका उपचार सभी अस्पताल मेंहै।
T l	isakA upacAra saBI aspawAloM meM hE
T s	Its treatment is available in all hospitals.
Anusaaraka	इसके लिए अब उपलब्ध भी एक गोली है।
T l	isake lie aba upalabXa BI eka golI hE
T s	For this, there is now available also a pill.
GRU	इसका निदान सभी सभी अस्पताल मेंउपलब्ध है।
T l	isakA nixAna saBI saBI aspawAloM meM upalabXa hE
T s	The solution for this is available in all all hospitals.
LST M	उसका इलाज सभी अस्पताल मेंउपलब्ध है।
T s	usakA ilAja saBI aspawAloM meM upalabXa hE
T l	The treatment for that is available in all hospitals.
BiLST M	इसका उपचार सभी अस्पताल मेंउपलब्ध है।
T l	isakA upacAra saBI aspawAloM meM upalabXa hE
T s	The treatment for this is available in all hospitals.

Comparing the performance of different neural network architectures (without attention mechanism)

Table 6: Evaluating output quality : Adding Attention Mechanism

GRU_{Att}	अपनी रोज क दिनचयाव्यायामें को ज र शिमल करें।
T l	apanI roja kI xinacaryA meM vyAyAma ko jarUra SAmila kareM
T s	Do include exercise in your daily routine.
$LST M_{Att}$	एक्सरसाइज को अपने निकैद दिनचयाशिमलें करें।
T l	eksarasAija (transliteration) ko apane xEnika xinacaryA meM SAmila kareM
T s	Include exercise in your everyday routine.
$BiLST M_{Att}$	व्यायाम को अपनी दिनकै दिनचयाशिमलें करें।
T l	vyAyAma (translation) ko apanI xEnika xinacaryA meM SAmila kareM
T s	Include exercise in your everyday routine.

5. EXPERIMENTS AND RESULTS

We employ a sequence-to-sequence model with Recurrent Neural Networks to train our models. We conduct experiments on two and four layers of encoder and decoder respectively. We use the architecture as described in Section 4. We use the seq2seq model available in Tensorflow[1] to implement the above mentioned architecture.

For training the model, we extract 200,000 sentences from the HindEnCorp (Bojar et al., 2014) corpus. We employed pruning using appropriate rules to remove unsuitable sentences. For

----
[1]It can be accessed at : https://github.com/google/seq2seq

example, all sentences of length greater than fifty were removed from the corpus. The reason was low scalability of neural networks to translate sentences of length greater than 50. Also, sentences of length less than three were removed to discourage memorization, instead of syntactic and semantic learning of concepts. Pruning was also done to remove special characters and hyperlinks from the sentences.

After removing discrepancies, rest of the sentences were randomly shuffled to create the parallel training corpus. We test the performance of our model using the ILCI test set (Jha, 2010) and the WMT 2014 English-Hindi test set.

We observe that our model is able to produce grammatically fluent translations, as opposed to traditional approaches. Some problems which still need to be solved are presence of repeated tokens and unknown or unmapped words. A bi-directional LSTM model with attention mechanism shows improvement over normal RNN's in both these aspects.

Table 7: Evaluating output quality : Two layers vs. Four layers

$Test$	40 साल से अधिक आयुके सभी व्यिक्य के विषर्कजाँच अवश्य की जानी चिहए ।
Tl	40 sAla se aXika Ayu ke saBI vyakwiyoM kI vArRika jAzca avaSya kI jAnI cAhie
Ts	An annual check-up of everybody above the age of 40 years must be done .
$LSTM_{2l}$	40 वष क उमर् के ऊपर पत्र्येक व्यिक क विषर्कजाँच करनी होगी ।
Tl	40 varRoM kI umra ke Upara prawyeka vyakwi kI vArRika jAzca karanI hogI
Ts	An annual checkup of each person above 40 years of age will have to be done.
$LSTM_{4l}$	40 वष क उमर् के ऊपर पत्र्येक व्यिक का विषर्कजाँच किया जाना चिहए ।
Tl	40 varRoM kI umra ke Upara prawyeka vyakwi kA vArRika jAzca kiyA jAnA cAhie
Ts	An annual check-up of each person above 40 years of age should be done.
$BiLSTM_{2l}$	40 वर्षक उमर् से अधिक पत्र्येक व्यिक क विषर्कजांच िनश्चत प से की जानी चिहए ।
Tl	40 varRa kI umra ke Upara hara sAla vArRika jAzca karanI cAhie
Ts	After 40 years of age, every year an annual checkup should be done.
$BiLSTM_{4l}$	40 वर्षक उमर् से अधिक पत्र्येक व्यिक क विषर्कटेस्ट करनी चिहए ।
Tl	40 varRa kI umra ke prawi hara eka vArRika testa karanI cAhie
Ts	After 40 years of age, every one annual test should be done.

Table 8: Results on WMT Test data

	BLEU	NIST	METEOR	RIBES
GRU	1.57	1.46	0.0738	0.277
$Anusaaraka$	4.40	2.72	0.12	0.488
$LSTM$	6.57	2.89	0.163	0.611
$BiLSTM$	8.42	3.26	0.198	0.67
$BiLSTM_{Att}$	9.23	3.67	0.211	0.71

Performance evaluation on WMT test set

Table 4 demonstrates the performance of our model during various stages as measured by the above-mentioned metrics. We observe on manual inspection of samples that there is a significant improvement in performance over rule-based and statistical approaches by using deep neural networks, thereby producing quality translation as shown by the use of semantically correct synonyms. For example, Table 3 shows a sample sentence from the ILCI test corpus ($ILCI_{\text{test}}$) and its corresponding output obtained by our model. The English as well as Hindi meaning of both the sentences is the same, although they differ in their structure and words used in the Hindi output. The LSTM output displays an impressive usage of the phrase "cAra cAzxa lagAwe hEM" - a contextually suitable and semantically correct idiom in Hindi which conveys "enhancing of personality".

Anusaaraka has a BLEU score of 6:98 on ILCI test data (Table 2). We observe a 4:72 point increase in the BLEU score by using GRUs. Similar improvements can be seen for other metrics by using different RNN architectures. Table 5 shows the variation in quality of translation obtained on using different RNN architectures. The Anusaaraka output does not make much sense (is syntactically as well as semantically poor) and the GRU a grammatically incorrect sentence. While the LSTM model produces a better translation with a minor error in pronoun usage, the Bi-directional LSTM model generates the correct output.

We demonstrate the effect of addition of attention mechanism in Table 6. Table 7 compares the output of two-layered model and four-layered model obtained on the different architectures using sample translations. We can observe that the four-layered model is able to perform better in many cases two-layered counterpart. The reason can be attributed to higher complexity of this model and sufficient data for training.

We also conduct experiments and report results on the WMT-14 corpus in Table 8. The results further improve on using Bi-directional LSTM with attention to give a BLEU score of 9.23, comparable to (Dungarwal et al., 2014), a system fully trained on the WMT training corpus.

6. CONCLUSION AND FUTURE WORK

In this paper, we build sequence-to-sequence models using Recurrent Neural Networks. We experimented with Gated Recurrent Units, Long Short Term Memory Units and the attention mechanism. We demonstrated results using this approach on a linguistically distant language pair En ! Hi and showed a substantial improvement in translation quality. We conclude that Recurrent Neural Networks perform well for the task of English-Hindi Machine Translation. The bi-directional LSTM units perform best, specially on compound sentences. Future work includes performing experiments on other languages, specially among morphologically rich languages, like Indian to Indian language MT. We would like to explore MT for resource-scarce languages, in conditions where large parallel corpora for training are not available.

REFERENCES

[1]   Gary Anthes. 2010. Automated translation of indian languages. Communications of the ACM 53(1):24– 26.

[2]   Michael Auli, Michel Galley, Chris Quirk, and Geoffrey Zweig. 2013. Joint language and translation modeling with recurrent neural networks. In EMNLP . volume 3, page 0.

[3] Akshar Bharati, Vineet Chaitanya, and Rajeev Sangal. 1994. Anusaraka or language accessor: A short introduction. Automatic Translation, Thiruvananthpuram, Int. school of Dravidian Linguistics .

[4] Akshar Bharati, Vineet Chaitanya, Rajeev Sangal, and KV Ramakrishnamacharyulu. 1995. Natural language processing: a Paninian perspective . Prentice-Hall of India New Delhi.

[5] Roger M Blench and M Post. Rethinking sino-tibetan phylogeny from the perspective of north east indian languages. paper accepted for a volume of selected papers from the 16th himalayan languages symposium 2-5 september 2010 school of oriental and african studies, london. ed. Nathan Hill. Mouton de Gruyter .

[6] Ondrej Bojar, Vojtech Diatka, Pavel Rychlỳ, Pavel Stranák, Vít Suchomel, Ales Tamchyna, and Daniel Zeman. 2014. Hindencorp-hindi-english and hindi-only corpus for machine translation. In LREC . pages 3550–3555.

[7] Kyunghyun Cho, Bart Van Merriënboer, Caglar Gulcehre, Dzmitry Bahdanau, Fethi Bougares, Holger Schwenk, and Yoshua Bengio. 2014. Learning phrase representations using rnn encoder-decoder for statistical machine translation. arXiv preprint arXiv:1406.1078 .

[8] Junyoung Chung, Caglar Gülçehre, Kyunghyun Cho, and Yoshua Bengio. 2015. Gated feedback recurrent neural networks. In ICML . pages 2067–2075.

[9] Marie-Catherine De Marneffe, Bill MacCartney, Christopher D Manning, et al. 2006. Generating typed dependency parses from phrase structure parses. In Proceedings of LREC . Genoa Italy, volume 6, pages 449–454.

[10] George Doddington. 2002. Automatic evaluation of machine translation quality using n-gram co-occurrence statistics. In Proceedings of the second international conference on Human Language Technology Research . Morgan Kaufmann Publishers Inc., pages 138–145.

[11] Piyush Dungarwal, Rajen Chatterjee, Abhijit Mishra, Anoop Kunchukuttan, Ritesh Shah, and Pushpak Bhattacharyya. 2014. The iit bombay hindi english translation system at wmt 2014. ACL 2014 page 90.

[12] Aria Haghighi and Dan Klein. 2009. Simple coreference resolution with rich syntactic and semantic features. In Proceedings of the 2009 Conference on Empirical Methods in Natural Language Processing: Volume 3-Volume 3 . Association for Computational Linguistics, pages 1152–1161.

[13] Hideki Isozaki, Tsutomu Hirao, Kevin Duh, Katsuhito Sudoh, and Hajime Tsukada. 2010. Automatic evaluation of translation quality for distant language pairs. In Proceedings of the 2010 Conference on Empirical Methods in Natural Language Processing . Association for Computational Linguistics, pages 944–952.

[14] Girish Nath Jha. 2010. The tdil program and the indian langauge corpora intitiative (ilci). In LREC .

[15] Nal Kalchbrenner and Phil Blunsom. 2013. Recurrent continuous translation models. In EMNLP . 39, page 413.

[16] Nayan Jyoti Kalita and Baharul Islam. 2015. Bengali to assamese statistical machine translation using moses (corpus based). arXiv preprint arXiv:1504.01182 .

[17] Philipp Koehn, Hieu Hoang, Alexandra Birch, Chris Callison-Burch, Marcello Federico, Nicola Bertoldi, Brooke Cowan, Wade Shen, Christine Moran, Richard Zens, et al. 2007. Moses: Open source toolkit for statistical machine translation. In Proceedings of the 45th annual meeting of the ACL on interactive poster and demonstration sessions . Association for Computational Linguistics, pages 177–180.

[18] Alon Lavie and Michael J Denkowski. 2009. The meteor metric for automatic evaluation of machine translation. Machine translation 23(2):105–115.

[19] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton. 2015. Deep learning. Nature 521(7553):436–444.

[20] Minh-Thang Luong and Christopher D Manning. 2015. Stanford neural machine translation systems for spoken language domains. In Proceedings of the International Workshop on Spoken Language Translation .

[21] Minh-Thang Luong, Hieu Pham, and Christopher D Manning. 2015. Effective approaches to attention-based neural machine translation. arXiv preprint arXiv:1508.04025 .

[22] Anthony McEnery, Paul Baker, Rob Gaizauskas, and Hamish Cunningham. 2000. Emille: Building a corpus of south asian languages. VIVEK-BOMBAY- 13(3):22–28.

[23] Kishore Papineni, Salim Roukos, Todd Ward, and Wei-Jing Zhu. 2002. Bleu: a method for automatic evaluation of machine translation. In Proceedings of the 40th annual meeting on association for computational linguistics . Association for Computational Linguistics, pages 311–318.

[24] Reinhard Rapp and Carlos Martin Vide. 2006. Example-based machine translation using a dictionary of word pairs. In Proceedings, LREC . pages 1268–1273.

[25] Alexander J Ratner, Christopher M De Sa, Sen Wu, Daniel Selsam, and Christopher Ré. 2016. Data programming creating large training sets, quickly. In Advances in Neural Information Processing Systems . pages 3567–3575.

[26] Matthew Snover, Bonnie Dorr, Richard Schwartz, Linnea Micciulla, and John Makhoul. 2006. A study of translation edit rate with targeted human annotation. In Proceedings of association for machine translation in the Americas . volume 200.

[27] Martin Sundermeyer, Ralf Schlüter, and Hermann Ney. 2012. Lstm neural networks for language mod-eling. In Interspeech . pages 194–197.

[28] Ilya Sutskever, Oriol Vinyals, and Quoc V Le. 2014. Sequence to sequence learning with neural networks.

[29] In Advances in neural information processing systems . pages 3104–3112.

[30] Nicola Ueffing, Gholamreza Haffari, Anoop Sarkar, et al. 2007. Transductive learning for statistical machine translation. In Annual Meeting-Association for Computational Linguistics . volume 45, page 25.

[31] Paul J Werbos. 1990a. Backpropagation through time: what it does and how to do it. Proceedings of the IEEE 78:1550–1560.

[32] Paul J Werbos. 1990b. Backpropagation through time, what it does and how to do it. Proceedings of the IEEE 78.

[33] David Yarowsky. 1995. Unsupervised word sense disambiguation rivaling supervised methods. In Pro-ceedings of the 33rd annual meeting on Association for Computational Linguistics . Association for Computational Linguistics, pages 189–196.

COMPARING THE CUCKOO ALGORITHM WITH OTHER ALGORITHMS FOR ESTIMATING TWO GLSD PARAMETERS

Jane Jaleel Stephan[1], Haitham Sabah Hasan[2] and Alaa Hamza Omran[3]

[1,2,3] University of Information Technology & Communications, Iraq

ABSTRACT

This study introduces and compares different methods for estimating the two parameters of generalized logarithmic series distribution. These methods are the cuckoo search optimization, maximum likelihood estimation, and method of moments algorithms. All the required derivations and basic steps of each algorithm are explained. The applications for these algorithms are implemented through simulations using different sample sizes (n = 15, 25, 50, 100). Results are compared using the statistical measure mean square error.

KEYWORDS

Cuckoo search optimization (CSO) algorithm, maximum likelihood estimation (MLE) algorithm, method of moments (MOM) algorithm, mean square error (MSE).

1. INTRODUCTION

The process of modifying a system to present several new features that corporate in enhancing the system and work more efficiently is known as optimization process. Also the Optimization process can be defined as the process of finding alternative solution to increase the performance of the system under specific constraints such as increasing the desired parameters and decrease the undesired parameters in the system which has a problem to solve it [1]. The increasing means trying to get additional good results without additional cost such as the optimization which occurs on computer or any android phone will results in increasing the speed of processing which makes them run faster with less memory requirements. There are many algorithms in solving optimization problems such as cukoo search algorithm which introduced for the first time by Yang and Deb [2]. Many researchers work on testing this algorithm on some benchmark functions and compare the results with other algorithms like PSO, GA; the obtained results show that the cukoo algorithm is better than the others. One of the popular met heuristic, combinatorial search optimization techniques is ACO (Ant Colony Optimization) which is developed from natural ant behavior ACO was used along with Rough Sets and Fuzzy Rough Sets in feature selection in [3], [4], [5] also it is used for optimizing of firewall rules in [6]. Today the Cuckoo search algorithm became as the one of the most optimization algorithm which used in every domain like scheduling planning, forecasting, image processing, feature selection and engineering optimization [7]. This paper presents a Comparing of the Cuckoo Algorithm with Other Algorithms for Estimating Two GLSD Parameters. Some important functions are defined as follows:

The discrete random variable (x) exhibits the generalized logarithmic series distribution (GLSD) with two parameters (α and β), where (α) is a scale parameter and (β) is a shape parameter. Let

$$\theta = -\frac{1}{\log(1-\alpha)},$$

Where Θ is a function from α. The positive matrix factorization (p.m.f.) of GLSD is defined by Eq. (1) as follows:

$$p(X = x) = \frac{\theta\,\Gamma(\beta x)\,\alpha^x(1-\alpha)^{\beta x - x}}{x!\,\Gamma(\beta x - x + 1)}, \tag{1}$$

Where $x = 1, 2, \ldots, \infty$, $\beta \geq 1$, $0 \leq \alpha \leq 1/\beta$, $0 < \theta < 1$.

The distribution in Eq. (1) depends on the zero-truncated generalized negative binomial defined by Eq. (2):

$$pr(X = x, \alpha, \beta, k) = \frac{k}{k+\beta x}\,\frac{C_x^{k+\beta x}\,\alpha^x(1-\alpha)^{k+\beta x - x}}{1-(1-\alpha)^k}, \tag{2}$$

Where $x = 1, 2, \ldots, \infty$, $k > 0$ $1 \leq \beta \leq \frac{1}{\theta}$

When limit (k→0) is considered for Eq. (2), we obtain the studied distribution in Eq. (1).

The mean of GLSD is defined in Eq. (1), and the variance obtained from the general formula of the (k^{th}) moments about the mean is as follows:

$$\mu_k = E(x-\mu)^k, \qquad\qquad \theta = [-\ln(1-\alpha)]^{-1},$$

$$\mu_1 = E(x) = \frac{\alpha\theta}{(1-\alpha\beta)}, \tag{3}$$

$$\sigma^2 = \mu_2 - \mu_1^2 = \frac{(1-\alpha)\,[2\alpha\beta - \alpha - \alpha^2\beta]}{(1-\alpha\beta)^2}. \tag{4}$$

2. ESTIMATING PARAMETERS

We apply different methods for the *p.m.f.* parameters in Eq. (1).

2.1 Maximum Likelihood Estimation (MLE)

The Maximum Likelihood Estimation (MLE) [8], [9] that corresponds to Eq. (1) is given by:

$$L(x; \alpha, \beta) = \prod_{i=1}^{n} p(X_i = x_i),$$

$$\log L =$$
$$n\log\theta + n\bar{x}\log\alpha + \sum_{x=1}^{k}\sum_{j=1}^{x-1} f(x)\log(\beta x - j) + n\bar{x}\,(\beta-1)\log(1-\alpha) - \sum_{i=1}^{\infty} f(x_i)\log x_i! \tag{5}$$

$$\frac{\partial \log L}{\partial \alpha} = \frac{n\bar{x}}{\alpha} + \frac{n\bar{x}(\beta-1)}{(1-\alpha)} - \frac{n\theta}{(1-\alpha)} = 0,$$

And

$$\frac{\partial \log L}{\partial \beta} \Longrightarrow -\frac{n\bar{x}}{\theta} + \sum_{x=1}^{k}\sum_{j=1}^{x-1}\left[\frac{xf(x)}{(\beta x-j)}\right].$$

This equation derives:

$$\hat{\beta}_{MLE} = \frac{1}{\hat{\alpha}} - \frac{\hat{\theta}}{\bar{x}}. \tag{6}$$

From $\frac{\partial \log L}{\partial \alpha} = 0$, we obtain $\hat{\alpha}_{MLE}$.

2.2 Method of Moments (MOM) Estimator for GLSD Parameters

Method of Moments (MOM) Estimator for GLSD Parameters [10], these estimators $(\hat{\alpha}_{mom}, \hat{\beta}_{mom})$ are obtained by solving the following:

$$\mu'_r = m'_r,$$

$$m'_r = \sum_{x=1}^{\infty} x^r \, p(X = x)$$

When $r = 1$,

$$m'_1 = \sum_{x=1}^{\infty} \frac{x\theta\Gamma(\beta x)\alpha^x(1-\alpha)^{\beta x - x}}{x!\,\Gamma(\beta x - x + 1)}, \tag{7}$$

$$m'_1 = \bar{x} = \frac{1-\alpha}{(1-\alpha\beta)^2}.$$

When $r = 2$,

$$m'_2 = \sum_{x=1}^{\infty} \frac{x^2\theta\Gamma(\beta x)\alpha^x(1-\alpha)^{\beta x - x}}{x!\,\Gamma(\beta x - x + 1)}, \tag{8}$$

$$m'_2 = \theta(1-\alpha\beta)^{-3}\alpha(1-\alpha).$$

Given that:

$$\bar{x}^2 = \frac{(1-\alpha)^2}{(1-\alpha\beta)^4}$$

and

$$\sigma^2 = E(x^2) - [E(x)]^2 \,;$$

then,

$$S^2 = m'_2 - (m'_1)^2 = \frac{(1-\alpha)(2\alpha\beta - \alpha - \alpha^2\beta)}{(1-\alpha\beta)^4}.$$

We have

$$m'_1 = \theta(1-\alpha\beta)^{-1}\alpha, \tag{9}$$

$$m'_2 = \theta(1-\alpha\beta)^{-3}\alpha(1-\alpha), \tag{10}$$

and

$$S^2 = m_2' - (m_1')^2,$$

which is simplified as follows:

$$S^2 = \frac{(1-\alpha)(2\alpha\beta - \alpha - \alpha^2\beta)}{(1-\alpha\beta)^4}$$

We also obtain the following:

$$\bar{x}^2 = \frac{(1-\alpha)^2}{(1-\alpha\beta)^4}. \tag{11}$$

Then,

$$\frac{S^2}{\bar{x}^2} = \frac{(2\alpha\beta - \alpha - \alpha^2\beta)}{(1-\alpha)}. \tag{12}$$

We derive the first three non-central moments obtained from $[m_r' = E(x^r)]$.
Then,

$$\begin{aligned}
m_1' &= \theta(1-\alpha\beta)^{-1}\,\alpha, \\
m_2' &= \theta(1-\alpha\beta)^{-3}\,\alpha(1-\alpha), \\
m_3' &= \frac{\theta\alpha(1-\alpha)(1-2\alpha+2\alpha\beta-\alpha^2\beta)}{(1-\alpha\beta)^5}.
\end{aligned} \tag{13}$$

Given that:

$$m_r' = \frac{\sum x_i^r}{n},$$

We obtain the following based on the preceding relation:

$$\frac{\sum x_i^3}{\sum x_i^2} = \frac{[(1-\alpha) + \frac{S^2}{\bar{x}^2}(1-\alpha)]}{(1-\alpha\beta)^2},$$

$$\frac{\sum x_i^3}{\sum x_i^2} = \frac{(1-\alpha)\left(1 + \frac{S^2}{\bar{x}^2}\right)}{(1-\alpha\beta)^2}. \tag{14}$$

Eq. (14) can be simplified into

$$\frac{\bar{x}^2 \sum x_i^2}{\sum x_i^3}\left(1 + \frac{S^2}{\bar{x}^2}\right) = \frac{\alpha^2\theta^2}{(1-\alpha)}. \tag{15}$$

Given that

$$\theta = -\frac{1}{\log(1-\alpha)},$$

Eq. (15) can be written as follows:

$$\frac{\bar{x}^2 \sum x_i^2}{\sum x_i^3}\left(1 + \frac{S^2}{\bar{x}^2}\right) = \frac{\alpha^2 \log(1-\alpha)^{-2}}{(1-\alpha)}, \tag{16}$$

which is an implicit function that can be solved numerically to determine $(\hat{\alpha}_{mom})$ based on observation. We then obtain $(\hat{\beta}_{mom})$ by using $(\hat{\alpha}_{mom})$ and solving Eq. (11).

2.3 Cuckoo Search Optimization (CSO) Algorithm

This algorithm is based on the breeding behaviour of the cuckoo bird. It has three basic optimization rules [11], [12].

1. Each bird lays one egg at a time, and each egg is placed randomly in a selected nest.

2. The best nest with the highest fitness value will be carried over to the next generation.

3. The number of available host nests is fixed. $(p_\alpha \in [0,1])$ represents the probability of the host bird discovering egg/s in its nest. The host bird can either throw away the egg/s or abandon the nest to build a new one [13][14].

The latter scenario can be regarded as the new best solution.

Let:

$X_i^{(t)}$ Be the nest where the cuckoo bird initially lives, and

$X_i^{(t+1)}$ Be the new nest with the highest fitness value.

When random walk is used, the performance of the cuckoo (*i*) that applies levy flight is expressed as [5, 7]:

$$X_i^{(t+1)} X_i^{(t)} + S \, levy \, \lambda.$$

Levy flight was first introduced by the French mathematician Paul Pierre.

$$S \sim Normal \, (\mu_{10}, \, \sigma^2 = 1)$$

The probability $(p_\alpha \in [0,1])$ indicates that the egg/s in the nest may be from another bird, and thus, the cuckoo bird may leave this host nest and build another one. The *n* hosts may be changed to new hosts with random positions (probability p_α of change). Thus, the objective function belongs to the maximization type and the objective must be fitted into this type. The most important algorithm that can be applied is one used to solve nonlinear equation problems or one used in neural networks because these objects allow the algorithm to be transformed from state to state to reach the optimal solution. Given that GLSD has two parameters (θ and β), then the algorithm implements the following steps.

Each bird lays one egg at a time in a randomly selected nest. The number of selected nests is equal to the number of parameters to be estimated. The number of nests is determined from the following equation:

Number of nests = *LB* + (*UB* − LB) × random number (0, 1).

Let $X_i^{(t)}$ be the nest where the cuckoo bird initially lives.

$X_i^{(t+1)}$ is the new nest with the highest fitness value.

$$X_i^{(t+1)} \ X_i^{(t)} + S\,t^{-\lambda}$$

Each nest contains the parameters to be estimated, and the number of nests is also determined based on these parameters.

Step (1):

Number of nests = $LB + (UB - LB) \times$ random number (0, 1)

Step (2):

The objective function for each nest is calculated as follows:

$$O = \sum_{i=1}^{m} \left[F\left(x_{(i)}, \hat{\theta}, \hat{\beta}\right) - \frac{nx_{(i)}}{n} \right]$$

Step (3):

The best values of the parameters determine the best nest with respect to the eggs.

Step (4):

The repetition begins. Let

$$X_i^{(t+1)}$$

be the nest in which the cuckoo bird initially lives, and

$$X_i^{(t+1)} \ X_i^{(t)} + S\,t^{-\lambda}$$

be the new nest with the highest fitness value.

Step (5):

A new nest is generated for the cuckoo from k, as follows:

$$k = \left[\Gamma(1+\beta) \frac{sin\left(\pi_{i\frac{\beta}{2}}\right)}{\Gamma\left(\frac{1+\beta}{2}\right)\beta\,2^{\frac{\beta-1}{2}}} \right]^{1/\beta},$$

$$U = rand(1,2)k,$$
$$L = rand(1,2),$$
$$step: \frac{U}{|L|^{1/\beta}},$$

$$step\ size = (0.01)step\ (nest - best),$$
$$new\ nest = n\ set + step\ size \times rand\ (1,2)$$

Step (6):

The objective function for each new nest is computed.

Step (7):

The solution is continued until the stopping rule ends with the total frequency. The best solution determined is then printed.

The CSO algorithm, which represents a meta-heuristic algorithm, is adopted to estimate $(\hat{\theta}, \hat{\beta})$. Then, $(\hat{\theta})$ provides the estimate of (α). More details on this algorithm are explained in detail in [15].

3. SIMULATION

The three estimators of (α and β), i.e., the CSO, MLE, and MOM algorithms, are compared through MATLAB: A11 program. Different sample sizes (n = 15, 25, 50, 100) are considered, and the results are compared using the statistical measure mean square error (MSE) and run of each experiment (R = 1000).

TABLE 1: Comparison of the Different Estimators When β = 1.5 and α = 0.3

n	Method	β = 1.5	α = 0.3	Kurtosis	Skewness
15	mle	1.0512	0.3056	1	0
	mse_mle	0.6889	0.0019		
	mom	1.0961	0.7347		
	mse_mom	0.8226	0.1897		
	cuckoo	1.3836	0.3010		
	mse_cuckoo	0.0313	0.0014		
	best	cuckoo	cuckoo		
25	mle	1.3894	0.2991	1.7500	0
	mse_mle	0.0271	0.0018		
	mom	1.0121	0.5908		
	mse_mom	0.2558	0.0869		
	cuckoo	1.3689	0.3292		
	mse_cuckoo	0.0364	8.6762e-004		
	best	cuckoo	cuckoo		
50	mle	1.4254	0.3277	1.7000	0
	mse_mle	0.0479	0.0048226		
	mom	1.2055	0.7163		
	mse_mom	0.0937	0.1765		
	cuckoo	1.3983	0.2991		
	mse_cuckoo	0.0357	8.2262e-004		
	best	mle	mle		
100	mle	1.4910	0.3034	1.7877	0
	mse_mle	0.0220	7.4992e-004		
	mom	1.2194	0.6353		
	mse_mom	0.0788	0.1139		
	cuckoo	1.4032	0.2994		
	mse_cuckoo	0.0343	0.0022		
	best	mle	mle		

TABLE 2: Comparison of the Different Estimators When $\beta = 2$ and $\alpha = 0.2$

n	Method	$\beta = 2$	$\alpha = 0.2$	Kurtosis	Skewness
	mle	1.8177	0.2233	1	0
	mse_mle	0.0673	0.0017		
15	mom	1.0430	0.6648		
	mse_mom	0.9581	0.2182		
	cuckoo	1.9709	0.2107		
	mse_cuckoo	0.0422	0.0015		
	best	cuckoo	cuckoo		
	mle	1.9701	0.2077	1.7314	0
	mse_mle	0.0407	8.8789e-004		
25	mom	1.1209	0.7815		
	mse_mom	0.7887	0.3383		
	cuckoo	1.9801	0.2193		
	mse_cuckoo	0.0375	0.0016		
	best	cuckoo	cuckoo		
	mle	1.9914	0.2036	1.7982	0
	mse_mle	9.1436e-004	5.7535e-004		
50	mom	1.2229	0.7853		
	mse_mom	0.6041	0.3470		
	cuckoo	1.8305	0.2102		
	mse_cuckoo	0.0425	0.0014		
	best	mle	mle		
	mle	2.0130	0.2198	1.7997	0
	mse_mle	7.8137e-004	4.2334e-004		
100	mom	1.2277	0.6513		
	mse_mom	0.6014	0.2035		
	cuckoo	1.9860	0.1971		
	mse_cuckoo	0.0161	0.0012		
	best	mle	mle		

TABLE 3: Comparison of the Different Estimators When $\beta = 2.2$ and $\alpha = 0.4$

n	Method	$\beta = 2.2$	$\alpha = 0.4$	Kurtosis	Skewness
15	mle	1.9464	0.6294	1.7832	0
	mse_mle	0.1197	0.1129		
	mom	1.2001	0.7940		
	mse_mom	0.9998	0.1553		
	cuckoo	2.4615	0.3879		
	mse_cuckoo	0.8312	0.0031		
	best	cuckoo	cuckoo		
25	mle	1.9705	0.3929	1.7955	0
	mse_mle	0.0982	0.0030		
	mom	1.2136	0.8431		
	mse_mom	0.9731	0.1968		
	cuckoo	2.1559	0.3919		
	mse_cuckoo	0.0480	0.0029		
	best	cuckoo	cuckoo		
50	mle	2.0000	0.4325	1.7990	0
	mse_mle	0.0804	0.0022		
	mom	1.2003	0.8801		
	mse_mom	0.9432	0.2326		
	cuckoo	2.3042	0.3823		
	mse_cuckoo	0.0110	0.0050		
	best	Cuckoo	mle		
100	mle	2.1386	0.4386	1.7998	0
	mse_mle	0.0063	0.0021		
	mom	1.5161	0.7435		
	mse_mom	0.4677	0.1184		
	Cuckoo	2.0096	0.4441		
	mse_Cuckoo	0.0071	0.0022		
	best	mle	mle		

TABLE 4: Comparison of the Different Estimators When $\beta = 3$ and $\alpha = 0.33$

n	method	$\beta = 3$	$\alpha = 0.33$	Kurtosis	Skewness
	mle	3.6985	0.8433	1.7997	0
	mse_mle	0.6205	0.2643		
	mom	2.1156	0.8854		
15	mse_mom	0.7822	0.3097		
	cuckoo	2.6793	0.3326		
	mse_cuckoo	0.1882	0.0022		
	best	cuckoo	cuckoo		
	mle	3.5721	0.6693	1.7990	0
	mse_mle	0.3273	0.1835		
25	mom	2.1598	0.8443		
	mse_mom	0.7059	0.2646		
	cuckoo	2.7307	0.3326		
	mse_cuckoo	0.1482	0.0022		
	best	cuckoo	cuckoo		
	mle	3.1131	0.3312	1.7945	0
	mse_mle	0.0128	1.4400e-006		
	mom	2.3598	0.6443		
50	mse_mom	0.4099	0.0988		
	cuckoo	2.8307	0.3316		
	mse_cuckoo	0.0287	2.5600e-006		
	best	mle	mle		
	mle	3.0030	0.3310	1.7800	0
	mse_mle	9.0000e-006	1.0000e-006		
100	mom	2.5598	0.4443		
	mse_mom	0.1938	0.0131		
	cuckoo	2.9307	0.3313		
	mse_cuckoo	0.0048	1.6900e-006		
	best	mle	mle		

TABLE 5: Comparison of the Different Estimators When $\beta = 1.8$ and $\alpha = 0.5$

n	Method	$\beta = 1.8$	$\alpha = 0.5$	Kurtosis	Skewness
	mle	2.4976	0.8870	1.7998	0
	mse_mle	0.4867	0.1498		
	mom	1.1168	0.8875		
15	mse_mom	0.4668	0.1502		
	cuckoo	1.6294	0.4769		
	mse_cuckoo	0.0626	0.0046		
	best	cuckoo	cuckoo		
	mle	2.2176	0.8095	1.7990	0
	mse_mle	0.1744	0.0959		
25	mom	1.1642	0.8400		
	mse_mom	0.4045	0.1159		
	cuckoo	1.7142	0.4684		
	mse_cuckoo	0.0074	0.0052		
	best	cuckoo	cuckoo		
	mle	1.8522	0.6278	1.7958	0
	mse_mle	0.0027	0.0311		
	mom	1.2056	0.7846		
50	mse_mom	0.3534	0.0815		
	cuckoo	1.7278	0.4649		
	mse_cuckoo	0.0052	0.0057		
	best	mle	cuckoo		
	mle	1.8022	0.5349	1.7832	0
	mse_mle	4.8400e-006	0.0014		
100	mom	1.2154	0.7430		
	mse_mom	0.3418	0.0595		
	cuckoo	1. 7663	0.4899		
	mse_cuckoo	0.0011	0.0039		
	best	mle	mle		

4. CONCLUSION

After estimating (α and β) using the three different methods (i.e., MOM, CSO, and MLE) with different sample sizes (n = 15, 25, 50, 100), we determined that the best estimator for small sample sizes (n = 15, 25) based on MSE was the CSO estimator, as shown in Tables 1 to 5. By contrast, MLE was the best estimator for large sample sizes (n = 50, 100). However, we conclude that the CSO estimator is the best type for small sample sizes (n = 15, 25) because the CSO algorithm depends on the number of eggs in the host nest, which is limited.

REFERENCES

[1]   Azizah Binti Mohamad, Azlan Mohd Zain & Nor Erne Nazira Bazin, (2014), "Cuckoo Search Algorithm for Optimization Problems—A Literature Review and its Applications", Applied Artificial Intelligence An International Journal Volume 28, Issue 5.

[2]   Xin She Yang and Sush Deb, "Nature & Biologically Inspired Computing," in IEEE, University of Cambridge, Trumpinton Street, CB2 1PZ, UK, 2010.

[3] Ravi Kiran Varma P, Valli Kumari V, and Srinivas Kumar S, "A novel intelligent attribute reduction technique based on Ant Colony Optimization," International Journal of Intelligent Systems Technologies and Applicaitons, vol. 1, no. 1, pp. 23-45, 2015.

[4] Ravi Kiran Varma P, Valli Kumari V, and Srinivas Kumar S, "Feature selection using relative fuzzy entropy and ant colony optimization applied to real-time intrusion detection system," Procedia Computer Science, vol. 85, no. 2016, pp. 503-510, 2016.

[5] Ravi Kiran Varma P, Valli Kumari V, and Srinivas Kumar S, "Application of Rough Sets and Ant Colony Optimization in feature selection for Network Intrusion Detection," International Journal of Applied Engineering Research, vol. 10, no. 22, pp. 43156-43163, 2015.

[6] Ravi Kiran Varma P, Valli Kumari V, and Srinivas Kumar S, "Ant Colony Optimization Based Anomaly Mitigation Engine," Springerplus, vol. 5, no. 1, pp. 1-32, 2016.

[7] Xin-She Yang and Suash, ""Engineering optimisation by cuckoo search"," International Journal of Mathematical Modelling and Numerical Optimisation, vol. 1, no. 4, pp. 330-343, 2010.

[8] D. S. Bunch, "Maximum Likelihood Estimation (MLE) of probabilistic choice models", SIAM Journal on Scientific and Statistical Computing, 8(1):56-70.

[9] M.S.Prasad Babu et al, (2012), "Development of Maize Expert System using Ada-Boost Algorithm and Navie Bayesian Classifier", International journal of computer Applications technology and research, volume 1-issue 3, 89-93.

[10] Persi D., "Application of the Method of Moments in Probability and Statistics", Auspices national science foundation grant DMS86-00235, Nov. 1986.

[11] Xin She Yang and Suash, "A brief literature review: Cuckoo Search and Firefly Algorithm," Studies in Computational Intelligence, vol. 516, pp. 49-62, 2014.

[12] Hongqing Zheng and Yongquan Zhou,(2013), A Cooperative Coevolutionary Cuckoo Search Algorithm for Optimization Problem", Journal of Applied Mathematics, J. Appl. Math. Volume 2013, Special Issue (2013).

[13] Najla Akram AL-Saati, Marwa Abd-AlKareem, (2013), "The Use of Cuckoo Search in Estimating the Parameters of Software Reliability Growth Models", International Journal of Computer Science and Information Security,Vol. 11, No. 6.

[14] Manjeet Kumar, Tarun Kumar Rawat,(2015), "Optimal design of FIR fractional order differentiator using cuckoo search algorithm", Expert Systems with Applications, volume 42, Issue 7, Pages 3433–3449.

[15] Prasad Babu, B.Jyothsna, (2015), "Implementation of Cuckoo Search Optimization Algorithm using Semantic Web – Based Coconut Expert System", International Journal of Advanced research in Computer Science and Software Engineering, Vol.5, Issue 9.

A COMPARATIVE EVALUATION OF DATA LEAKAGE/LOSS PREVENTION SYSTEMS (DLPS)

Kamaljeet Kaur[1], Ishu Gupta[2] and Ashutosh Kumar Singh[2]

[1]Govt. Sr. Sec. School, Ambala, Haryana, India
[2]Department of Computer Applications, National Institute of Technology, Kurukshetra, Haryana, India

ABSTRACT

Data is the most valuable assets of an organization that need to be secured. Due to limited computational resources, Customers outsource their workload to cloud and economically enjoy the massive computational power, bandwidth, storage, and even appropriate software that can be shared in a pay-per-use manner. Despite of tremendous benefits of cloud computing, protection of customers' confidential data is a major concern. Data leakage involves the intentional or unintentional release of secure or confidential information to non-trusted environment. Data leakage poses a serious issue for companies as the number of incidents and the cost to those experiencing them continue to increase. Data leakage is enhanced by the fact that transmitted data (both inbound and outbound); including emails, instant messaging, website forms and file transfers. Data leakage prevention system (DLPS) is a strategy for making sure that end users do not send the confidential data or information outside the corporate network. This review paper aims to study data leakage prevention through some challenges and data protection approaches as well as considering some limitations. This survey of DLPS can benefit academics as well as professionals.

KEYWORDS

Data Leakage Prevention (DLP), Insider Attacks, Sensitive Data, Data Access & Protection

1. INTRODUCTION

Data leakage is defined as the accidental or intentional distribution of confidential data to an unauthorized entity. Confidential data of companies and organizations include intellectual property, financial information, personal credit card data scores, information about their sanctions and other information depending upon the business. Data leakage is a serious threat to organizations as the number of incidents and the cost to those experiencing them continue to increase. Data leakage is magnified by the fact that transmitted data are not regulated and monitored on the way to their destination. The diffusion of data can be done through digital media as well as by the company's official person also.

It is more severe when this is carried out by insiders. The researchers discovered that despite the security policies, procedures, and tools currently in place, employees around the world are engaging in risky behaviors that put corporate and personal data at risk [1]. Organizations provide easy access to databases for information sharing, storage and compression technology has allowed for more powerful (high-risk) endpoints. An 80-MB mobile device now holds 6000

Microsoft Word documents or 7, 20,000 emails, and new 64-GB removable devices allow an entire hard drive to be copied onto a device same as the size of a pack of gum. These devices make it easier for employees, partners, or data thieves to access, move, or lose intellectual property or customer data. Mitigating data leakage from insider threats is a difficult challenge [2], [3]. Data leakage can occur in many forms and in any place [4], [5]. In survey of United States in 2014, Cybercrime emphasize on the seriousness of attacks caused by insiders of the companies. According to the survey report, companies experienced 37% internal attacks caused by insiders and researchers mentioned that the ratios of insider attacks are more destructive as compared to the attacks that are performed outside of the company. The ratio of private information that accidentally opens to the elements was 82% and in 76% of cases, confidential accounts were stolen [6].

According to statistics, it is stated that insider attacks has a high rate among other attacks that causes data leakage. By using Deep Content Analysis (DCA) techniques such as rule-based, regular expressions, database fingerprinting, exact file matching, statistical analysis, DLPS easily finds out the 'sensitivity' of the information and used to detect 'sensitive' information within traffic. This can be done either to classify the information into categories (e.g. 'confidential', 'secret') or to detect sensitive information within (outgoing) data. When a sensitive piece of information is found leaving the company, DLPS triggers the appropriate alert and action to be taken. There is necessity to implement DLP controls and supporting information security controls on time so that the effectiveness of these controls monitored over time. It helps to improve the management of data with minimum risk. The aim to design and develop DLPSs is to prevent data from breaches.

We can solve the data leakage problem by using Data Leakage/Loss Prevention System (DLPS). Generally DLPS as represented in Fig. 1 is used to discover, monitor, and protect the following type of data [7], [8].

- *Data at Rest*- Inactive data that is stored physically in any digital form like in spreadsheets, mobile devices, laptops and in databases etc. Examples include: - vital corporate files stored on the hard drive of an employee's notebook computer and files on an external backup medium.

- *Data in Motion*- Any data that is moving through the network to the outside via Internet like an email being sent.

- *Data in Use*- Data at the endpoints of the network like data stored in computer's RAM, cache, external drivers and data on USB devices etc. Examples include: - data that is being written, revised, or deleted.
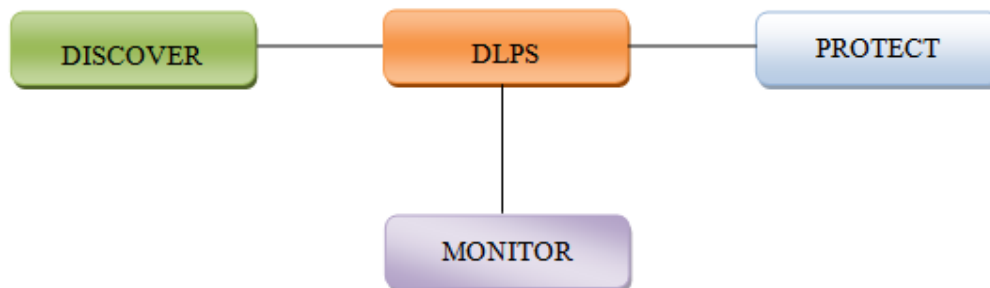

Figure 1. Data leakage prevention system (DLPS)

2. CHALLENGES IN DLPS

There are Common behaviors resulting in potential risk of data leakage like both physical and logical Access control, Accessing unauthorized websites, Leaving passwords unprotected and many more. This section illustrates the current challenges as shown in Fig. 2 to be solved by the DLP as follows:

1. *Encryption Challenge-* encryption is only one approach to secure data and security also requires access control, data integrity, system availability and auditing. So, it is difficult to detect and intercept encrypted confidential data and to recognize the data leakage occurring over encrypted channels [9].

Figure 2. DLPS challenges

2. *Access Control Challenge-* In the field of Information Security, Access control is a way of limiting access to a system, or to physical or virtual resources. In corporate, it is not easy to control employee's access to data repositories. For e.g. An employee of a company want to access data that he/she is not involved into, can steal some information if an access control system grants full access to all code repositories for all employees [10].

3. *New Data and Customization Challenge-* Sometimes, it is difficult to customize a DLP system particular for an employee, if the system utilizes old methods of data protection like regular expressions, keywords, or digital fingerprints. To create regular expressions, manual keywords for new customization process may take longer time. Moreover, this process is meant to be repeated as new type of confidential data appears.

4. *Social Network Challenge-* It is not sufficient to capture heterogeneous communication groups where people belong to more than one group, or even more when new communication groups are formed, old one disappears. In this situation, it is difficult to reveal a person who leaks the data (an outsider) in a communication or to detect persons having limited access to data [11].

3. CURRENT APPROACHES FOR DLP

This section categorizes current approaches for Data Leakage Prevention and identifies their main benefits and shortcomings:

A Learning and specification based system for Data leakage Prevention- This hybrid model combines signature based and anomaly based solutions, enabled on both detection and prevention. Two main dimensions are used to characterize the model: *i) filtering approach*, which describes whether users are permitted or not and *ii) model construction*, which describes how model is constructed. In Filtering, *blacklist* is used for well-known threats or undesired behaviors and *white listing* is used to identify the permissible activities. Only those transactions are considered to be legitimate that will match the model. Two main approaches are used to build the model *i) Specification approach and ii) Learning-approach* [12].

- *Specification-approach:* This approach is based on expert's knowledge and background of the transactions that lead to very accurate models. As, for instance, specification based blacklisting systems, also known as *Signature- based systems* that find the known attacks. A specification-based white listing system is used to detect unknown attacks.

- *Learning-approach*: This approach automatically learns the behavior of model using some techniques like machine learning and statistical modeling.

Shortcomings: These approaches created models that are less accurate as compared to those manually specified. As a consequence, these are inclining to high false positive rate. To check whether transaction is legitimate or not, a large number of alerts are generated and analyzed by human operator that cause to high operational cost [13].

Secure Key Stream Analyzer for Data Leakage Prevention- This approach illustrates that many data leakage prevention solutions depend on scanning file content. Key Stroke Profile not only scans the content of file rather it is capable to parse different file formats. But, risk of data leakage still exists for unsupported file formats. This approach proposed a new DLP model named as *Secure Key stream Analyzer (SKA)* [14].

- *Secure Key Stream Analyzer-* This SKA works on keyboard Application program interface (API). By hooking on keyboard API, it helps to track profile user key stroke behavior and discovers sensitive data. Data creator can be identified according to keystroke behavior.

Shortcomings: There are some issues in keyboard API that needs to be solved: Instead of using a keyboard, if a user uses mouse to make some text modifications like copying text and pick information from auto filled forms, in this situations SKA does not work. It only detects the text typed linearly [15].

A Result based Approach for Data Leakage Prevention- This approach discussed an information flow between one origin and many destinations (receivers) .The *Partially Observable Markov Decision Processes* (POMDPs) method is used over a fixed period called decision epochs where:

- To share a packet is equally important between origin and destination (i.e. a deterministic receiver either leaks all the packets, it receives or none of them).

- Leakage of packets that have been shared is a reward for destination; although disagreeable from the origin (i.e. the receiver is deterministic and considered a foggy receiver who leaks % f of the packets, it always receives).

- Sharing decision from origin is determined by using faulty observations of the accidental leakage of information from the destination, i.e. if packets are shared from origin with multiple foggy receivers and a different percentage of packet leaks occur at each destination [16].

Shortcomings: As the ratio of leak packets increase, it increases the tolerance at origin side, results in effect on the expected incentive of its most favourable strategy.This POMDP requires a huge amount of calculation and it suffers from scalability limitations.

There is a need of DLP solution that will allow secure sharing of confidential information in companies [17].

A Turkish Language Based Data Leakage Prevention System- This approach proposed a data leakage prevention system for Turkish language consisting two phases *i) training phase* and *ii)detection phase*. Two algorithms are used to describe the system: *Boyer Moore (BM Algorithm)* [17] is used to search exact sensitive strings exposed to whitespace attack and *Smith Waterman (SW) sequential alignment algorithm* [18] is used to detect modified string attacks.

- *Training Phase*- during this phase, list of sensitive words are generated from the sensitive document.

- *Detection Phase*- This phase is used to detect the modified sensitive content that attacker used to bypass the security system.

TF-IDF method is used to extract the sensitive words of sensitive documents. Latent Semantic Indexing (LSI) is used to construct the model document topics. This approach used Zemberek tool for extracting and analyzing the Turkish language [19].

Shortcomings: Attacks like adding, deleting and changing characters in 'sensitive' word, deleting white spaces from both sides of 'sensitive' word and adding white space to the middle of the 'sensitive' word were used to design the system. This tool is not only required for Turkish/English, but also for other languages [20].

4. DATA LEAKAGE PROTECTION TECHNIQUES

Data protection for various data states is represented in Table 1. Fig. 3 shows the various activities performed by DLPS to protect the data at various states.

Safety measures for Data-at-Rest: To protect data leakage, content discovery solutions is required. It helps to detect the sensitive data reside in separate locations by performing scanning in laptops, FTP servers, SMTP servers and in database [21]. Techniques for content discovery are as follows:

- *Local scanning of data*- In this technique, an agent is installed on the host machine that regularly scans the content which are stored in the files. It relocates, encrypts and quarantines the content after finding anything malicious in it. During the process, agents are always active, execute a policy even when devices are not placed locally and are not connected to the network.

  Disadvantage: On the target system, agents have low processing power and less memory.

- *Remote Scanning*- Scanning is performed from remotely located computers by maintaining a connection with server and application level protocols.

  Disadvantage: When scanning is performed from a remote computer that results in increased network traffic and low performance.

Table 1. Data leakage protection for different data states.

| Type	Description	DLP goal
Data-at-rest	Information stored in an organization like files, servers, document management systems and email servers.	Content discovery
Data-in-motion	Organization data is restricted to network traffic such as web traffic	Block transmission of sensitive data.
Data-in-use	Information currently used at the end points such as http, https, print, file to USB and outlooks.	Prevents unauthorized usage of data (e.g. copying to a thumb drive).
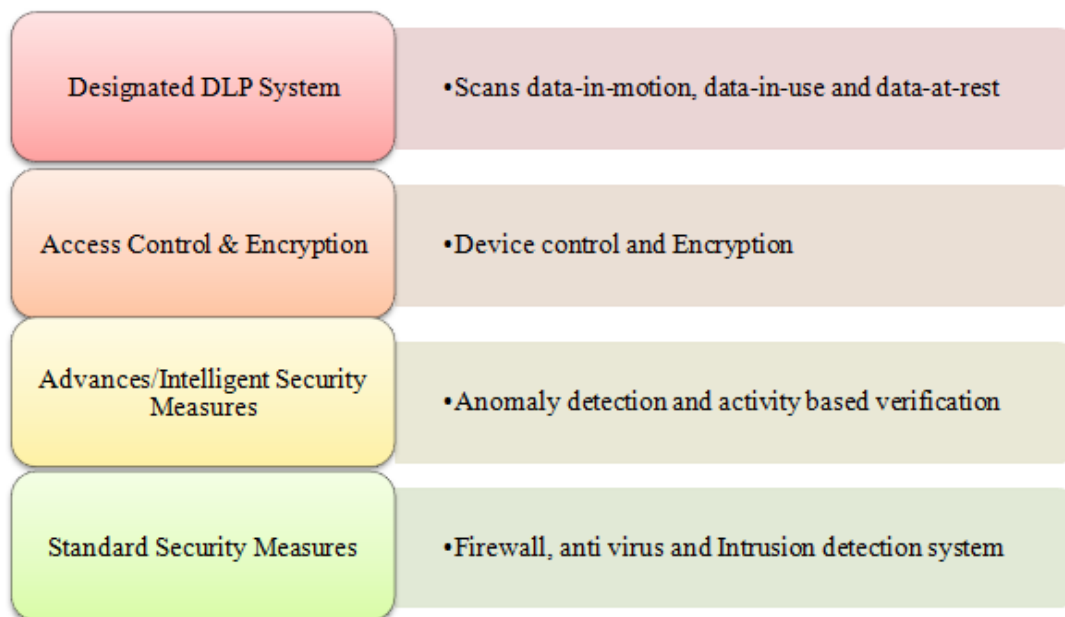
Figure 3. DLPS activities

Safety measures for Data-in-Motion: Network-based solutions are deployed on company's gateway. Gateway computer search the sensitive content and block the malicious activities immediately that violates the policy. These solutions capture the full data and perform the content analysis in real time [22], [23].

Safety measures for Data-in-Use: Local agents and host machines regularly check sensitive data such as data copied from one location and pasted into another location, data from print screen, unauthorized data transmission and copying data to a USB/CD/DVD [5].

5. LIMITATIONS

A DLP solution help organization to control sensitive data, but it has some pretty significant limitations also.

- *Graphics*- Graphics files consist sensitive information of companies like company's design documents, academic records, credit card scores etc. that demands scanning to prevent data leakage from unauthorized users. Scrutinize a file manually and then blocking the information shows that there is a gap exists in company's control. Companies having considerable IP for scanning graphics format should expand strong policies that administrate the use and allotment of data.

- *Third-party service providers*- While sending the company's sensitive information to third party, there should be mirrors of same level to control over the information. A vigorous third-party should comprise effective convention speeches over data leakage prevention and a supporting audit program that will help to moderate the risk.

- *Cross-application support*- DLPs have limited application level type functionalities. If DLP agent monitors data manipulation in any application and at the same time, it wants to perform same operation on another file then it is not able to do so. Companies must be ensured about DLP solutions that will prevent data leakage and identify applications which manipulate company's sensitive data.

- *Limited client OS support*— Many DLP solutions do not support data leakage prevention solutions for operating systems such as Linux and Mac operating systems because their usage as clients are fewer in companies [24].

6. FUTURE ANALYSIS FOR DLPS

In future, following activities will be followed to prevent company's data from leakage.

- *System Isolate*- To prevent data from leakage, companies should isolate their departments. They should close FTP port, TELNET port. Only HTTP ports should work but with some protection policies. Companies should ensure that traffic will pass through HTTP port.

- *E-mail Security*- In companies, grouping can be performed to prevent data leakage. There can be a group of 10 persons who can exchange emails within the group only. There should be some restrictions for sending emails. Companies should enforce some policies while sending an email from one department to another department so that the person of another department could not send an email to outside the network.

- *System Specific*- To prevent data leakage, each employee of the company must be restricted to their system. Administrator of the company should ensure that employees will use their allotted system only.

- *Smart Phones*- The employees of the companies uses smart phones and it cannot be stopped completely. Smart phones are enabled with new functionalities that handles as much data as you need. For companies, these smart phones are the main cause of sensitive data leakage such as transferring of e-mails and important documents accidently or intentionally.

These are the major factors that contribute to grow Data Leakage market. DLP solution focuses on organizations towards meeting regulatory and compliance requirements and data saved on public and private cloud.

7. CONCLUSIONS AND FUTURE DIRECTIONS

In this paper, we discussed the challenges in DLPs and current approaches for data leakage prevention. We described how company's confidential information can be protected from unauthorized user's access. We explained various techniques like learning and specification, secure key stream analyzer, result based approach for data leakage prevention, but still there are various elements that leak the company's data. As we know data leakage happens through social media, cybercrimes and with the help of insider attacks. All these factors have a great impact on the company's reputation. Companies know which data is important to their business, where it is located and how it is sent to the outside network. Companies should enforce some policies, rule & regulations to prevent their data from unauthorized user's access.

Data Leakage Prevention System is a solution for all these problems that helps to discover, monitor and project the company's important data. There are some challenges that need to be solved. Cluster analysis algorithm has the ability to group data into cluster for further analysis that will help to cope with access control challenge and social network challenge.

Hence, there is necessity of research that will take a balanced approach for cloud computing data leakage and incorporate not only to end-users, but also with cloud provider and the cloud customers.

REFERENCES

[1]   Ernst & Young, "Data loss prevention: Keeping your sensitive data out of the public domain," Insights on governance, risk and compliance, October 2011.

[2]   S. Alneyadi, E. Sithirasenan and V. Muthukkumarasamy, "Detecting Data Semantic: A Data Leakage Prevention Approach," 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, 2015, pp. 910-917.

[3]   S. Alneyadi, E. Sithirasenan and V. Muthukkumarasamy, "Discovery of potential data leaks in email communications," 2016 10th International Conference on Signal Processing and Communication Systems (ICSPCS), Gold Coast, QLD, 2016, pp. 1-10.

[4]   B. M. Babu and M. S. Bhanu, "Prevention of Insider Attacks by Integrating Behavior Analysis with Risk based Access Control Model to Protect Cloud," Procedia Computer Science, Vol. 54, pp. 157-166, 2015.

[5]   D. Kolevski and K. Michael, "Cloud computing data breaches a socio-technical review of literature," 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), Noida, 2015, pp. 1486-1495.

[6]   S. Mathew and M. Petropoulos, "A data-centric approach to insider attack detection in database systems, " in Recent Advances in Intrusion Detection, ser. LNCS 6307, Springer, pp. 382–401, 2010.

[7]   Frost and Sullivan, "World Data Leakage Prevention Market," Technical Report ND34D-74, United States, 2008.

[8]   B. Hauer, "Data and Information Leakage Prevention Within the Scope of Information Security," in IEEE Access, vol. 3, no., pp. 2554-2565, 2015.

[9]   P. Raman, H. G. Kayacık, and A. Somayaji, "Understanding Data Leak Prevention," in 6th Annual Symposium on Information Assurance (ASIA'11), pp. 27, 2011.

[10]   S. Alneyadi, E. Sithirasenan,V. Muthukkumarasamy, "A survey on data leakage prevention systems," Journal of Network and Computer Applications, Vol. 62, pp. 137-152, February 2016.

[11] DLP Technologies, Challenges and Future Directions 268462340_ [accessed Jun 23, 2017].

[12] E. Costante, D. Fauri, S. Etalle, J. D. Hartog and N. Zannone, "A Hybrid Framework for Data Loss Prevention and Detection," 2016 IEEE Security and Privacy Workshops (SPW), San Jose, CA, 2016, pp. 324-333.

[13] A. Shabtai, Y. Elovici and L. Rokach, "A survey of data leakage detection and prevention solutions", ser. Springer Briefs in Computer Science, Springer-Verlag, New York, 2012.

[14] J. S. Wu, Y. J. Lee, S. K. Chong, C. T. Lin and J. L. Hsu, "Key Stroke Profiling for Data Loss Prevention," 2013 Conference on Technologies and Applications of Artificial Intelligence, Taipei, 2013, pp. 7-12, 2013.

[15] K. Revett, F. Gorunescu, M. Gorunescu, M. Ene, S. T. de Magalh˜aes and H. M. D. Santos, "A machine learning approach to keystroke dynamics based user authentication," Int. J. Electronic Security and Digital Forensics, Vol. 1, No. 1, pp. 55–70, 2007.

[16] J. Marecki, M. Srivatsa and P. Varakantham, "A Decision Theoretic Approach to Data Leakage Prevention," 2010 IEEE Second International Conference on Social Computing, Minneapolis, MN, 2010, pp. 776-784.

[17] M. Srivatsa, P. Rohatgi, S. Balfe and S. Reidt, "Securing information flows: A metadata framework," in Proceedings of 1st IEEE Workshop on Quality of Information for Sensor Networks (QoISN), 2008.

[18] Y. Jeong, M. Lee, D. Nam, J.-S. Kim, and S. Hwang, "High performance parallelization of Boyer–Moore algorithm on many-core accelerators," Cluster Computing, vol. 18, pp. 1087-1098, 2015.

[19] Y. Canbay, H. Yazici and S. Sagiroglu, "A Turkish language based data leakage prevention system," 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, 2017, pp. 1-6.

[20] Y. Liu, C. Corbett, K. Chiang, R. Archibald, B. Mukherjee, and D. Ghosal, "Detecting sensitive data exfiltration by an insider attack," in Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, pp. 16, 2008.

[21] R. Tahboub and Y. Saleh, "Data Leakage/Loss Prevention Systems (DLP)," 2014 World Congress on Computer Applications and Information Systems (WCCAIS), Hammamet, 2014, pp. 1-6.

[22] S. Liu and R. Kuhn, "Data Loss Prevention," in IT Professional, vol. 12, no. 2, pp. 10-13, March-April 2010.

[23] G. Lawton, "New Technology Prevents Data Leakage," in Computer, vol. 41, no. 9, pp. 14-17, Sept. 2008.

[24] "Data leak prevention," Information Systems Audit and Control Association, Technical Report, 2010.

INTENTIONAL BLANK

A Security Period Update Method Using Evaluation Function for Improving Energy Efficiency of Statistical En-Route Filtering-Based WSNs

Jung-Sub Ahn[1] and Tae-Ho Cho[2]

[1]College of Information and Communication Engineering,
Sungkyunkwan University, Suwon 16419, Republic of Korea
[2]College of Software Platform, Sungkyunkwan University,
Suwon 16419, Republic of Korea

ABSTRACT

In recent years, Wireless Sensor Networks(WSNs) research has been carried out with the goals of achieving high security and energy efficiency. In a WSN, sensor nodes are vulnerable to physical attacks because they are deployed in an open environment. An attacker can inject a false report into networks using these vulnerabilities. F. Ye et al. proposed statistical en-route filtering to prevent false report injection attacks. In order to effectively use their scheme, techniques for determining thresholds using fuzzy logic have been studied. To effectively apply these techniques to the network, an appropriate update period should be set according to the network environments. In this paper, we propose a security period update method in order to improve the lifetime of the network in the statistical en-route filtering approach based on a wireless sensor network of the cluster environment. The experimental results show that up to an 11.96% improvement of the energy efficiency can be achieved when the security threshold is set to the optimal period.

KEYWORDS

Network Simulation, Wireless Sensor Network, Statistical En-route Filtering, False Report Injection Attack, Energy Efficiency.

1. INTRODUCTION

A wireless sensor network (WSN) consists of hundreds to thousands of sensor nodes and a base station (BS), providing real-time monitoring of sensor fields in industrial, medical, and military applications. A sensor node consists of a processor, memory, a battery, and a wireless transmitter [1-2]. Due to battery limitations, research involving increasing the network lifetime considering limit factors is currently actively studied [3]. If an event occurs, the sensor node generates a report with detected information and sends it to the BS using a hop-by-hop technique to notify the

user. Sensor nodes are vulnerable to physical attacks because they have limited memory and batteries, and are deployed in open environments [4]. The attacker can compromise the sensor node and generate a false report using the secret information contained in the node. In addition, the attacker can inject a false report with the wrong event data type into the networks, as shown in Figure 1.

If a WSN consists of a cluster, false report insertion attacks are divided into two cases when the cluster head (CH) node that generates the report is compromised and when the member (MB) node that creates the authentication key is compromised. If the CH node is compromised, the attacker generates an arbitrary report and transmits it to the next node, causing false notification and energy exhaustion problems of intermediate nodes in the routing path [5-6]. If the MB node is compromised, it can generate a false event notification to the CH node, depleting the energy of the cluster region and deploy incapacitating nodes. To minimize this problem, it is necessary to detect and remove the false report early and to filter out incorrect alarms to users. To prevent false report injection attack, F. Ye et al. proposed statistical en-route filtering (SEF) [7]. In SEF, it is important to set an appropriate security threshold because the security threshold has a trade-off relationship between power consumption and filtering probability. Security threshold determining methods using fuzzy logic were proposed to obtain an appropriate security threshold value [8]. However, this method does not consider the update cycle of the fuzzy logic process. If the update period is not taken into consideration, the worst case consumes more power.
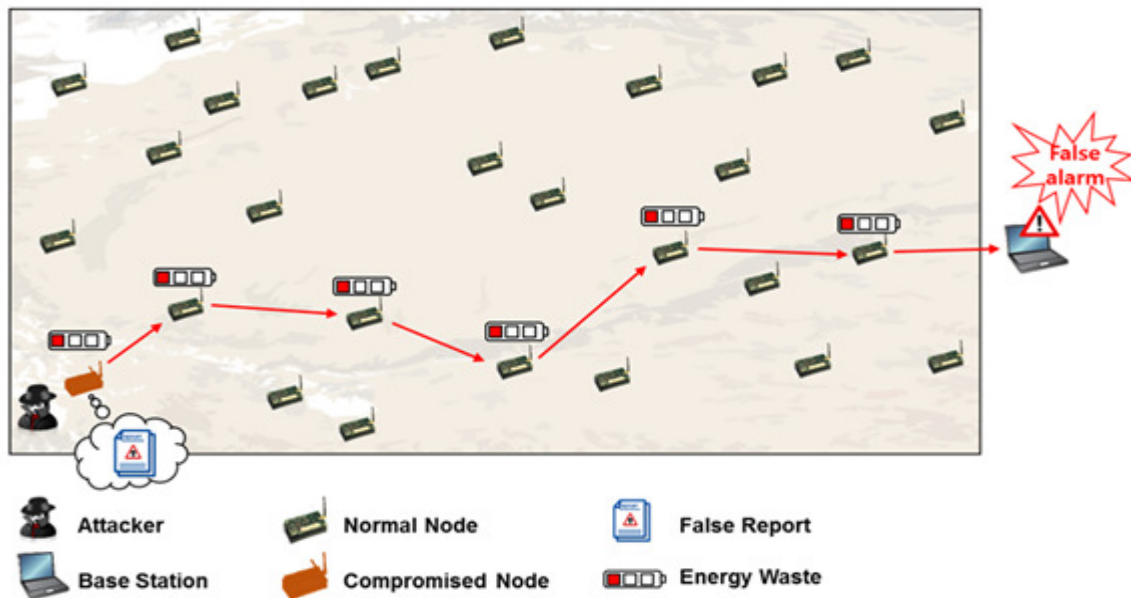

Figure 1. False report injection attack

In this paper, we propose a security period update method using an evaluation function to improve the energy efficiency of SEF-based WSNs. The proposed method automatically determines the update cycle considering network environment factors. Nodes that are updated on a periodic basis do not have to send the information messages needed for the update and can save energy by adjusting the security strength in a timely manner. We demonstrated the performance of the proposed method through performance analysis by applying the evaluation function. The experimental results show that the proposed method saves up to 11.96% of energy.

The remainder of the paper is organized as follows. In Section 2, we explain the statistical en-route filtering scheme and motivation. Section 3 introduces the proposed evaluation function and fuzzy logic. Section 4 details the experiment results and, finally, the conclusions of this study are discussed in Section 5.

2. RELATED WORKS

2.1. Statistical En-route Filtering (SEF)

F. Ye et al. proposed SEF to prevent false report injection attacks. SEF statistically filters false reports by adding threshold values for authentication to the report generated by the representative node. The intermediate node verifies the report when a false report is transmitted. In addition, the intermediate nodes block false reports, thereby reducing unnecessary energy consumption to the BS. The SEF method consists of four phase: the key distribution phase, report generation phase, intermediate filtering phase, and BS node verification phase. In the key distribution phase, the user sets various setting values including the threshold value before the sensor nodes are deployed in the target area. The higher the threshold, the greater the false report detection rate, which makes it difficult for an attacker to generate false reports. However, high thresholds require high power consumption to transmit reports. Each node is randomly distributed among the key sets divided by the partition in the global key pool created at the BS. Figure 2 shows the key distribution process, where P1 to pl denote the partition containing the key.
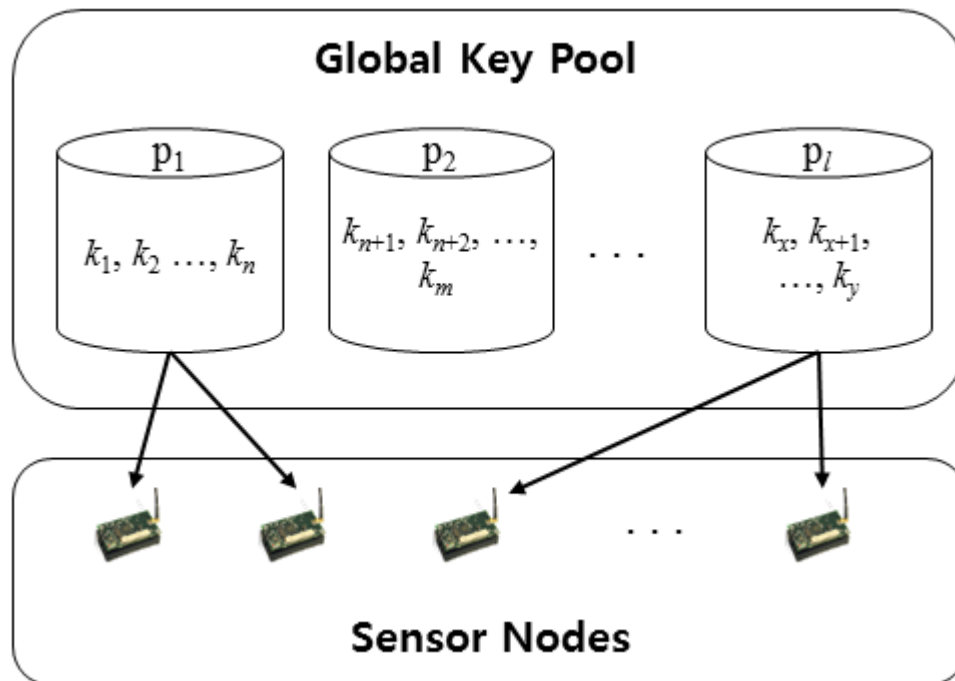

Figure 2. Key distribution phase in SEF

After the key distribution process is over, the nodes are deployed in the target area where they want to collect information. When the deployed sensor nodes detect the event, the node with the highest detection rate is selected as the representative node. The representative node broadcasts

event information to find neighboring nodes that have detected the same event signal value. Neighboring nodes that have received the event information compare whether occurrence same event information. If the generated events are the same, the message authentication code (MAC) is generated and transmitted to the representative node using the pre-distributed key and hash function. The generated MACs are used to verify the report. The threshold value signifies the number of MACs included in the report when the representative node generates the report. If a MAC is collected that is smaller than the threshold for collecting MACs, no reports are generated. The representative node generates the report by including event contents and MACs that vary from one another as the threshold value. Since each node has a certain probability of a common key, it can probabilistically detect false reports. Event reports are transmitted to the BS node through multi-hop routing. If the forwarding node receives the report, it goes through the verification process shown in Figure 3

1) Check that $T\{i_j, M_{ij}\}$ tuples exist in the packet; drop the packet otherwise.

2) Check that the T key indices $\{i_j, 1=j=T\}$ belong to T instinct partitions; drop the packet otherwise.

3) If it has one key $K \in \{K_{ij}, 1=j=T\}$, it computes $M = MAC(K, L_e\|t\|E)$ using Equation 1. Determine if the corresponding M_{ij} is the same as M. If so, it sends the packet to the next hop; otherwise, the packet is dropped.

4) If it does not have any of the keys in $\{K_{ij}, 1=j=T\}$, send the packet to the next hop.

Figure 3. Four operation phases of en-route filtering

M_{ij} refers to the MACs included in the report. The MAC consists of K, which is the key value of the node, Le is the event information, t is the event occurrence time, and E is the contents of the event. Finally, when the BS node receives the report, it verifies all MACs included in the report using the global key pool. If the BS node determines that it is a normal report after verification, it sends the event contents to the user.
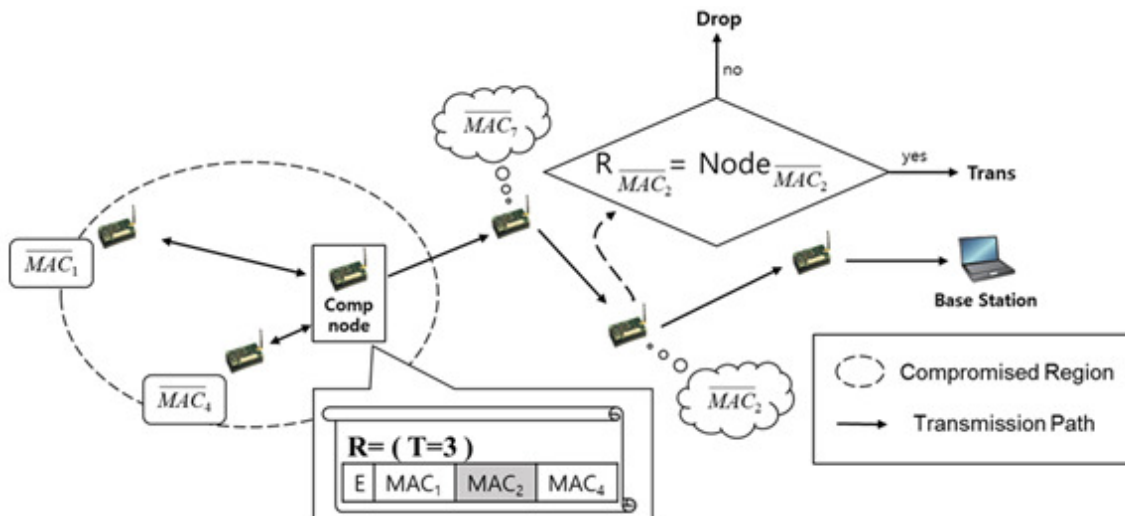

Figure 4. False report filtering process

Figure 4 shows the false report filtering process. In Figure 4, MAC_n refers to the MAC belonging to n partitions. The attacker must compromise the same number of nodes as the threshold value to generate a complete false report using the compromised node. In Figure 4, assuming that the partition compromised two different nodes in a situation where the threshold value is 3, MAC_1 and MAC_4 are known, but MAC_2 is unknown. In the forwarding node, the node having MAC_2 compares it to the verification report to verify the compromised MAC and drops the report. This mechanism can reduce unnecessary energy consumption by performing intermediate filtering of false reports.

2.2 Motivation

Setting an erroneous threshold according to the environment in the SEF has an adverse effect on the energy consumption efficiency [9]. To perform this task, research was conducted to determine the threshold value using fuzzy logic [8]. However, we did not consider the cycle of updating the threshold value for efficient use of this scheme. If the update period is wide, the node information value must be requested to the node every time, which is inefficient in an environment where the attack rate does not change. Conversely, if the period is narrow, it is inefficient in environments where the attack rate changes frequently. Therefore, in order to manage energy efficiently, it is important to determine the threshold update period. In particular, a method of determining the threshold update period is needed to establish an adaptive fuzzy system that can reduce energy consumption while maintaining security. In addition, the network manager analyzes the update cycle to help the nodes efficiently manage their energy.

3. PROPOSED SCHEME

3.1. Assumptions

It is assumed that the plurality of sensor nodes is randomly placed in the destination field and arranged closely to each other. The route path is set during the pre-deployment phase and is assumed to use single-path routing. Each sensor node has a unique identification number. Each time the CH nodes transmit node information to the BS, the BS knows the specific information of the CH node. The WSN uses a cluster approach, which is advantageous because it considers performance and limited resources [10]. One cluster consists of a cluster head node and nine member nodes. Each member node collects the event and notifies the cluster head node, and the cluster head sends the report to the BS.

3.2 Overview

We analyzed the power consumption depending on the update period to the experimental environment based on SEF. Threshold determination fuzzy logic uses the information transmitted at a particular node to determine the threshold. Fuzzy inference uses the min-max composition [11] of the mandani model, which is one of the inference models, and the center of area (COA) method is used for the defuzzification method. Figure 5 shows that the CH node receives specific data and determines a new threshold value for the environment according to the cycle from the evaluation function. The FTR(False Traffic Ratio), BS_H(Base Station Hop), and RE(Remaining Energy) were used as inputs.
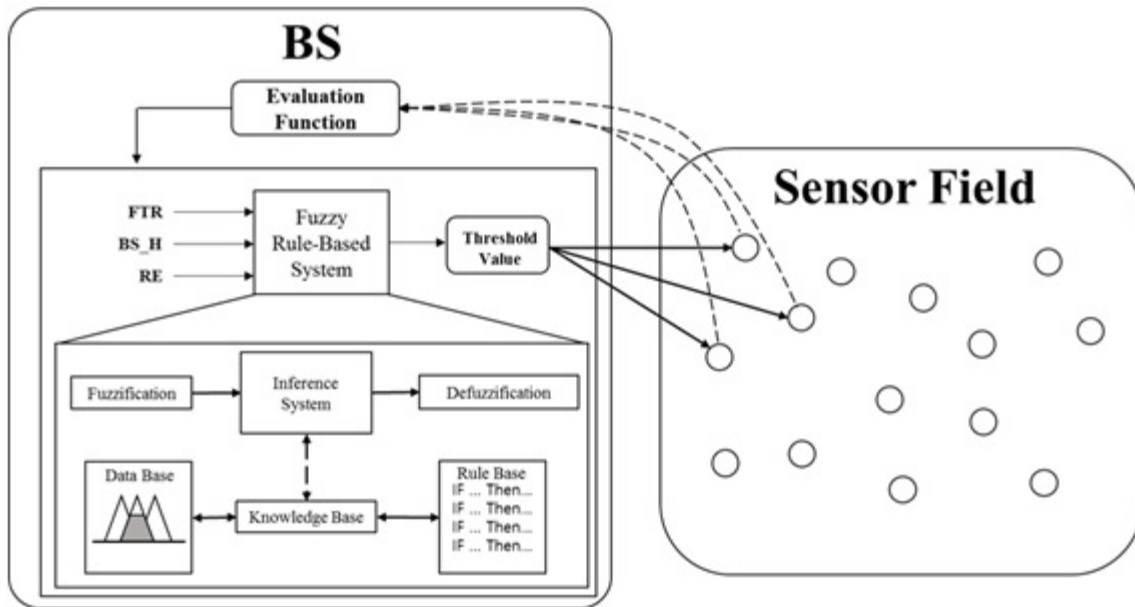
Figure 5. Overview of the proposed scheme

3.3 Security Period Update Method

In the initial period in the CH, the CH transmits specific information such as the current set period value, the power consumption value of the node, and the attack rate to the BS. The BS transmits a new threshold value and period to the CH node after determining whether to update the update period through the received information and the evaluation function.

$$f(x) = \left(\sqrt{(x - 50)^2} \right)^F + MP$$

Equation 1. Evaluation Function

Equation (1) describes the evaluation function used in the proposed method, where x is the measured attack rate, F is the flexibility for period determination, and MP is the minimum period value. The BS evaluates the security rate for determining the new period. When the cycle is determined, the new threshold value is output using the fuzzy algorithm as shown below.

   · **False Traffic Ratio(FTR) = {L(Low), M(Middle), H(High)}**

   · **Base Station Hop(BS_H) = {VN(Very_Near), N(Near), M(Middle), F(Far),**

   VF(Very_Far)}

   · **Remaining Energy(RE) = {VL(Very_Low), L(Low), H(High), VH(Very_High)}**

Figure 6 (a), (b), and (c) show the membership function to find the optimal threshold. The input values are defined as follows.

(a) False Traffic Ratio

(b) BS Hop

(c) Remaining Energy

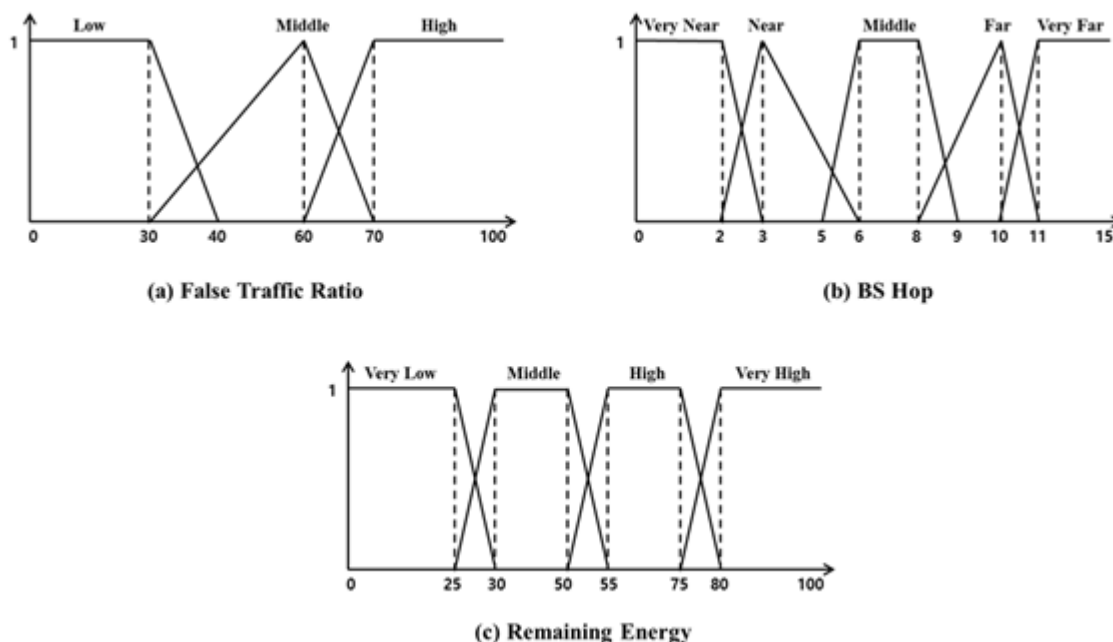Figure 6. Fuzzy membership functions

- (a) FTR: The attack rate measured per cycle, which is used to improve the filtering performance.

- (B) BS_H: The number of hops from the cluster head node to the BS. This can reduce energy consumption by considering the number of hops.

- (C) RE: This value is calculated as a percentage of the energy remaining in the node. It is used to save energy consumption and increase the node life time.

The proposed scheme adjusts the security strength and the energy consumption of the node by setting the attack rate, the energy state measured by the period, and the distance to the BS as the input value of the fuzzy system to set the new threshold value suitable for the current network situation. The new threshold and the new period are broadcast to the sensor network, as shown in Figure 5.

Table 1. Fuzzy if-then rules

rule	Input			output
No.	FTR	BS_H	RE	T
7	L	N	H	T3
17	L	VF	VL	T2

24	M	VN	VH	T2
41	M	VF	VH	T4
56	H	F	VH	T5

4. EXPERIMENTAL RESULTS

Table 2. Simulation parameters

Parameters		Value
Network Environment	Field Size	1,000 m x 1,000 m
	Number of Nodes	1,000
	Cluster Head Nodes	100
	Number of Events (Discrete Occur)	1,000
	Node Transmit Range	100–150 m
Transmit Size	Report Size	25 + MAC Size
	MAC Size	1 byte
	CH Node Info Size	2 byte
Energy Consumption	Transmit	16.25 µJ (per 1byte)
	Receive	12.5 µJ (per 1byte)
	Report Generation	70 µJ
	MAC Generation	15 µJ
	Verification	75 µJ
Security Value	SEF Threshold Value	2-6
	Key Number Per Node	1
	Global Key Pool Size	50

In this section, we compared the performance of the SEF with the fuzzy update period through experiments. Table 2 shows the parameter values for the experiment. The node information was created based on the Micaz model [12]. The report size depends on the threshold value. The reason why the threshold value starts from 2 is that if the threshold value is 1, even if only one node is damaged, a complete false report can be made. If the false report threshold is 1, the BS cannot filter the false report. The threshold is updated every cycle and is determined by the fuzzy rule. The global key pool size is 50 and 5 partitions are used. Events occur 1,000 times at random locations.
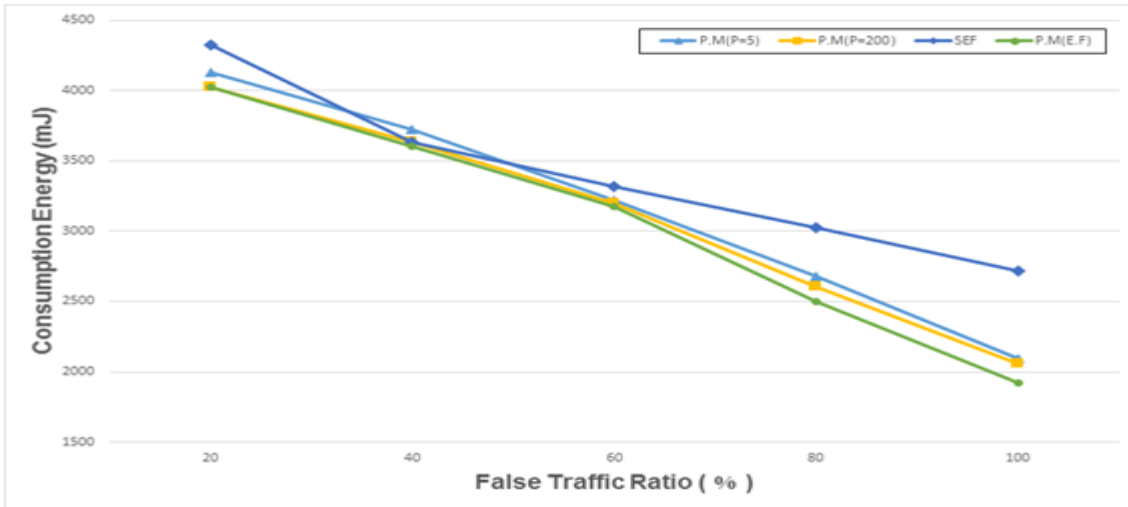

Figure 7. Energy consumption as a function of the FTR

Figure 7 shows the energy consumption of the FTR and fuzzy logic according to the threshold update period. If P is 200, it means that the threshold value is adjusted every 200 events.
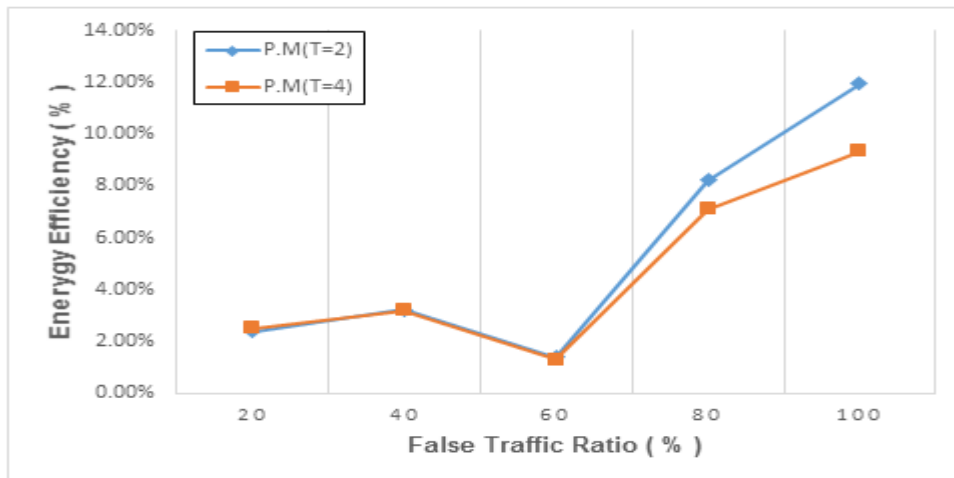

Figure 8. Increased energy efficiency with optimal cycles

Figure 8 shows the graph of the energy efficiency comparison with the optimum cycles. When the thresholds are 2 and 4, the energy efficiency improved by up to 11.96% and 9.36%, respectively. If the user applies the proposed technique in an area where the attack is high, it helps to save energy.

5. CONCLUSIONS

WSN is vulnerable to false report injection attacks because nodes are exposed to the open environment. To solve this problem, Fan Ye et al. proposed a SEF scheme that performs en-route filtering using a key. In statistical filtering techniques, thresholds affect energy management. Although research has been conducted to establish thresholds appropriate to the environment, energy management is adversely affected if the cycle is set incorrectly because the threshold update period is not taken into consideration. In this paper, we proposed a method of updating the threshold value through the evaluation function to update the appropriate period of the threshold value suitable for the network environment. The experimental results show that the energy efficiency increased by 11.96% with the optimum cycles.

REFERENCES

[1]   Reejamol, K. J., and P. Dhanya Raj. "Hole handling techniques in wireless sensor networks: A survey." Computational Intelligence and Computing Research (ICCIC), 2016 IEEE International Conference on. IEEE, (2016)

[2]   Nam, Su Man, and Tae Ho Cho. "A fuzzy rule-based path configuration method for LEAP in sensor networks." Ad Hoc Networks 31 (2015)

[3]   Sen, Soumita, Chandreyee Chowdhury, and Sarmistha Neogy. "Design of cluster-chain based WSN for energy efficiency." Applied and Theoretical Computing and Communication Technology (iCATccT), 2016 2nd International Conference on. IEEE, (2016)

[4]   Winkler, Thomas, and Bernhard Rinner. "Security and privacy protection in visual sensor networks: A survey." ACM Computing Surveys (CSUR) 47.1 (2014)

[5]   Gupta, Pallavi, Vinay Prakash, and Preetam Suman. "Noticeable key points and issues of sensor deployment for large area Wireless Sensor Network: A survey." System Modeling & Advancement in Research Trends (SMART), International Conference. IEEE, (2016)

[6]   Alanwar, Amr, et al. "PrOLoc: resilient localization with private observers using partial homomorphic encryption: demo abstract." Proceedings of the 16th ACM/IEEE International Conference on Information Processing in Sensor Networks. ACM, (2017)

[7]   F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," Selected Areas in Communications, IEEE Journal on, vol. 23, pp. 839-850, (2005)

[8]   Kim, Cho. "Determination Method of Security Threshold using Fuzzy Logic for Statistical Filtering based Sensor Networks." Journal of the Korea Society for Simulation 16.2 27-35 (2007)

[9]   Ahn, Cho. "A Correlation Analysis of the MAC Length in Statistical En-route Filtering based WSNS." International Journal of Advanced Research(IJAR) 4.8 (2016).

[10] Sahul, Ashwani, Bindiya, and Gursewak "Location Based-Balanced Clustering Algorithm for Wireless Sensor Network." International conference on Signal Processing, Communication, Power and Embedded System (SCOPES) (2016)

[11] Babuška, Robert. "Fuzzy systems, modeling and identification." Delft University of Technology, Department of Electrical Engineering Control Laboratory, Mekelweg 4 (1996).

[12] Quwaider, Muhannad. "Real-time intruder surveillance using low-cost remote wireless sensors." Information and Communication Systems (ICICS), 2017 8th International Conference on. IEEE, (2017)

AUTHORS

Jung Sub Ahn received a B.S. degree in Computer Engineering from Kyunil University in 2016 and is currently pursuing an M.S. degree in the Department of Electrical and Computer Engineering from Sungkyunkwan University.

Tea Ho Cho received a Ph.D. degree in Electrical and Computer Engineering from the University of Arizona, USA, in 1993, and B.S. and M.S. degrees in Electrical and Computer Engineering from Sungkyunkwan University, Republic of Korea, and the University of Alabama, USA, respectively. He is currently a professor at the College of Information and Communication Engineering, Sungkyunkwan University, Korea.

INTENTIONAL BLANK

A COHESION BASED FRIEND RECOMMENDATION SYSTEM

Shamsu Shehu

Al-qalam University, Katsina, Nigeria

ABSTRACT

Social network sites have attracted millions of users with the social revolution in Web2.0. A social network is composed by communities of individuals or organizations that are connected by a common interest. Online social networking sites like Twitter, Facebook and Orkut are among the most visited sites in the Internet chew, (2008). In the social network sites, a user can register other users as friends and enjoy communication. However, the large amount of online users and their diverse and dynamic interests possess great challenges to support such a novel feature in online social networks kwon, (2010). In this work, we design a general friend recommendation framework based on cohesion after analyzing the current method of friend recommendation. The main idea of the proposed method is consisted of the following stages- measuring the link strength in a network and find out possible link on this network that is yet to be established; detecting communities among the network using modularity and recommending friends. Considering the noticeable attraction of users to social networking sites, lots of research has been carried out to take advantage of the users 'information available in these sites. Knowledge mining techniques have been developed in order to extract valuable pieces of information from the users' activities. This paper deals with a methodology to generate a social graph of users' actions and predict the future social activities of the users based upon the existing relationships. This graph is updated dynamically based on the changes in the selected social network. The forecasting performed is based upon some predefined rules applied on the graph.

1. INTRODUCTION

Social Networking Sites (SNS) are the dominating entities in the modern web Hassan, (2006) Online friendship is now similarly appealing to people as offline friendship if not more. People tend to enjoy the fellowship of their real life friends in a virtual world. At the same time they are interested in making online friends. But With the rapid growth of SNS's resulting in information overload people are in dilemmas to choose the right friend and rightly so. Potential choice of friends is influenced by many intrinsic as well as exogenous factors with respect to SNS's. And with the invent of all types of virtual communication tools it is becoming more unpredictable who will like whom. This is of more importance to search engine companies and SNS's because the increase of people of similar minds expedites the probability of buying similar products. Hence Product advertisement which is the driving force of modern e-commerce gets easier Hashima, (2006). The recent surge of research in recommendation algorithms is therefore not surprising. Popular movie recommendation site Netflix (www.netflix.com) had even conducted competition with $ 1M grand prize for a 10% improvement on their movie recommendation algorithm Silva, (2010).However, recommendation of products and recommendation of human beings areas

disparate as can be. Historically there has been two main recommendation algorithms content based and collaborative algorithm. Content based algorithm requires textual information as its name suggests and recommends websites newspaper articles and other contents. Collaborative based algorithm recommends products to a user which it believe shave been light by similar users. Both of these algorithms have yielded unsatisfactory results in friend recommendation because of their lack of intuition in judging rational beings.

In the last few years, social networks have been increasing in both size and services. Social networking services (SNSs) such as Facebook, MySpace, Twitter, Flickr, YouTube and Orkut are growing in popularity and importance and to some extent they are also contributing to a change in human social behavior Salim, (2003). Online social friends are more influencing and people are now eager to make friendship with their same mentality. As the size is growing, it is very difficult to find out good friends and sometimes the user gets negative result. So the user of this social networking site expects that the system administrator will help them by friend recommendation system. Many researches are going on this point to find out recommendation system on various ways. We also try to improve the recommendation system on the basis of cohesiveness of friendship.

2.1 Social Networking

With the advent of Web 2.0, social computing has emerged as one of the hot research topics recently. It involves the collecting, extracting, accessing, processing, computing and visualizing of social signals and information. SNSs are an online phenomenon which provides social network based services to support easy message posting, information sharing and inter-friend communication Guy, (2009).SNA has its origins in both social science and in the broader fields of network Analysis and graph theory. Network analysis concerns itself with the formulation and solution of problems that have a network structure; such structure is usually captured in a graph. Graph theory provides a set of abstract concepts and methods for the analysis of graphs.

A social network is a set of people or groups of people with some pattern of contacts or interactions between them Dominic, (2010). The patterns of friendships between individuals, business relationships between companies, and intermarriages between families are all examples of networks that have been studied in the past. Social Network Sites are defined as web-based services that allow individuals to(1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system Dumas, (2003). Social Networking sites(SNS's) provide users with opportunity to connect with their offline friends as well as making new friends with latent ties who otherwise would never have met them. They also supplement their relationships with close relations and help to maintain the social capital Kim, (2010). People tend to trust the opinions of friends they know rather than the opinions of strangers.

2.2 Key Terminologies of Social Network

As social networking sites like facebook, twitter, google plus etc are getting popular day by day, social networking analysis are becoming an important subject for the researcher. There are some basic terminologies in social networking analysis. Some of them are discussed below.

Vertex (pl. vertices): The fundamental unit of a network, also called a site(physics), anode (computer science), or an actor (sociology).

Edge: The line connecting two vertices. Also called a bond (physics), a link (computer science), or a tie (sociology).

Directed/undirected Edge: An edge is directed if it runs in only one direction (such as a one-way road between two points), and undirected if it runs in both directions. Directed edges, which are sometimes called arcs, can be thought of as sporting arrows indicating their orientation. A graph is directed if all of its edges are directed. An undirected graph can be represented by a directed one having two edges between each pair of connected vertices, one in each direction.

Degree: The number of edges connected to a vertex. Note that the degree is not necessarily equal to the number of vertices adjacent to a vertex, since there may be more than one edge between any two vertices. In a few recent articles, the degree is referred to as the \connectivity" of a vertex, but we avoid this usage because the word connectivity already has another meaning in graph theory. A directed graph has both an in-degree and an out-degree for each vertex, which are the numbers of in-coming and out-going edges respectively.

Diameter: The diameter of a network is the length (in number of edges) of the longest geodesic path between any two vertices. A few authors have also used this term to mean the average geodesic distance in a graph, although strictly the two quantities are quite distinct.

Degree centrality: A node's (in-) or (out-) degree is the number of links that lead into or out of the node. In an undirected graph they are of course identical. Often used as measure of a node's degree of connectedness and hence also influence and/or popularity
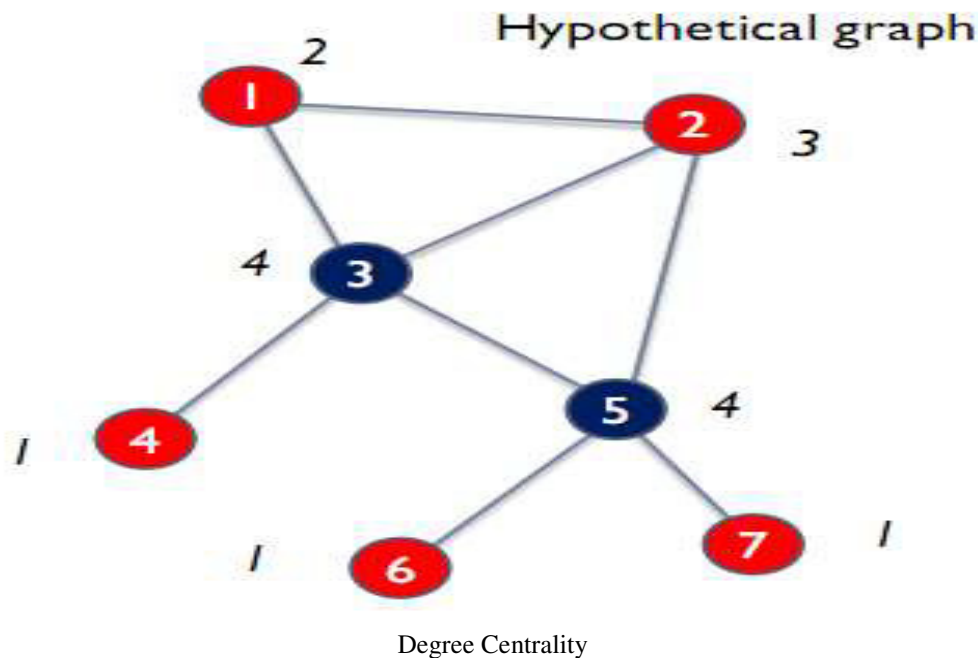
Degree Centrality

It is useful in assessing which nodes are central with respect to spreading information and influencing others in their immediate _neighborhood'.

Betweeness centrality: The number of shortest paths that pass through a node divided by all shortest paths in the network. It shows which nodes are more likely to be in communication paths between other nodes. It is also useful in determining points where the network would break apart.
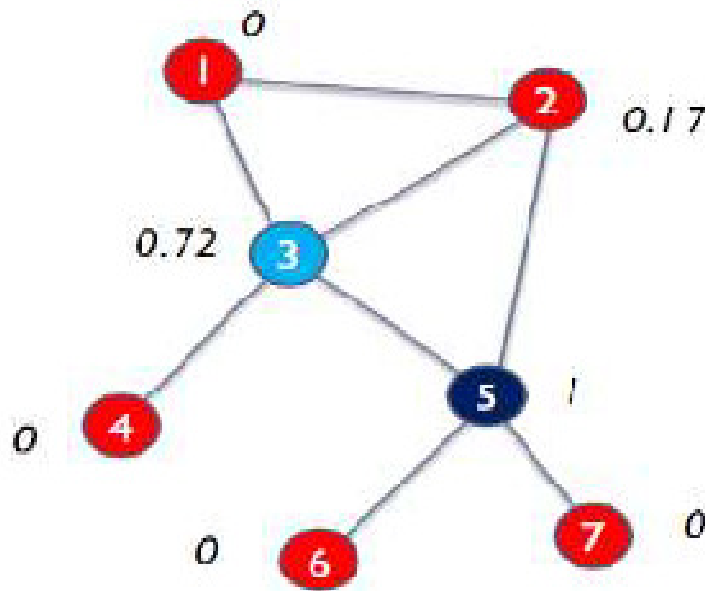
Betweeness centrality

Closeness centrality: The mean length of all shortest paths from a node to all other nodes in the network It is a measure of reach, i.e. how long it will take to reach other nodes from a given starting node.

3. RECOMMENDER SYSTEM

Over the last decade, Recommender Systems became an important research area to find out new approaches of recommendation both in industry and academia. The interesting this area still remains high because of the abundance of practical applications that help users to deal with information overload and provide personalized recommendations, content and services to them. Recommender systems can be traced back to the extensive work in the cognitive science, approximation theory, information retrieval, forecasting theories, and also have links to management science, and also to the consumer choice modeling in marketing. Recommender systems or recommendation systems are a subclass of information filtering system that seek to predict the 'rating' or 'preference' that a user would give to an item (such as music, books, or movies) or social element (e.g. people or groups) they had not yet considered, using a model built from the characteristics of an item or the user's social environment. The recommendation problem can be formulated as follows: Let C be the set of all users and let S be the set of all possible items

that can be recommended, such as books, movies, or friends. Let u be a utility function that measures usefulness of item s to user c, i.e. u :$C \times S \rightarrow R$,

Where R is a totally ordered set (non-negative integers or real numbers within a certainrange). Then for each user c ∈C, we want to choose such item s′ ∈ S that maximizes theuser's utility. More formally:

∀c∈ C, s ′c = arg max u(c, s)

In recommender systems the utility of an item is usually represented by a rating,which indicates how a particular user liked a particular item Chaoji, (2006).Generally Recommender systems are divided into two categories.

- Content-based recommendations: the user is recommended items similar to theones the user preferred in the past

- Collaborative recommendations: the user is recommended items that people withsimilar tastes and preferences liked in the past

3.1 Content-based filtering methods are based on information about and characteristics of the items that are going to be recommended. In other words, these algorithms try to recommend items that are similar to those that a user liked in the past(or is examining in the present). In particular, various candidate items are compared with items previously rated by the user and the best-matching items are recommended. The system creates a content-based profile of users based on a weighted vector of item features. The weights denote the importance of each feature to the user and can be computed from individually rated content vectors using a variety of techniques. Simple approaches use the average values of the rated item vector while other sophisticated Methods use machine learning techniques such as Bayesian Classifiers, cluster analysis, decision trees, and artificial neural networks in order to estimate the probability that the user is going to like the item. Content-based approach to recommendation has its roots in information retrieval and information filtering research. Because of the significant and early advancements made by the information retrieval and filtering communities and because of the importance of several text-based applications, many current content-based systems focus on recommending items containing textual information, such as documents, Web sites(URLs), and Usenet news messages. Info finder Abe, (2006) and News weeder Cavalcanti, (2006) are some examples of content-based model. Content-based approach has some limitations like the following:

Limited content analysis: The content must either be in a form that can be parsed automatically by a computer (e.g., text), or the features should be assigned to items manually. Another problem with limited content analysis is that, if two different items are represented by the same set of features, they are indistinguishable. Therefore, since text based documents are usually represented by their most important keywords, content based systems cannot distinguish between a well-written article and a badly written one, if they happen to use the same terms.

Over-specialization: The system can only recommend items that score highly against a user's profile; the user is limited to being recommended items similar to those already rated.

New User Problem: user has to rate a sufficient number of items before a content based recommender system can really understand user's preferences and present the user with reliable recommendations. Therefore, a new user, having very few ratings, would not be able to get accurate recommendations.

3.2 Collaborative Filtering models recommend new items based on previous transactions as well as preference of similar users Anderson, (2007). This method collect and analyze a large amount of information on users' behaviors, activities or preferences and predicting what users will like based on their similarity to other users. User-based collaborative filtering attempts to model the social process of asking a friend for a recommendation. A key advantage of the collaborative filtering approach is that it does not rely on machine analyzable content and therefore it is capable of accurately recommending complex items such as movies without requiring an "understanding" of the item itself. Collaborative filtering is mainly divided in two categories: memory-based and model-based collaborative algorithms Dumas, (2003). The entire user-product database is used in memory-based algorithms to make a prediction while the model-based algorithm first generates a model of ratings and then predict. Though this approach has demonstrated its usefulness in many applications, it still has limitations that includes,

New user problem: The system must first learn the user's preferences from the ratings that the user makes.

New item problem: New items are added regularly to recommender systems. Collaborative systems rely solely on users 'preferences to make recommendations. Therefore, until the new item is rated by a substantial number of users, the recommender system would not be able to recommend it.

Sparsity: The number of ratings already obtained is usually very small compared to the number of ratings that need to be predicted. Effective prediction of ratings from a small number of examples is important. Also, the success of the collaborative recommender system depends on the availability of a critical mass of us. There are some **hybrid models** also where content-based and collaborative-based models have been unified to compromise their shortcomings Wolfgang, (2007). They use components like linear combination of predicted ratings, various voting schemes, incorporating one component as a part of the heuristic for the other. For example, H. Kashima & N. Abe, 2006 uses hybrid recommendation system.

3.4 Friend Recommendation System

With the rapid growth of social networks, users of SNSs may easily get overwhelmed by the excessive volume of information. The friendship can significantly affect the quality of recommendations. Therefore, the recommendation of better friend is the essential factor of social network sites to find truly valuable information. There are many friend recommendation systems for social networking sites. Topological characteristics of Social networks have been well researched [13, 14] while the theoretical research of complex systems has also grown Dominic, P. D. D., & Jati, H. (2010,). Silva, N., Tsang, defined the link prediction problem as given a snapshot of a social network at time t, predicting the edges that will be added to the network during the time interval

Silva, (2010) introduced a new clustering index and user calibration procedure with Genetic Algorithm to suggest friends. Knowledge of the structure and topology of these complex networks combined with quantitative properties such as size, density, average path length or cluster coefficient is used in this approach. Albeit a topology based approach, the innovative approach towards this problem certainly opened a new possibility. Balfanz, D(2008) proposed the SCAN method to find potential cohesive subgroups which can be used further to friend recommendation. This method was invented in a social hypertext context.

Moreover, Graph based features have also been used in proposing efficient friend recommendation system. L. Katz (2006)proposed WMR- a graph based friend recommendation algorithm. They show weighted minimum-message ratio (WMR) which generates a limited, ordered and personalized friend lists by the real message interaction number among web members. In Collaborative and Structural recommendation of friends Liben-Nowel, (2003) uses the link structure of a social network and content-based recommendation using mutual declared interests. They investigate the problem of link recommendation in such weblog-based social networks and describe an annotated graph-based representation for such networks. It uses graph feature analysis to recommend links (u, v) given structural features of individual vertices and joint features of the start and end points of a candidate link, such as distance between them. Spiritual and Social context was used by Kwon (2010) to propose a method that measures friendship strength and then suggests friends from a list. The main idea of the proposed method is consisted of the following three stages; (1) computing the friendships core using physical context; (2) computing the friendship score using social context; (3)combining all of the friendship scores and recommending friends by the scoring values.

Proposed System

In the previous chapter, we have extensively discussed about the existing friend recommendation system. We have tried to find out the problems of that system and gain a lot of information about social networking and friend recommendation. After analyzing those, we also try to make a new system for suggesting friends in social networking sites. In this section, we present our proposed friendship algorithm based on cohesion

Cohesion in Social Community

Cohesion is an abstract term that is easy to grab by intuition but surprisingly difficult to define in a strict manner. Informally cohesion is the sum of all the factors that attract people to join or to be part of a group. Cohesion refers to the degree to which the elements of a module belong together. Modules with high cohesion tend to be preferable because high cohesion is associated with several desirable traits of software including robustness, reliability, reusability, and understandability whereas low cohesion is associated with undesirable traits such as being difficult to maintain, difficult to test, difficult to reuse, and even difficult to understand. In Social Networking, Cohesion is defined in a connected network and it is considered that network with high degree connectedness is more cohesive. Cohesion is an integral part of physical community and it is assumed that cohesion will have the same impact on social networking. So the impact of the cohesion cannot be ignored in online social networking and it is very effective term to recommending friends for a person in social networking sites. From the definition we can see that cohesion can be thought of two parameters. One is connectedness and another is density. Whenever this parameter comes, the term modularity is suitable to explain cohesion. Because

modularity is one measure of the structure of networks or graphs. It was designed to measure the strength of division of a network into modules (also called groups, clusters or communities). Networks with high modularity have dense connections between the nodes within modules but sparse connections between nodes in different modules. Modularity is used for detecting community structure in networks with strong cohesion. We have also used this method to finding out cohesive communities in networks for recommending friends.

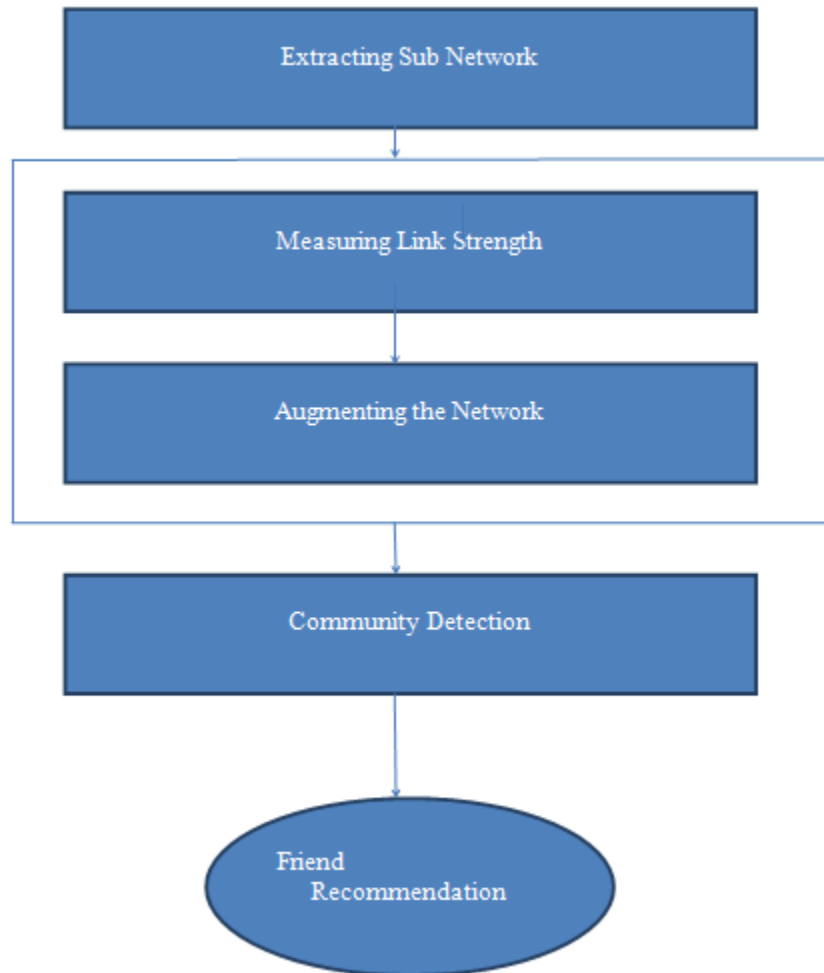## Frame Work of proposed approach

Figure: A Framework of proposed friend recommendation system

4. DETAIL EXPLANATION OF PROPOSED SYSTEM

Extracting Sub-network

Social Networking sites are very large entity with its size. Day by day the size of the network is increasing and as the people are joining there is huge number of information overload happens on those sites

For experiment of our proposed system, we take the whole network of a random individual. After getting the whole network of a client for who are going to suggest friends, we extract the sub-network of _x' people from the visualized graph.

Measuring Link Strength

This is an important step of our proposed friend recommendation system. In this step we first collect data from the users of the extracted graph and requested them to provide our desired data of mutual friend, group information and application use. For measuring the link strength between to users, we will consider these three parameters.

A. **Mutual Friend**: Mutual friend means common friend. In the social networking sites, as there are several common friends between the users. The traditional social networking sites mainly use this _mutual friend' information to suggest friend. Formally, we can define mutual friend as like, w is a mutual friend of u and v, if and only if w is friends to both u and v.

mathematically, **Mutual (u,v,w) I ff f (u, w)/\f (v,w)**

B. **Group:** In social networking we can see that there are many types of groups for different purposes. People join these groups whenever they feel important on that. Sometimes for professional, ideological and academic reasons people join these group that should count bin calculating the strength between the links/.

C. **Application use:** People join these type of social network not only for interaction but also they want to get interesting things that can make their time enjoyable. So this social networking sites always try to introduce different application that user can get interest. It is observable that people are using this type of application very frequently.

Formula of measuring link strength with example

We measure the link strength of a client node T and any node Friend T1 by the following rules-

Link $_{strength}$(T, T1) = Weight$_1$ * f1 (T, T1) + Weight$_2$ * f$_2$ + Weight$_3$ * F$_3$ (T, T1) b

Where,

F1 (T, T1) = Number of mutual friends/ Total friends of T

F2 (T, T1) = Number of groups both have joined/ Total groups joined by T

F3 (T, T1) = Number of same apps both use/ Total apps used by T

Weight$_1$ (mutual firend) = 0.5; Weight$_2$ (group) = 0.3; Weight$_3$ (App use) = 0.2

The weights for different parameters have set empirically

Example: subject A has 7 mutual friends with subject B. There are 3 groups where they both have joined and 4 apps they both use. And the total number of friends of A is 12.

The total group joined by A is 5 while A used a Total number of 6 applications.

So, the link strength between A to B can be easily calculated using the rules specified earlier

$\text{Link}_{\text{strength}}(A, B) = 0.5 * \frac{7}{15} + 0.3 * \frac{3}{5} + 0.2 * \frac{4}{6} = 0.546$

Augmenting the Network

After measuring the link strength, we augment the network with links between people that we think can happen but not present in the network. To consider possible links for a client T, we will only take into account his 'friends of friends', thereby creating triads, increasing clustering co-efficient. To determine whether a link can happen, we have used the 'Lenient Conjecture' rule.

Lenient Conjecture rule:

For a client T, a link between him and his friend of friend T2 can happen if

$\frac{Link_{strength}(T,T_2) + Link_{strength}(T_2,T)}{2} >$ Threshold

Where,

Threshold $= \frac{\sum_{i=0}^{n} Existing\ Link_{strength\ (i)}\ for\ T}{n}$

Explanation of 'Linient Conjecture' rule:

Let, subject A is friend with Subject B & C. hence, Subject A's Threshold to be friend with another node. So the threshold of A can be calculated by this rule

Threshold $= \frac{Link_{strength}(A,B) + Link_{strength}(A,C)}{2} = (0.561 + 0.588)/2 = 0.5745$

Now, let, subject D is a friend of subject A. for D have to be A' is friend the following condition must be true-

$\frac{Link_{strength}(A,D) + Link_{strength}(D,A)}{2} >$ Threshold

But here, (0.478+ 0.4125)/2 > 0.5745. 0.442 is not greater than 0.5745. so the link between A and D is not possible and we will not augment this connection.

Community Detection & Friend recommendation:

In the study of networks, such as social networks a number of different characteristics have been found to occur commonly, including the small-world property, heavy-tailed degree distributions, and clustering, among others. Another common characteristic is community structure. In the context of networks, community structure refers to the occurrence of groups of nodes in a network that are more densely connected internally than with the rest of the network.

In this step of our proposed system, we detect community in the social networks using the state-of-the-art "Louvaine Method'. This method uses modularity and link strength to detect the community among the networks.

The Louvain method is a simple, efficient and easy-to-implement method for identifying communities in large networks. The method unveils hierarchies of communities and allows to zoom within communities to discover sub-communities, sub-sub-communities, etc. it is today one of the most widely used method for detecting communities in large networks.

The method is a greedy optimization method that attempts to optimize the "modularity" of a partition of the network. The optimization is performed in two steps. First, the method looks for "small" communities by optimizing modularity locally. Second, it aggregates nodes belonging to the same community and builds a new network whose nodes are the communities. These steps are repeated iteratively until a maximum of modularity is attained and a hierarchy of communities is produced.

After detecting community, we will recommend a client people from same communities who are yet to be friends. Also, also for people already friends with all of their neighbors in the same community, we have recommended them with people with the highest $Link_{strength}$ from other communities.

5. EXPERIMENT AND RESULT ANALYSIS

5.1 Experiment Details

We experiment our whole proposed system based on the popular social networking site Face book. For extraction of the sub-network, we took the whole Face book network of a random individual and visualize it with industrial-Strength research tool Gephi 0.8.1. Then, we cut off a random sub-network of 10 people.
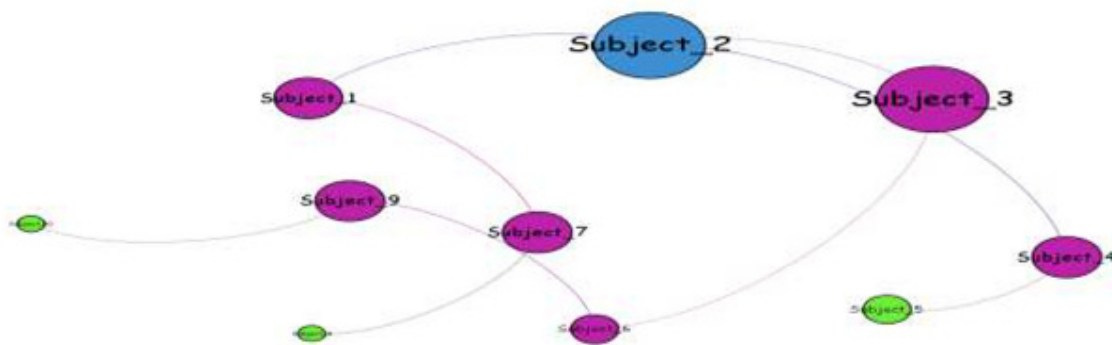

Figure: Extracted sub-network of 10 people

After extraction of sub-network of 10 people we use the roster method to collect our desired data that is needed to calculate link strength. We requested each member of the network to provide the information of mutual friend, groups and application use.

Some of the data of Subject _2 is shown on the following table.

Table: Data for calculating link strength

Connection	Mutual friend	Total friend	Same group	Total group	Same App. Use	Total App. Use
Subject – 2- Subject – 3	8	20	3	8	2	10
Subject – 2- Subject _ 4	4	20	2	8	4	10
Subject _ 2 Subject _ 1	9	20	3	8	2	10
Subject _ 2- Subject _ 9	9	20	5	8	1	10

After collecting data from each users of the network, using perl scripts we calculate the link strength of the connection between existing links. Then we got the result between different links. Some of the results are shown below:

Table: Link Measurement result

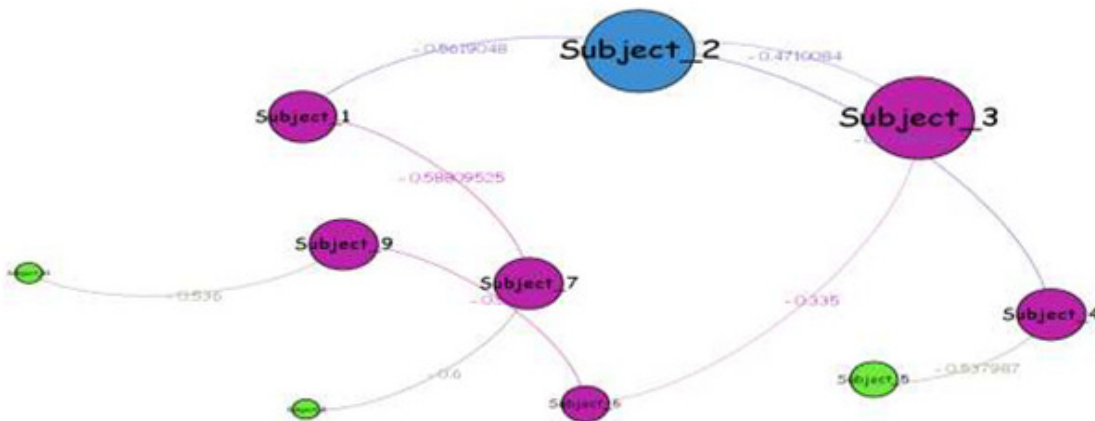|	
Subject _1- Subject_2	0.561904761904762 b
Subject_2- Subject_ 3	0.471008403361344
Subject_3 – Subject _ 6	0.335
Subject _6- Subject s_ 9	0.575238095238095
Subject_9- Subject_10	0.536134453781513
Subject_1- Subject_7	0.588095238095238

Figure: Link strength connection

After that we augment the network that means we create some connections between different nodes (people) that are not present in the network but yet they can be friend of each other. In case of augmenting the network we do not randomly create a connection. We use the lenient

conjecture rule that check the possibility of link creation between too connections. For the calculations we took the link strength is greater than the Threshold value then we will create connection and augment the network. If the link strength is less than the threshold value, we do not recommend those links. Some of the results are shown in the following table.

Link	Strength	Strength2	Avg. Between link	Threshold	Link Possibility
Subject_1-Subject_3	0.561	0.588	0.578	0.4875	Possible
Subject_1-Subject_4	0.1041	0.114	0.1091	0.165	Not possible
Subject_1-Subject_8	0.471	0.527	0.678	0.703	Not possible
Subject_2-	0.471	0.527	0.678	0..334	Possible

After that getting the augmented network, we applied the state-of-the-art louvaine method that is a simple, efficient and easy-to-implement method for identifying communities in large network. This louvaine method is implemented in different social networking tools. Gephi is one of the tolls we used to implement the louvaine method to detect community.
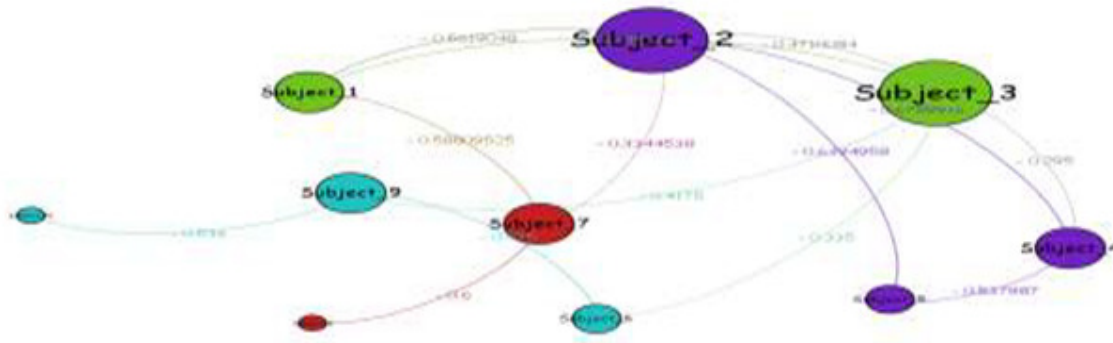

Figure: Community Detection

Using the Gephi tool we detect the community in the networking the figure the same color consist of same community. Then finally we recommend friends within the same community those are yet to be friends. In the time of recommending friends, we check link strength where the link strength is so high they are more cohesive and very good possibility to become friends.

5.2 Result Analysis

We have analyzed out result with the use acceptance value and find out the percentage of success. We have also analyses our system using any of the one parameter (mutual friend, group, application use and got the following result.

	Mutual friend	Group	App use	All three parameters together
Community Detected	3	5	3	4
Recommended	8	4	7	14
Accepted	5	3	4	10
Acceptance Rate	62.5%	75%	57.14%	71.422%

From the result we can see that if we use only the mutual friend that means the trivial FOF (friend of friend) system then the acceptance rate is less than if we use also group and application use parameter. Though we have experimented our system with a small sub-network because of the unavailability of social networking data, but according to the definition of cohesiveness it is expected that with the combination of this three parameters, the calculation of link strength and recommending friends will be better.
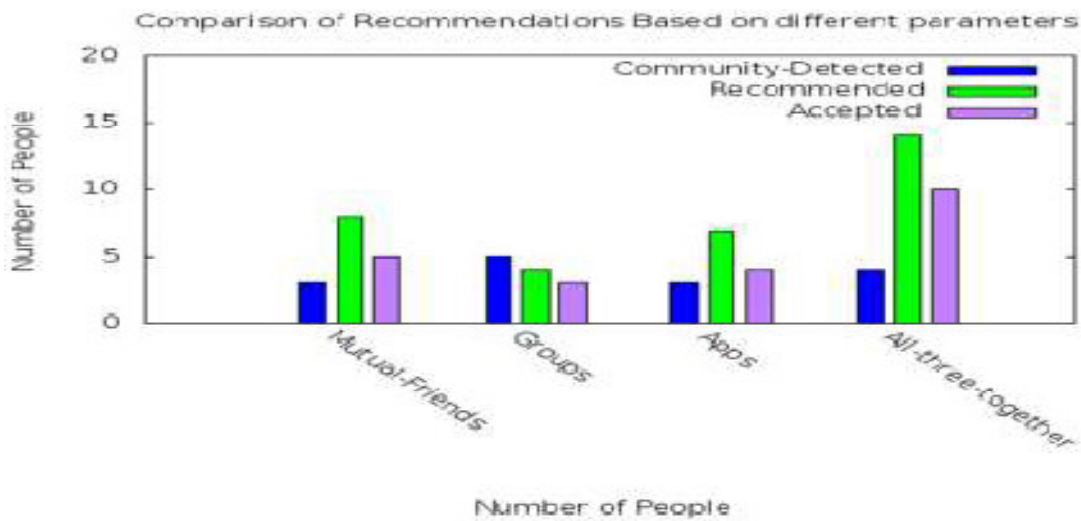

Figure: Result analysis

6. CONCLUSION AND FUTURE WORK

With the revolution of web 2.0, social Networking Sites are getting popularity increasingly. People are joining in those sites to share their views to online friends like their real life friends. For this reason, the size and information of these sites are increasingly day by day. Users of these sites hope that the system administrator will provide them recommendation system to make friends. But the recommendation system of human being is not same as the product recommendation as the psychology of human being is different for every person. After realizing this issue, we review the existing system of friend recommendation system in SNSs. And we find that cohesion can be a good measurement in case of social networking recommendation system. So we are proposing this cohesion based friend recommendation system. We hope that this frame work of recommendation system will improve the quality of friend suggestion and will help user to social networking sites.

Though social networking is now so famous and not that much research has conducted so there are vast scopes to find technique and upgrade the system. For future work, it is important to test the proposed mechanism more intensively in a larger algorithm of friend recommender system. There is also scope on work not to recommend a possible good recommendation a bad one. If the system recommends some people who are not at all related to the user then the user might lose their faith from the sites.

The work we have done can be extended in future. There is a huge scope to improvise this technique a friend recommendation is a new research area and create an application on the proposed system. We have used modularity which has the resolution limit so sometimes it cannot detect small communities in a network. Also using unique parameters, we can improve the robustness of the link strength of the network. We have used a sub-network as our experiment it is extensible to larger network to find out the perfect result of the recommendation system and using a working application.

REFERENCES

[1] Liben-Nowel, D., And Kleinberg, J, "The Link prediction problem for social networks," Proceedings of the twelfth international conference on Information and knowledge management, pp 556-559. 2003.

[2] Guy, I., Ronen I., and Wilcox E. "Do you know? Recommending people to invite into your social network" Proc. IUI pp. 77-86. 2009.

[3] Kwon, J. and Kim, S. "Friend Recommendation Method using Physical and social Context". IJCSNS International of Computer Science and network security, VOL. 10 No.11, November 2010.

[4] Wolfgang Woerndl and Georg Grog, "Utilizing Physical and Social Context to Improve Recommender systems". In WI- IATW 'o7: Proceedings of the 2007 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology – Workshops, pp. 123-128, 2007.

[5] M. Hasan, V. Chaoji, S. Slem, and M. Zaki. "Link Prediction using supervised learning." In Workshop on Link Analysis, Counterterrorism and Security (SDM), 2006.

[6] H. Kashima and N. Abe. "A parameterized probabilistic model of network evolution for supervised link prediction." In ICDM '06, 2006.

[7] L. Katz. "A new ststus index derived from sociometric analysis." Psychometrika, 18:39-43,1953.

[8] Silva, N.,Tsang, I., Cavalcanti, G., and Tsang, I." A Graph-Based Friend recommendation System Using Genetic Algorith". WCCI 2010 IEEE World Congress on Computational Intellegence July, 18-23, 2010-CCIB Barcelona, Spain CEC.

[9] Chiew, T. K., & Salim, S. S. (2003). Webuse: Website usability evaluation tool. Malaysian Journal of Computer Science, 16(1), 47-57.

[10] Chew, M., Balfanz, D. & Laurie, B. 2008. (Under)mining Privacy in Social Networks

[11] Donghee Yvette Wohn, The "S" in Social Network Games: Initiating, Maintaining, and Enhancing Relationships, Michigan State University, USA, 2011.

[12] Dominic, P. D. D., & Jati, H. (2010, June). Evaluation method of Malaysian university website: Quality website using hybrid method. In Information Technology (ITSim), 2010 International Symposium in (Vol. 1, pp. 1-6). IEEE.

[13] Dumas, J. S. 2003. User-based evaluations. The human-computer interaction handbook: fundamentals, evolving technologies and emerging applications. L. Erlbaum Associates Inc

[14] Dix, A., E. Finlay, J., D. Abowd, G. & Beale, R. 2004. Human-Computer Interaction, 3rd Edition

[15] Anderson, T. & Garrison, D. R. (2007). Learning in a networked world: New roles and responsibilities. In Gibson, C. (Ed.), Distance Learners in Higher Education.

BLOCKCHAIN-BASED SMART CONTRACTS : A SYSTEMATIC MAPPING STUDY

Maher Alharby[1,2] and Aad van Moorsel[1]

[1]School of Computing Science, Newcastle University, Newcastle, UK
[2]College of Computer Science and Engineering, Taibah University,
Medina, KSA

ABSTRACT

An appealing feature of blockchain technology is smart contracts. A smart contract is executable code that runs on top of the blockchain to facilitate, execute and enforce an agreement between untrusted parties without the involvement of a trusted third party. In this paper, we conduct a systematic mapping study to collect all research that is relevant to smart contracts from a technical perspective. The aim of doing so is to identify current research topics and open challenges for future studies in smart contract research. We extract 24 papers from different scientific databases. The results show that about two thirds of the papers focus on identifying and tackling smart contract issues. Four key issues are identified, namely, codifying, security, privacy and performance issues. The rest of the papers focuses on smart contract applications or other smart contract related topics. Research gaps that need to be addressed in future studies are provided.

KEYWORDS

Blockchain, Smart contracts, Systematic mapping study, Survey

1. INTRODUCTION

Transactions between parties in current systems are usually conducted in a centralised form, which requires the involvement of a trusted third party (e.g., a bank). However, this could result in security issues (e.g., single point of failure) and high transaction fees. Blockchain technology has emerged to tackle these issues by allowing untrusted entities to interact with each other in a distributed manner without the involvement of a trusted third party. Blockchain is a distributed database that records all transactions that have ever occurred in a network. Blockchain was originally introduced for Bitcoin (a peer-to-peer digital payment system), but then evolved to be used for developing a wide range of decentralised applications. An appealing application that can be deployed on top of blockchain is smart contracts.

A smart contract is executable code that runs on the blockchain to facilitate, execute and enforce the terms of an agreement between untrusted parties. It can be thought of as a system that releases digital assets to all or some of the involved parties once the pre-defined rules have been met [1]. Compared to traditional contracts, smart contracts do not rely on a trusted third party to operate, resulting in low transaction costs. There are different blockchain platforms that can be utilised to develop smart contracts, but Ethereum is the most common one. This is because Ethereum's language supports Turing-completeness feature that allows creating more advanced and

customised contracts. Smart contracts can be applied to different applications (e.g., smart properties, e-commerce and music rights management).

The main aim of this study is to identify the research topics that have been carried out about blockchain-based smart contracts and current challenges that need to be addressed in future studies. To achieve this aim, we selected a systematic mapping study as the methodology for our study. We followed the systematic mapping process presented in [2] to search for relevant papers in scientific databases and to produce a map of current smart contract research. The produced map could help researchers identify gaps for future studies. The focus of our study is to only explore smart contract studies from a technical point of view.

The structure of this paper is as follows. Section 2 discusses background information about blockchain and smart contracts technologies. It also discusses several smart contract platforms and potential applications. Section 3 describes the research methodology adopted for our study. Section 4 presents the results of searching and screening for relevant papers and the results of classifying smart contract topics. Section 5 discusses the results and answers the research questions of the study. Section 6 concludes the paper.

2. BACKGROUND

This section presents general background information about blockchain and smart contracts technologies. It also discusses some blockchain platforms that support the development of smart contracts. Finally, it provides some potential use cases for smart contracts.

2.1. Blockchain Technology

A blockchain is a distributed database that records all transactions that have ever occurred in the blockchain network. This database is replicated and shared among the network's participants. The main feature of blockchain is that it allows untrusted participants to communicate and send transactions between each other in a secure way without the need of a trusted third party. Blockchain is an ordered list of blocks, where each block is identified by its cryptographic hash. Each block references the block that came before it, resulting in a chain of blocks. Each block consists of a set of transactions. Once a block is created and appended to the blockchain, the transactions in that block cannot be changed or reverted. This is to ensure the integrity of the transactions and to prevent double-spending problem.

Cryptocurrencies have emerged as the first generation of blockchain technology. Cryptocurrencies are basically digital currencies that are based on cryptographic techniques and peer-to-peer network. The first and most popular example of cryptocurrencies is Bitcoin. Bitcoin [3] is an electronic payment system that allows two untrusted parties to transact digital money with each other in a secure manner without going through a middleman (e.g., a bank). Transactions that occurred in the network are verified by special nodes (called miners). Verifying a transaction means checking the sender and the content of the transaction. Miners generate a new block of transactions after solving a mathematical puzzle (called Proof of Work) and then propagate that block to the network. Other nodes in the network can validate the correctness of the generated block and only build upon it if it was generated correctly. However, Bitcoin has limited programming capabilities to support complex transactions. Bitcoin, thus, does not support the creation of complex distributed applications on top of it.

Other blockchains such as Ethereum have emerged as the second generation of blockchain to allow building complex distributed applications beyond the cryptocurrencies. Smart contracts, which will be discussed in the following section, are considered as the main element of this generation [4]. Ethereum blockchain is the most popular blockchain for developing smart contracts. Ethereum is a public blockchain with a built-in Turing-complete language to allow writing any smart contract and decentralised application.

There are two types of blockchain, namely, public and private blockchain [5]. In a public blockchain, any anonymous user can join the network, read the content of the blockchain, send a new transaction or verify the correctness of the blocks. Examples of public blockchains are Bitcoin, NXT and Ethereum. In a private blockchain, only users with permissions can join the network, write or send transactions to the blockchain. A company or a group of companies are usually responsible for giving users such permissions prior to joining the network. Examples of private blockchains are Everledger, Ripple and Eris.

2.2. Smart Contracts

A smart contract is executable code that runs on the blockchain to facilitate, execute and enforce the terms of an agreement. The main aim of a smart contract is to automatically execute the terms of an agreement once the specified conditions are met. Thus, smart contracts promise low transaction fees compared to traditional systems that require a trusted third party to enforce and execute the terms of an agreement. The idea of smart contracts came from Szabo in 1994 [6]. However, the idea did not see the light till the emergence of blockchain technology. A smart contract can be thought of as a system that releases digital assets to all or some of the involved parties once arbitrary pre-defined rules have been met [1]. For instance, Alice sends X currency units to Bob, if she receives Y currency units from Carl.

Many different definitions of a smart contract have been discussed in the literature. In [7], the author classified all definitions into two categories, namely, smart contract code and smart legal contract. Smart contract code means "code that is stored, verified and executed on a blockchain" [7]. The capability of this smart contract depends entirely on the programming language used to express the contract and the features of the blockchain. Smart legal contract means code to complete or substitute legal contracts. The capability of this smart contract does not depend on the technology, but instead on legal, political and business institutions. The focus of this study will be on the first definition, which is smart contract code.
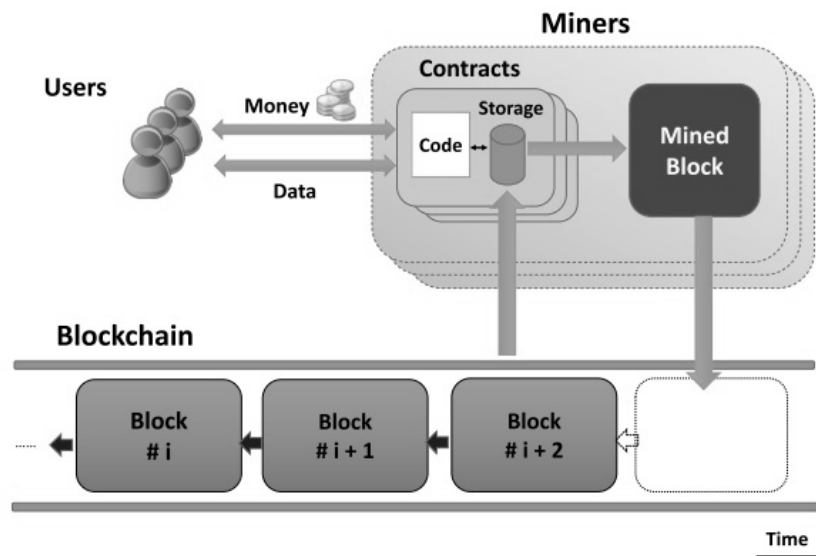

Figure 1. Smart contract system [8].

A smart contract has an account balance, a private storage and executable code. The contract's state comprises the storage and the balance of the contract. The state is stored on the blockchain and it is updated each time the contract is invoked. Figure 1 depicts the smart contract system.

Each contract will be assigned to a unique address of 20 bytes. Once the contract is deployed into the blockchain, the contract code cannot be changed. To run a contract, users can simply send a transaction to the contract's address. This transaction will then be executed by every consensus node (called miners) in the network to reach a consensus on its output. The contract's state will then be updated accordingly. The contract can, based on the transaction it receives, read/write to its private storage, store money into its account balance, send/receive messages or money from users/other contracts or even create new contracts.

There are two types of smart contracts, namely, deterministic and non-deterministic smart contracts [9]. A deterministic smart contract is a smart contract that when it is run, it does not require any information from an external party (from outside the blockchain). A non-deterministic smart contract is a contract that depends on information (called oracles or data feeds) from an external party. For example, a contract that requires the current weather information to be run, which is not available on the blockchain.

2.3. Platforms for Smart Contracts

Smart contracts can be developed and deployed in different blockchain platforms (e.g., Ethereum, Bitcoin and NXT). Different platforms offer distinctive features for developing smart contracts. Some platforms support high-level programming languages to develop smart contracts. We will only focus on three public platforms in this section.

- Bitcoin [3] is a public blockchain platform that can be used to process cryptocurrency transactions, but with a very limited compute capability. Bitcoin uses a stack-based bytecode scripting language. The ability of creating a smart contract with rich logic using Bitcoin scripting language is very limited [10]. In Bitcoin, a simple logic that requires multiple signatures to sign a single transaction before confirming the payment is possible. However, writing contracts with complex logic is not possible due to the limitations of Bitcoin scripting language. Bitcoin scripting language, for example, neither supports loops nor withdrawal limits [1]. To implement a loop, the only possible way is by repeating the code many times, which is inefficient.

- NXT is a public blockchain platform that includes built-in smart contracts as templates [10]. NXT only allows developing smart contracts using those templates. It does not, however, allow customized smart contracts due to the lack of Turing-completeness in its scripting language.

- Ethereum [1,11] is a public blockchain platform that can support advanced and customized smart contracts with the help of Turing-complete programming language. Ethereum platform can support withdrawal limits, loops, financial contracts and gambling markets. The code of Ethereum smart contracts is written in a stack-based bytecode language and executed in Ethereum Virtual Machine (EVM). Several high-level languages (e.g., Solidity, Serpent and LLL) can be used to write Ethereum smart contracts. The code of those languages can then be compiled into EVM bytecodes to be run. Ethereum currently is the most common platform for developing smart contracts.

2.4. Smart Contract Applications

There are various possible applications where smart contracts can be applied to. Some of these applications are as follows:

- Internet of Thing and smart property [12]: there are billions of nodes that are sharing data between each other through the Internet. A potential use case of blockchain-based smart contracts is to allow those nodes to share or access different digital properties without a trusted third party. There are various companies that investigate this use case. For example, Slock.it is a German company that utilises Ethereum-based smart contracts for

renting, selling or sharing anything (e.g, selling a car) without the involvement of a trusted third party.

- Music rights management [13]: a potential use case is to record the ownership rights of a music in the blockchain. A smart contract can enforce the payment for music owners once a music is used for commercial purposes. It also ensures the payment is being distributed between the music's owners. Ujo is a company that investigates the use of blockchain-based smart contracts in the music industry.

- E-commerce: a potential use case is to facilitate the trade between untrusted parties (e.g., seller and buyer) without a trusted third party. This would result in reduction of trading costs. Smart contracts can only release the payment to the seller once the buyer is satisfied with the product or service they received [14].

There are other possible applications such as e-voting, mortgage payment, digital right management, motor insurance, distributed file storage, identity management and supply chain.

3. RESEARCH METHODOLOGY

We selected the systematic mapping study presented in [2] as the research methodology for our study to explore studies related to smart contracts. The results of this systematic mapping study would allow us to identify and map research areas related to smart contracts. In addition, it would allow us to identify research gaps that need to be considered for future studies. The process for the systematic mapping study falls into five steps as depicted in Figure 2.
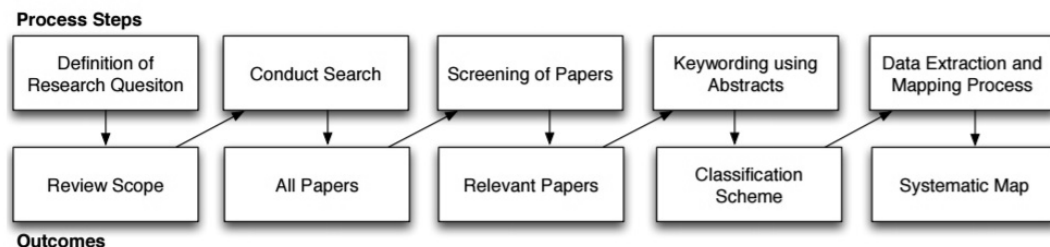

Figure 2. Steps of the systematic mapping study [2].

Definition of research questions:

This step is to identify the research questions the study is aiming to answer. For our study, we defined the following research questions:

RQ1. What are the current research topics on smart contracts?

RQ2. What are the current smart contract applications?

RQ3. What are the research gaps that need to be addressed in future studies?

Conducting the search:

This step is to search and to find all scientific papers that are related to the research topic, which is smart contracts. For our study, we decided to select the term 'smart contract' as the main keyword to search for papers. We selected this term because we wanted to narrow down the focus of our study to only cover smart contract related works. After identifying the keyword for the searching process, we selected the scientific databases to conduct our search. We selected IEEE Explore, ACM Digital Library, ScienceDirect, Springer, Ebsco and Scopus. Our focus was to only include high quality papers published in conferences, journals, workshops, symposiums and books.

Screening for relevant papers:

This step is to search for papers that are relevant to our research questions. We followed the same approach as in [15] to look for relevant papers. We first tried to exclude papers that were irrelevant to our study based on their titles. If we were unable to decide on a paper, we would go a step further by examining its abstract. We also used exclusion criteria to screen each paper. We excluded: (1) non-English papers, (2) papers without full text available, (3) papers that utilised smart contracts in fields other than computer science, (4) redundant papers and (5) articles, newsletters and grey literature.

Key-wording using abstracts:

This step is to classify all relevant papers using the key-wording technique described in [15]. We first read the abstract of each paper to identify the most important keywords and the main contribution. Those keywords were then used to classify papers into various categories. After classifying all papers, we read the papers and made changes to the classification when necessary.

Data extraction and mapping process:

This process is to gather all the required information to address the research questions of this study. We gathered different data items from each paper. These data items embrace the main aims and contributions of papers.

4. STUDY RESULTS

This section discusses the results of the systematic mapping study that we conducted on smart contracts. We first discuss the results of searching and screening for relevant papers. Then, we discuss the results of the classification process.

4.1 Searching and Screening Results

Searching and screening for relevant papers are two steps of the systematic mapping study that we discussed in Section 3. The results of these steps are as follows. In the searching phase, we looked for all papers using the term 'smart contract' in different scientific databases. We gathered 154 papers in total (as on 5 May 2017). In the screening phase, we first excluded irrelevant papers based on their titles and/or their abstracts (we excluded 109 irrelevant papers). There are two reasons why we had a high number of excluded papers. First, many papers were irrelevant to our study, since our focus was to explore smart contracts from a technical perspective. For instance, many papers discussed the topic from an economic or legal point of view. Another reason is that some excluded papers were about cryptocurrencies or blockchain in general, which do not contribute to our research questions. After that, 17 papers were removed as they were duplicates, resulting in 28 papers. Among the 28 papers, four papers were excluded as they only discuss general information about smart contract and how it works, without providing any useful contribution. Thus, we only selected 24 papers to conduct our systematic mapping study. Figure 3 summaries the results of searching and screening for relevant papers.
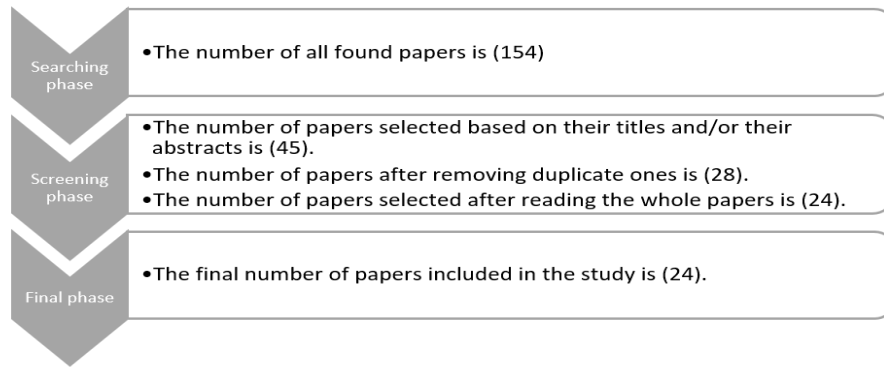
Figure 3. Searching and screening results.

4.2 Classification Results

By applying the Key-wording technique that we discussed in Section 3, we classified the papers into two categories, namely, smart contract issues and other smart contract related topics. We found about two thirds of the papers fall into smart contract issues category. We classified those issues into four categories, namely, codifying, security, privacy and performance issues. *Codifying issues* mean challenges that are related to the development of smart contracts. *Security issues* mean bugs or vulnerabilities that an adversary might utilise to launch an attack. *Privacy issues* mean issues related to disclosing contracts information to the public. *Performance issues* mean issues that affect the ability of blockchain systems to scale. Table 1 summaries the identified issues and the proposed solutions. For other smart contract related topics category, there are nine papers that developed smart contract applications or reported about other topics (e.g., the combination of smart contract and The Internet of Thing).

Table 1. Smart contract issues and the proposed solutions.

Smart contract issues		Proposed solutions
Codifying issues	Difficulty of writing correct smart contracts [8,16,17,18].	• Semi-automation of smart contracts creation [18]. • Use of formal verification methods [16,17]. • Education (e.g., online tutorials) [8].
	Inability to modify or terminate smart contracts [19].	• A set of standards for modifying/terminating smart contracts [19].
	Lack of support to identify under-optimised smart contracts [20].	• Use of 'GASPER' tool [20].
	Complexity of programming languages [21].	• Use of logic-based languages [21].
Security issues	Transaction-ordering dependency vulnerability [22,23].	• Use of 'SendIfReceived' function [22]. • Use of a guard condition [23]. • Use of 'OYENTE' tool [23].
	Timestamp dependency vulnerability [23].	• Use block number as a random seed instead of using timestamp [23]. • Use of 'OYENTE' tool [23].
	Mishandled exception vulnerability [23].	• Check the returned value [23]. • Use of 'OYENTE' tool [23].
	Re-entrancy vulnerability [23].	• Use of 'OYENTE' tool [23].

	Criminal smart contract activities [24].	• NA.
	Lack of trustworthy data feeds 'Oracles' [25].	• Use of 'Town Crier (TC)' tool [25].
Privacy issues	Lack of transactional privacy [26].	• Use of 'Hawk' tool [26]. • Use of encryption techniques [27].
	Lack of data feeds privacy [25].	• Use of 'Town Crier (TC)' tool [25]. • Use of encryption techniques [25].
Performance issues	Sequential execution of smart contracts [28].	• Parallel execution of smart contracts [28].

Codifying issues

From the literature, we found four issues that might face developers during writing smart contracts, namely, the difficulty of writing correct contracts, the inability to modify or terminate contracts, the lack of support to identify under-optimised contracts and the complexity of programming languages.

The first one is the difficulty of writing correct smart contracts [8,16,1718]. Correctness of smart contracts in this context means contracts that are functioning as intended by their developers. The reason why it is important to have correct smart contracts is because those contracts have valuable currency units [8,16]. Thus, if a smart contract was not executed as intended, some of its currency units would disappear. An example that illustrates this is the Distributed Autonomous Organisation (DAO) attack, which led to over 60 million US dollars being moved into an adversary account [23].

In an attempt to tackle this issue, three solutions were identified from the literature. The first solution is to semi-automate the creation of smart contracts [18] to ease the process of writing smart contracts. Semi-automation means the translation of human-readable contract representations to smart contract rules. The second solution is to provide developers with guidelines to aid them write correct contracts. Delmolino et al. [8], released online materials (e.g., a tutorial) to help developers write correct smart contracts. The last solution is the adoption of formal verification techniques to detect unintended behaviours of smart contracts [16,17]. This can help developers recognise those behaviours before posting their contracts to the blockchain. Bhargavan et al. [16] utilised formal methods to analyse and verify the correctness of smart contracts, while Bigi et al. [17] went a step further by combining formal methods with game theory techniques to validate smart contracts.

The second issue is the inability to modify or terminate smart contracts [19]. Due to the immutability feature of blockchain, smart contracts cannot be changed or terminated after deploying it into the blockchain. This is different from legal law which allows the rules to be modified or terminated. In an attempt to tackle this issue, Marino et al. [19] presented a set of standards to allow smart contracts to be changed or terminated. Such standards are taken from legal contracts and then defined to fit in the context of smart contracts. Those standards were then applied to Ethereum-based smart contracts to prove their success. For details about those standards and how can be applied to Ethereum-based smart contracts, we refer the reader to [19].

The third one is the lack of support to identify under-optimised smart contracts [20]. To run a smart contract, each computational or storage operation in the contract costs some money. An under-optimised smart contract is a contract that contains unnecessary or expensive operations. Such operations result in a high cost at the user's side. In an attempt to tackle this issue, Chen et al. [20] identified seven programming patterns (e.g., unnecessary and expensive operations in a loop) in smart contracts which lead to unnecessary extra costs. They also proposed ways to

enhance the optimisation of those patterns to reduce the overall cost of executing smart contracts. They proposed and developed a tool called 'GASPER' to detect contracts that suffer from those patterns. They used the tool to examine current Ethereum smart contracts and found most of them suffer from such patterns.

The last issue is the complexity of smart contract programming languages [21]. Current smart contracts are based on procedural languages such as Solidity. In a procedural language, the code is executed as a sequence of steps. Thus, programmers must specify what should be done and how to do it. This makes the task of writing smart contracts in those languages cumbersome and error prone [21]. In an attempt to tackle this issue, Idelberger et al. [21] proposed to utilise logic-based languages instead of procedural languages. In logic-based languages, programmers do not necessarily have to specify the sequence of steps for a contract. This will ease the complexity of writing smart contracts. However, algorithms for logic-based languages are expensive and inefficient.

Security issues

From the literature, we found six security issues, namely, transaction-ordering dependency, timestamp dependency, mishandled exception, criminal activities, re-entrancy and untrustworthy data feeds. In addition to these issues, Atzei et al. [29] surveyed several vulnerabilities in Ethereum smart contracts.

The first issue is transaction-ordering dependency [22,23]. This problem occurs when two dependent transactions that invoke the same contract are included in one block. The order of executing transactions relies on the miner. However, an adversary can successfully launch an attack if those transitions were not executed in the right order. For example, assume there is a puzzle contract that incentives the user who solves the puzzle. A malicious owner is listening to the solutions provided by the users. Once a user submitted a correct solution to the puzzle (Tu), the malicious owner sends a transaction (To) to update the contract's reward (e.g., reduce the reward) right away. Those two transactions (To and Tu) might be included in the same block by chance. If the miner executed To before Tu, the user would get a lower reward and the malicious owner would succeed in his attack [23]. To tackle this issue, Natoli et al.[22] suggested the use of Ethereum-based functions (e.g., SendIfReceived) to enforce the order of transactions. Similarly, Luu et al.[23] suggested using a guard condition such that "a contract code either returns the expected output or fails". A tool called 'OYENTE' developed by [23] can be used to detect contracts that are vulnerable to transaction-ordering dependency.

The second issue is timestamp dependency [23]. This problem occurs when a contract uses the block timestamp as a condition to trigger and execute transactions (e.g., sending money). For instance, a game-based contract that takes the block timestamp as a random seed to select the winner. The block timestamp is usually set as the current local time by the miner who generated the block. However, an issue with the timestamp is that a dishonest miner could vary its value by about 15 minutes from the current time, while the block is still accepted by the blockchain system. As the timestamp of a block is not guaranteed to be accurate, contracts that rely on timestamp value are vulnerable to threats by dishonest miners. To tackle this issue, Luu et al.[23] suggested using the block number as a random seed for contracts instead of using the block timestamp. This is because the value of the block number is fixed (miners cannot vary the block number value). To detect contracts that are vulnerable to timestamp dependency, 'OYENTE' tool presented in [23] can be used.

The third issue is mishandled exception vulnerability [23]. This problem occurs when a contract (caller) calls another contract (callee) without checking the value returned by the callee. When calling another contract, an exception (e.g., run out of gas) sometimes raised in the callee

contract. This exception, however, might/might not be reported to the caller depending on the construction of the call function. Having not reported an exception might lead to threats as in the KingOfTheEther (KoET) contract [23]. In KoET, an adversary might send a transaction that results in an exception in order to buy the throne from the current king for free. To tackle this issue, Luu et al.[23] highlighted the importance of checking the value returned by the callee. In the KoET example, the code can be improved to not release the throne till the payment from the adversary is completed successfully without any exception. The 'OYENTE' tool proposed by [23] can be used to detect mishandled exception vulnerability in smart contracts.

The fourth issue is re-entrancy vulnerability [23]. This problem occurs when an attacker utilises a recursive call function to conduct multiple repetitive withdrawals, while their balances are only deduced once. In June 2016, an attacker utilised the re-entrancy vulnerability in the Decentralised Autonomous Organisation (DAO) to steal over 60 million US dollars [23]. Luu et al. [23] developed a tool called 'OYENTE' to detect this vulnerability.

The fifth issue is criminal activities. Jules et al. [24] highlighted the feasibility of constructing three different types of criminal activities in smart contract systems, namely, "leakage/sale of secret documents, theft of private keys and calling-card crimes, a broad class of physical-world crimes (murder, arson, etc.)" [24]. These crimes can be implemented efficiently in the Ethereum blockchain by utilising cryptographic techniques as follows. Leakage of secret documents can be achieved with the support of Serphent (an Ethereum scripting language). Theft of private keys can be achieved using Succinct Non-interactive ARgument of Knowledge (SNARKs) cryptographic primitives. Authenticated data feeds, which is data from an external party, can facilitate the calling-card crimes. The authors of [24], however, did not attempt to tackle those crime activities, but instead, they highlighted the importance of constructing safeguards against such activities.

The last issue is the lack of trustworthy data feeds (oracles) [25]. As we explained in Section 2.2, some smart contracts require information (data feeds) from outside the blockchain. The problem is that there is no guarantee that the information provided by an external source is trustworthy. In an attempt to tackle this issue, Zhang et al. [25] built a Town Crier (TC) solution that acts as a trusted third party between external sources and smart contracts to provide authenticated data feeds for smart contracts. Figure 5 explains the architecture of TC solution. The TC solution consists of a TC contract that resides on the blockchain and a TC server that resides outside the blockchain. To send a data feeds request, a user contract can send a request to the TC contract, which will then be forwarded to the TC server. The server then communicates with external data sources via HTTPS to get the data feeds. Upon getting the required data feeds, the server will forward those feeds to the TC contract, which will then be forwarded to the user contract.
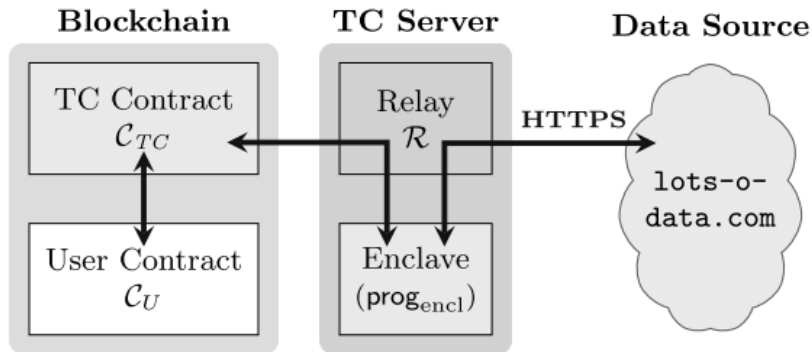

Figure 4. Architecture of TC solution [25].

Privacy issues

From the literature, we found two privacy issues, namely, the lack of transactional privacy and the lack of data feeds privacy.

The first issue is the lack of transactional privacy [26,27]. In blockchain systems, all transactions and users' balances are publicly available to be viewed. This lack of privacy could limit the adoption of smart contracts as many people consider financial transactions (e.g., stock trading) as confidential information [26]. To tackle this issue, Kosba et al.[26] built a tool called 'Hawk' that allows developers to write privacy-preserving smart contracts without the need of implementing any cryptography. The tool is responsible for compiling smart contract code to privacy-preserving one. Watanabe et al.[27] proposed to encrypt smart contracts before deploying them to the blockchain. Only participants, who are involved in a contract, can access the contract's content by using their decryption keys.

The second issue is the lack of data feeds privacy [25]. When a contract requires data feeds to operate, it sends a request to the party that provides those feeds. However, this request is exposed to the public as anyone in the blockchain can see it. To tackle this issue, Zhang et al. [25] extend their Town Crier (TC) tool to support private requests. A contract can encrypt the request using the TC's public key, before sending the request. Upon receiving the encrypted request, the TC can decrypt it using its private key. Thus, this would guarantee that the content of the request is kept secret from other users/contracts in the blockchain.

Performance issues

From the literature, we only found one performance issue, which is the sequential execution of smart contracts [28]. In blockchain systems, smart contracts are executed sequentially (e.g., one contract at a time). However, this would affect the performance of the blockchain systems negatively as the number of smart contracts that can be executed per second will be limited. With the growing number of smart contracts in the future, the blockchain systems will not be able to scale. Vukolić [28] suggested to execute smart contracts in parallel as long as they are independent (e.g., "do not update the same variables" [28]). By doing so, the performance of blockchain systems would be improved as more contracts can be executed per second.

Other topics

Apart from smart contract issues, we found nine papers from the literature that propose smart contract applications or discuss other smart contract related topics.

There are four smart contract applications proposed in the literature, namely, trading and fair exchange, identity management, Internet of Thing and agreements establishment applications. For trading and fair exchange, Bogner et al. [30] developed a smart contract application on top of the Ethereum blockchain to allow untrusted participants to share everyday objects (e.g., rent devices). For identity management, Al-Bassam et al. [31] built a system called `SCPKI' on top of the Ethereum blockchain to overcome the limitations (e.g, centralisation and lack of transparency) of the Public Key Infrastructure. This system allows entities to manage their identities in a transparent way without the involvement of a trusted third party such as central authorities. For the Internet of Thing, Huh et al. [32] used Ethereum smart contracts to define and manage the behaviours of a few devices under specified conditions. For example, an air conditioner that switches to energy saving mode when the usage of electricity reaches 170 KW. For agreements establishment, Carrillo et al. [33] developed an application that allows two untrusted parties (e.g., consumer and provider) to negotiate and then establish an agreement as a contract.

In addition to smart contract applications, there are different topics that were discussed in the literature. In [12], the authors discussed how the combination of blockchain-based smart contracts with the Internet of Thing could be powerful in terms of facilitating the sharing of services. In [9],

the authors discussed the possibility of applying blockchain-based smart contracts for licensing management. For example, the use of smart contracts to control the license of software products. In [14], the authors investigated the possibility of creating complex smart contracts without relying on scripts. In [34], the authors proposed a new consensus method called 'credibility' for contracts management (e.g., digital right management) to avoid the limitations of existing consensus methods. In [35], the authors proposed a semantic index approach to search for information in the Ethereum blockchain.

5. DISCUSSION

This section discusses the study results and answers the research questions that we defined in Section 3.

RQ1: What are the current research topics on smart contracts?

The results of this systematic mapping study showed that most of the current research on smart contracts is about identifying and tackling smart contract issues. Four different issues were identified, namely, codifying, security, privacy and performance issues. Codifying and security issues were among the most discussed issues. This is because smart contracts store valuable currency units and any security breach or coding error could result in losing money. The identified codifying issues are the difficulty of writing correct codes, the inability to modify or terminate contracts, the lack of support to identify under-optimised contracts and the complexity of programming languages. The identified security issues are transaction-ordering dependency, timestamp dependency, mishandled exception, re-entrancy, untrustworthy data feeds and criminal activities. The identified privacy issues are the lack of transactional privacy and the lack of data feeds privacy. The identified performance issue is the sequential execution of smart contracts. Although there are some proposed solutions to tackle these issues, some of them are only abstract ideas without including any concrete evaluation. A few others are still not tackled yet. For example, the solution proposed by [21] is only a suggestion to use alternative programming languages without any implementation. Criminal activities identified by [24] are still not overcome yet.

Other research proposed smart contract applications or studied other smart contract related topics. The proposed applications are trading and fair exchange, identity management, Internet of Thing and agreements establishment. The studied topics are combining smart contracts with the Internet of Thing and licensing management, studying scripting languages for smart contracts, proposing new consensus methods and proposing an indexing approach to search for useful information in blockchain systems.

RQ2: What are the current smart contract applications?

Smart contract applications are solutions that have been developed on top of blockchain technology. We identified some smart contract applications developed on top of the Ethereum blockchain. Those applications are to allow untrusted participants to share everyday objects, establish an agreement as a contract, manage their identities and control the behaviours of the Internet of Thing devices. Furthermore, we identified other applications that were built as a smart contract tool on top of the blockchain to detect or tackle codifying, security and privacy issues. Some of these tools are 'GASPER', 'OYENTE', 'HAWK' and 'Town Crier'.

RQ3: What are the research gaps that need to be addressed in future studies?

From this systematic mapping study, we identified a number of research gaps in smart contract research that can be studied by future research. The methodologies used to identify those gaps are as follows. First, observing issues or limitations from the papers included in this study (e.g., gaps

number 2, 3 and 5). Second, recognising issues that were highlighted by the papers included in this study, but still are not solved yet (e.g., gaps number 1 and 4).

The first one is the lack of studies on scalability and performance issues. The sequential execution of smart contracts affects the ability of blockchain systems to scale as we discussed in Section 4.2. With the growing number of smart contracts in the future, this issue will increase further. The author of [28] described a very high-level solution, which is parallel execution of contracts, without any concrete evaluation. Parallel execution of contracts faces a challenge in how to execute contracts that depend on each other at the same time. It is, therefore, essential to conduct research on identifying and tackling performance issues to ensure the ability of blockchain to scale.

The second gap is that almost all current research is discussing smart contracts on the Ethereum blockchain, although there are some other blockchains (e.g., NXT and Eris) that can support the creation of smart contracts. Different blockchains have distinctive features and advantages. Thus, future research might investigate different implementations of blockchain to deploy and run smart contracts.

The third gap is the small number of smart contract applications. Although the concept of smart contract has gained a lot of attention, there are only a few applications developed by the literature. This is because smart contract concept is still in its infancy stage. Banasik et al.[14] claimed that smart contracts are not widely common in practice. For future research, therefore, researchers could consider studying various potential applications such as e-commerce and cloud storage.

The fourth gap is the lack of research on tackling criminal activities in smart contracts. The author of [24] only identified three types of criminal activities that can be conducted on smart contracts without proposing any solution to them. Thus, future research could focus on identifying more types of criminal activities and proposing solutions to overcome them.

The last gap is the lack of high quality peer-reviewed research on smart contracts. Most of the research is conducted as blog articles or grey literature without providing great contributions. There is, therefore, a need for high quality publications on smart contracts.

6. CONCLUSION

Blockchain technology is a distributed database that records all transactions that have ever occurred in the network. The main feature of blockchain is that it allows untrusted parties to communicate between each other without the need of a trusted third party. Different distributed applications beyond cryptocurrencies can be deployed on top of blockchain. One of these applications is smart contracts, which are executable codes that facilitate, execute and enforce an agreement between untrusted parties. Ethereum is currently the most common blockchain platform for developing smart contracts, although there are some other available platforms.

To understand current topics on smart contracts, we decided to conduct a systematic mapping study. The main aim of this systematic mapping study was to identify and map research areas related to smart contracts. By doing so, we were able identify research gaps that need to be addressed in future studies. The focus of this study was on smart contracts from a technical point of view. Thus, we excluded studies with different perspectives (e.g., papers with an economic perspective). We extracted 24 papers from different databases. We found that most papers identifying and tackling issues on smart contracts. We grouped these issues into four categories, namely, codifying, security, privacy and performance issues. The rest of the papers focuses on proposing smart contract applications or discussing other smart contract related topics.

In this paper, we presented a few research gaps in smart contract research that need to be addressed in future studies. The identified gaps are the lack of studies on scalability and performance issues, the lack of studies on deploying smart contracts on different blockchain platforms other than Ethereum, the small number of the proposed smart contract applications, the

lack of studies on criminal activities in smart contracts and the lack of high quality research on smart contracts. These identified gaps could be studied by researchers as future works.

REFERENCES

[1] V. Buterin, "A next-generation smart contract and decentralized application platform.," Available online at: https://github.com/ethereum/wiki/wiki/White-Paper/ [Accessed 19/02/2017].

[2] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in Proceedings of the 12th International Conference on Evaluation and Assessment in Software Engineering, EASE'08, pp. 68-77, BCS Learning & Development Ltd., 2008.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[4] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A. B. Tran, and S. Chen, "The blockchain as a software connector," in 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA), pp. 182-191, IEEE, 2016.

[5] V. Buterin, "On public and private blockchains," Available online at: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/ [Accessed 01/03/2017].

[6] N.Szabo, "Formalizing and securing relationships on public networks.," Available online at: http:// rstmonday.org/ojs/index.php/fm/article/view/548/4691 [Accessed 15/02/2017].

[7] J. Stark, "Making sense of blockchain smart contracts," Available online at: http://www.coindesk.com/making-sense-smart-contracts/ [Ac-cessed 06/03/2017].

[8] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," in International Conference on Financial Cryptography and Data Security, pp. 79-94, Springer, 2016.

[9] V. Morabito, "Smart contracts and licensing," in Business Innovation Through Blockchain, pp. 101-124, Springer, 2017.

[10] A. Lewis, "A gentle introduction to smart contracts," Available online at: https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/ [Accessed 25/02/2017].

[11] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2014.

[12] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292-2303, 2016.

[13] W. Egbertsen, G. Hardeman, M. van den Hoven, G. van der Kolk, and A. van Rijsewijk, "Replacing paper contracts with ethereum smart contracts," 2016.

[14] W. Banasik, S. Dziembowski, and D. Malinowski, "Efficient zero-knowledge contingent payments in cryptocurrencies without scripts," in European Symposium on Research in Computer Security, pp. 261-280, Springer, 2016.

[15] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology?|a systematic review," PloS one, vol. 11, no. 10, p. e0163477, 2016.

[16] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy, et al., "Formal verification of smart contracts: Short paper," in Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, pp. 91-96, ACM, 2016.

[17] G. Bigi, A. Bracciali, G. Meacci, and E. Tuosto, "Validation of decentralised smart contracts through game theory and formal methods," in Programming Languages with Applications to Biology and Security, pp. 142-161, Springer, 2015.

[18] C. K. Frantz and M. Nowostawski, "From institutions to code: Towards automated generation of smart contracts," in 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W), pp. 210-215, IEEE, 2016.

[19] B. Marino and A. Juels, "Setting standards for altering and undoing smart contracts," in International Symposium on Rules and Rule Markup Languages for the Semantic Web, pp. 151-166, Springer, 2016.

[20] T. Chen, X. Li, X. Luo, and X. Zhang, "Under-optimized smart contracts devour your money," in 2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER), pp. 442-446, IEEE, 2017.

[21] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, "Evaluation of logic-based smart contracts for blockchain systems," in International Symposium on Rules and Rule Markup Languages for the Semantic Web,167-183, Springer, 2016.

[22] C. Natoli and V. Gramoli, "The blockchain anomaly," in 15th International Symposium on Network Computing and Applications (NCA), 310-317, IEEE, 2016.

[23] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pp. 254-269, ACM, 2016.

[24] A. Juels, A. Kosba, and E. Shi, "The ring of gyges: Investigating the future of criminal smart contracts," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pp. 283-295, ACM, 2016.

[25] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16, pp. 270-282, ACM, 2016.

[26] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in 2016 IEEE Symposium on Security and Privacy (SP),839-858, IEEE, 2016.

[27] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. J. Kishigami, "Blockchain contract: A complete consensus using blockchain," in 2015 IEEE 4th Global Conference on Consumer Electronics (GCCE), pp. 577-578, IEEE, 2015.

[28] M. Vukolić, "Rethinking permissioned blockchains," in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, BCC '17, pp. 3-7, ACM, 2017.

[29] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in International Conference on Principles of Security and Trust, pp. 164-186, Springer, 2017.

[30] A. Bogner, M. Chanson, and A. Meeuw, "A decentralised sharing app running a smart contract on the ethereum blockchain," in Proceedings of the 6th International Conference on the Internet of Things, pp. 177-178, ACM, 2016.

[31] M. Al-Bassam, "Scpki: A smart contract-based pki and identity system," in Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, BCC '17, pp. 35-40, ACM, 2017.

[32] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," in 2017 19th International Conference on Advanced Communication Technology (ICACT), pp. 464-467, IEEE, 2017.

[33] P. N. Carrillo, C. I. Peña, and J. L. d. L. Rosa, "Eurakos next: a cryptocurrency based on smart contracts," in Ebook: Artificial Intelligence Research and Development, vol. 288 of Frontiers in Artificial Intelligence and Applications, pp. 221-226, 2016.

[34] H. Watanabe, S. Fujimura, A. Nakadaira, Y. Miyazaki, A. Akutsu, and J. Kishigami, "Blockchain contract: Securing a blockchain applied to smart contracts," in 2016 IEEE International Conference on Consumer Electronics (ICCE), pp. 467-468, IEEE, 2016.

[35] A. Third and J. Domingue, "Linked data indexing of distributed ledgers," in Proceedings of the 26th International Conference on World Wide Web Companion, WWW '17 Companion, pp. 1431-1436, 2017.

INVESTIGATION THE EFFECT OF USING GRAY LEVEL AND RGB CHANNELS ON BRAIN TUMOR IMAGE

Ahmed B Salem Salamh

Department of Computer, Zawia University, Zawia City, Libya

ABSTRACT

Analysis the effect of using gray level on the Brain tumor image for improving speed of object detection in the field of Medical Image using image processing technique. Specific areas of interest are image binarization method, Image segmentation. Experiments will be performed by image processing using Matlab. This paper presents a strategy for decreasing the calculation time by using gray level and just one channel Red or Green or Blue in medical Image and analysis its impact in order to improve detection time and the main goal is to reduce time complexity.

KEYWORDS

Image Segmentation, Medical Image, Detection Time, Brain Tumor image, Image Channels, Time Complexity

1. INTRODUCTION

Image processing is a very important field in the whole world these days and has become the necessary field of enhancing and analyze images. The image processing technique provides massive of methods to process and manipulate pictures in many fields, for example edge detection, image compression, facial recognition and medical image. However, image processing overcomes traditional use as a result of computers become more efficient and reliable. A computer is used to making a picture with different types as the properties of images that distinguish its extensions. On the other hand, using technique to alter and interpret real images. The main objectives of image processing are enhancing image quality and detection of information in order to clarify image objects in spite of sophisticated details that sometimes make it difficult to process. It is useful to use image processing methods as the first step to digitize a picture into an image file. The next step is applying some technique to enhance image quality. In addition, Image processing is growing very rapidly, for example, processing of medical image is one of the most important fields due to many reasons such as breast cancer and fracture bone detection, which causes lots of trouble in many years due to lack of research In a global term, image processing is one of computer applications which it uses many algorithms to process the image. Moreover, each algorithm has advantages and disadvantages that affect on image in different positions. Many applications have been developed in order to reach optimal technique that enable researchers to work more efficient and fast in this field. One of the important medical images is Magnetic resonance imaging (MRI). X-ray scanners utilize solid magnetic fields, radio waves, and field inclinations to produce pictures of the organs in the body. For instance, MRI is used to diagnose brain tumor in order to detect mass of abnormal tumor which is abnormal cell.

MRI makes it conceivable to introduce many sorts of tissue differentiate by changing excitation and reiteration times, which makes it an exceptionally adaptable instrument for imaging diverse structures of intrigue. Because of the nature and appearance of cerebrum tumors, one MRI arrangement is not adequate to completed portion the tumor including all its sub regions.

2. RESEARCH PAPER OBJECTIVES

This paper focuses on:

1- Analysis The effects of using gray level on Medical Image (MRI image) in order to get less information and improve time complexity and investigate the benefits of using gray level on the brain tumor medical image.

2- Experiments of techniques this paper use on different brain images, analysis, contrast and discuss the results.

3- Produce the conclusion.

3. RELATED WORK

Magnetic resonance imaging (MRI)) is a fantastic medicnal imaging, especially for brain imaging. MRI inside the human body is useful to see the level of details. Specialists have real specialized and monetary significance of dependable also, quick detection and classification of brain malignancy, malignancy means in advanced stage. MRI is most proficient for the examination of brain tumor recognition and characterization when contrasted with other imaging procedures [1]. Brain tumor is a mass of tissue that grows out of control of the normal forces that regulates growth [2]. The Brain tumor is the most common, occurring malignancy among human beings [3]. The brain abnormality detection and segmentation of MRI images is an exceptionally hard to specify and crucial to assess which is utilized as a part of surgical and restorative arranging and appraisal. The trouble in brain picture examination is primarily because of the necessity of identification procedures with high exactness with speed time [4]. Brain tumor is diagnosed at advanced stages with the help of the MRI image [5]. Medical Image Analysis provides a forum for the dissemination information of new research results in the field of medical and biological image analysis, with special emphasis on efforts related to the applications of computer vision, virtual reality and robotics to biomedical imaging problems [6]. MRI image segmentation is an important but inherently difficult problem in medical image processing [7]. Image segmentation is used to separate objects from the background, and thus it has proved to be a powerful tool in bio-medical imaging. [8]. Tumor segmentation from magnetic resonance imaging (MRI) process is an important but time ingesting manual project performed by doctors. Magnetic resonance imaging (MRI), computed tomography (CT), virtual mammography, and other imaging strategy, supply an efficient way for detecting one-of-a-kind form of tumors[4]. In clinical photograph processing, the problems of reminiscence utilization and low execution velocity are compounded with ever-increasing sizes of information units. Normal high decision Computed Tomography (HRCT) photo sets now consist of masses of 512x512 slices, making up an (nearly) isotropic volume, that's quality treated as one volume for reasons of consistency of effects over the 0.33 axis [9].

In the medical field, it is still needed searching in this area, which is very important in the life because, it saves many people or enable specialized people to find out problems related to this as fast as possible. Many researchers have created image processing techniques to use it in specific system. This techniques has concentrated on advantage step of the process. For instance, using techniques such as an effecient segmentation algorithm by Fast scanning that was fast with the

speed [10] but is not for abnormal region of brain image. There are several basic ways to segment any type of image. For example, Threshold Technique, Edge-Based Segmentation, Region-based Segmentation. .However, all previous method work with convert RGB image to grayscale as first step, which consist of value between 0 to 255. From this is good to convert image to grayscale, but this paper proposes to process RGB image directly with extract of one color from the RGB image without converting images. Neeraja Menon and Rohit Ramakrishnan have proposed fast MRI Brain Image segmentation method based on Artificial Bee Colony (ABC) [11]. The first step of their work, convert MRI image to grayscale.

P. S. Juhi and S. S. Kumar proposed Bounding box based automatic segmentation of brain tumors using random walker and active contours from brain MRI. They introduced fast and accurate segmentation method by segmenting the most dissimilar regions of a tumor image[12]. None of any algorithms used to process MRI image significantly with one of RGB colors of the original image.

4. METHODS

This section shows examples of some common image processing techniques that have been used in brain tumor for image display, analysis and human interpretation.

Experiment Steps:

1. Load color image from original MRI image.

2. Convert a gray image and read Red, Green and Blue image in order to manipulate each one.

3. Image binarization for each Red, Green and Blue image to select objects and observe the difference between the three images.

4. Histogram for each gray image, Red, Green and Blue image for clarification.

5. Object detection with circle for each Red, Green and Blue image.

The following flowchart shows in pictorial form how a method is finished from begin to the end in sequential step order. Moreover, represent the five steps with flowchart is needed in order to understand the main objective of the paper and it will clarify stages as it appear in figure 1.
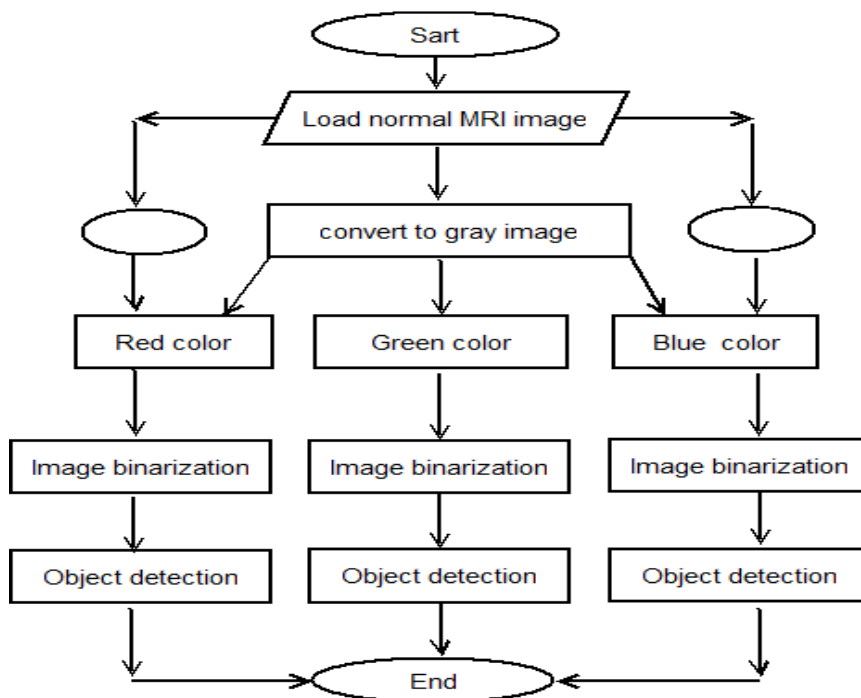
Figure 1. Clarification of experiment steps with different methods

4.1 First experiment.

In The first step, load the original MRI image with a brain tumor. The next step As we can see in the figure 2 convert MRI image to gray image in order to process images and makes the comparison.
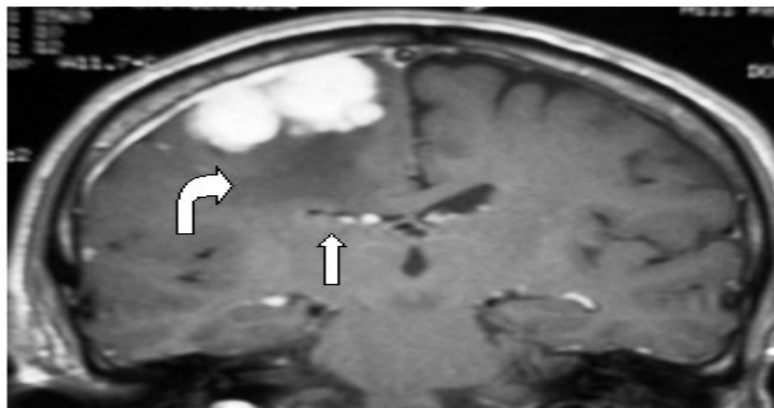

Figure 2. Presents gray level information from the original MRI image which captures brain tumor

The next part shows original red, green, blue colors of the image. In this part we have a choice to extract three colors from gray image or extract one channel from the original color image.

This paper uses the method to extract red, green, blue Sequentially and present them in order to apply segmentation and binarization on three colors as it appears in the following figure.
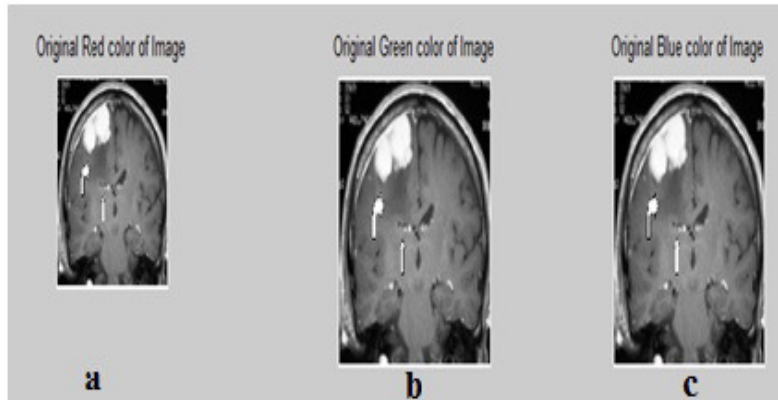
Figure 3. Separate gray image (a) Red (b) Green (c) Blue

The next section is applying segmentation and binarization and function to neglect the connected pixel in specified size in order to present object and detect brain tumor. Furthermore, this will apply on three colors sequentially to analysis the effect of object detection. This is clear in the figure 4.
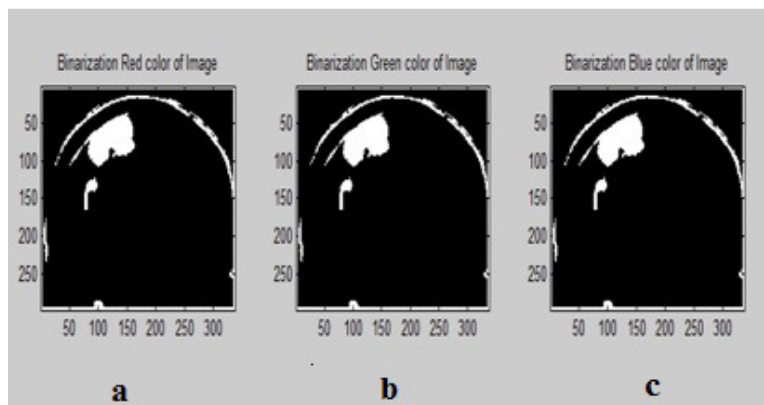

Figure 4. Presents image binarization (a) Red (b) Green (c) Blue image

The histogram is useful to check the a distribution of discrete intensity levels or the range of quantities in the specified graph. In the figure 5, it is clear to observe the distribution of one color in each part red, green, blue and its has the same distribution and its presented in figure 5.
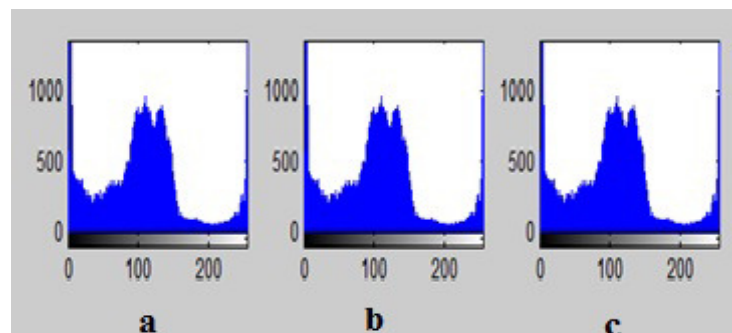

Figure 5. Presents histogram (a) Red (b) Green (c) Blue image.

The histogram in the next figure is to grayscale image comes from the original color image to demonstrate the comparison of any color red or green or blue as a result of this there is no difference between them as it showed in figure 6.
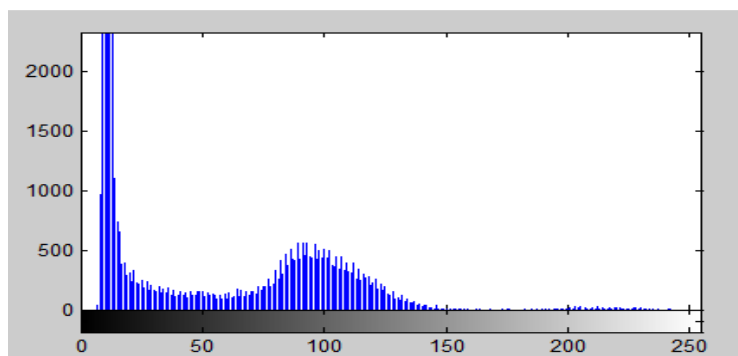

Figure 6. Presents histogram for the original gray image.

The object detection is very important and it takes part after applying segmentation using the threshold method with   value   between 180 and 200 in order to complete segmentation and binarization to extract a brain tumor from MRI image which is clear in the figure 7. In the three parts of colors red, green, blue the object appears and can observe. Moreover, the goal of this detection is to make notification about object detection on each color and observe the difference as a result the brain tumor appears in the figure 7.
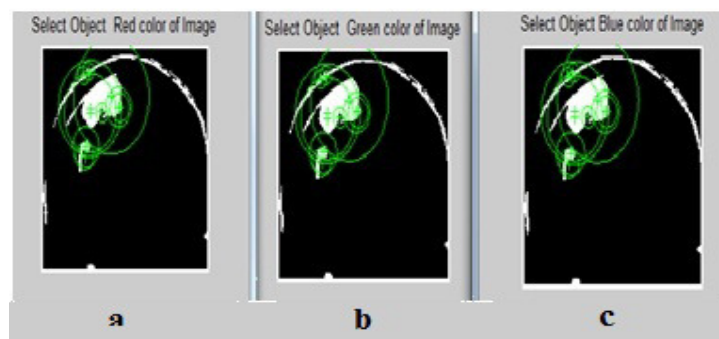

Figure 7. Shows object detection with circle(a) Red (b) Green (c) Blue image.

4.2. Second experiment.

It is valuable to test and check multiple brain tumor images , in this paper is tested , checked ,verified multiple brain images with different contrast, brightness, noise in order to achieve detection and make the comparisons and get accurate results, This section repeats the previous method and steps which starts with a grayscale image that comes from original MRI color image and its clearly in figure 8, combines all parts.
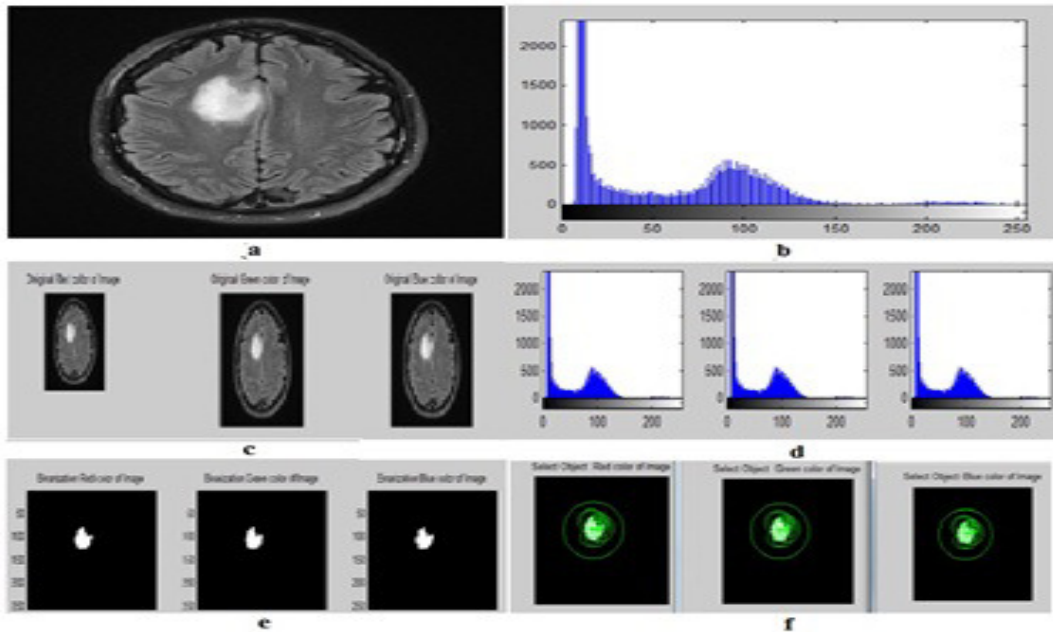
Figure 8. a) Presents gray level information from the original MRI image which captures brain tumor,
b) Presents histogram for the original gray image. c) Separate Red, Green and Blue of gray image,
d) Presents histogram for each Red, Green and Blue image , e) Presents image binarization for each Red,
Green and Blue image, f) Presents object detection with circle for each Red, Green and Blue image

5. DISCUSSION THE RESULTS

The suggested method is utilized to reduce the process of information needed in the whole brain
tumor original image to detect and segment tumor in another image at the beginning of any
algorithm, the method proposed dealing directly with the orginal MRI image without need to
convert the original image to grayscale image which will lead to reduce the complexity of code
and as the result will lead to reduce the time complexity of the process image as well as minimize
the information needed by using one color. Moreover, less information and calculation when
check one of three color data. The result of the segmentation and binarization when applying on
red, green, blue color of the original image is object detection, which makes the comparison more
sufficient to prove the results . The proposed method gives very good results for different MRI
images.

6. CONCLUSION

The results prove that, improve the speed of image processing is possible by separating image
colors this paper use medical image, brain tumor as a case study to test object detection   and the
result will be the same if it process separately this directly will lead to enhance of the whole
manipulation in the image. Moreover, processing color image to red or green or blue and working
with one color will bring this enhancement because of this extract on color for example Red color
from color image directly and working with it is better than change image to gray level,
furthermore it is like working with less information, less mathematic operation. The benefit of
this work will help online algorithm developers, online manipulation and even in image
uploading to test fast algorithms and online application. There is no difference in tumor detection
between gray image or using one color channel which is clear when compare histograms and

objects in this case it is better to use one channel from a color image without changing color image to grayscale for those cases.

ACKNOWLEDGEMENTS

REFERENCES

[1]   Ruchi D. Deshmukh & DYPIET Pimpri," Study of Different Brain Tumor MRI Image Segmentation Techniques ", April, 2014, International Journal of Computer Science Engineering and Technology, Vol 4, Issue 4,133-136.

[2]   T. Kim & Ubiquitous," computing and multimedia applications",(2011) Berlin: Springer.

[3]   Tai-Hoon Kim & Debnath Bhattacharyya, (2011) ," Analysis Brain Tumor Detection Using MRI Image", MPCT, Hannam, university, Vol.151,pp 307-314.

[4]   Madhurima Banerjee   &   Ranjita Chowdhury & Samir Kumar Bandyopadhyay, (2015), "DETECTION OF BRAIN TUMOR FROM MRI OF BRAIN",Vol. 02, Issue, 12, pp. 1555-1559.

[5]   S. Karthigaiselvi and T. Kalaiselvi,(2017),"Investigation of Image Processing Techniques in MRI Based Medical Image Analysis Methods and Validation Parameters for Brain Tumor", Current Medical Imaging Reviews, vol. 13.

[6]   N. Ayache & J.S. Duncan,(2016), Medical Image Analysis, journals., MICCAI Society .

[7]   Pankaj Kr. Saini1& Mohinder Singh& Maharishi Ved Vyas,(2015)," BRAIN TUMOR DETECTION IN MEDICAL IMAGING USING MATLAB", Engineering College Jagadhri, Yamuna Nagar India.

[8]   A. Aslam, E. Khan and M. Beg, "Improved Edge Detection Algorithm for Brain Tumor Segmentation", Procedia Computer Science, vol. 58, pp. 430-437, 2015.

[9]   Madhurima Banerjee   &   Ranjita Chowdhury & Samir Kumar Bandyopadhyay, (2015), "DETECTION OF BRAIN TUMOR FROM MRI OF BRAIN",Vol. 02, Issue, 12, pp. 1555-1559.

[10] Jian-Jiun Ding & Cheng-Jin Kuo & Wen-Chih Hong, "AN EFFICIENT IMAGE SEGMENTATION TECHNIQUE BY FAST SCANNING AND ADAPTIVE MERGING", Graduate Institute of Communication Engineering, National Taiwan University.

[11] N. Menon & R. Ramakrishnan,   2015 , "Brain Tumor Segmentation in MRI images using unsupervised Artificial Bee Colony algorithm and FCM clustering," 2015 International Conference on Communications and Signal Processing (ICCSP).

[12] P. S. Juhi & S. S. Kumar, "Bounding box based automatic segmentation of brain tumors using random walker and active contours from brain MRI,), 2014, " International Conference on Control, Instrumentation, Communication and Computational Technologies (ICCICCT.

AUTHOR

Ahmed B Salem Salamh
Department of Computer, Zawia University, Zawia City, Libya

REAL-TIME MOUTH DEFECTS DETECTION ON MILITARY CARTRIDGE CASES

Semra Aydin[1], Refik Samet[2] and Omer Faruk Bay[3]

[1]Education of Computer and Electronics, Gazi University, Ankara, Turkey
[2]Department of Computer Engineering, Ankara University, Ankara, Turkey
[3]Department of Electric and Electronics Engineering,
Gazi University, Ankara, Turkey

ABSTRACT

A military cartridge includes four elements; case, capsule, ammunition and powder. While manufacturing, defects may occur in the case. These defects should be detected and the defected cases should be separated. Defects could occur in the mouth, surface and primer parts of the case. This paper proposes the methodology that involves the real-time inspection of the defects in the mouth part of the cases using image processing techniques. The algorithms of the proposed methodology were implemented on real images and the obtained results have showed that common defects such as split and dent defects occurring on the mouth part of the case can be detected with high accuracy.

KEYWORDS

Military cartridge, case mouth defects, defect detection, circle detection.

1. INTRODUCTION

Computer vision systems are widely used in industrial applications to inspect defects in real-time. These systems control the real-time production lines by processing the images taken by cameras and separate defected products. Due to computer vision systems, the production capacity and quality of products increase and the product cost and inspection time decrease.

Main functions of the computer vision systems are fulfilled by image processing techniques. Some industrial products with cylindrical and metal surfaces need to be inspected in moving state. Inspection of dynamic and complex products using real-time image processing techniques is a nontrivial problem.

Image processing to inspect the products with cylindrical and metal surfaces has some challenges, which are related to quality of images taken in moving state. The first challenge is related to the glitters problem during illumination. In order to get images with high quality, a special ring lightning should be used. Due to cylindrical and metal surfaces, some part of the products can be glittered. The second challenge is related to the moving state of products. It is hard to capture images of moving product in the same position. The third challenge is the cylindrical surfaces itself. In order to inspect the whole 360-degree of the surface, it is necessary to capture the product surface on the fly. The pixel intensity is changed depending on the distance between

camera and cylindrical surface of the product. All of these challenges make image processing more complex.

The military cartridge consists of four parts: case, capsule, ammunition and powder. The military cartridge case consists of three elements: mouth, cylindrical surface and primer (Fig. 1).

          (a)   (b)   (c)

Figure 1. Parts of military cartridge case: (a) mouth, (b) cylindrical surface, (c) primer.

This study investigates the defects on the mouth of the cases where different defects, like split and dent defects, could occur. These defects are defined by NATO standards [1, 2]. At the final stage of the production process, defects should be inspected and then the defected ones should be separated. These operations should be done in real-time.

In this study, a computer vision system for the inspection of moving cartridge case is used. In this system, one camera is used for each of the mouth and the primer, and eight cameras are used for the cylindrical surface to take images. The images taken by the cameras are processed by real-time image processing algorithms to detect defects. The defected cases detected are separated at the final stage of computer vision processing.

This study proposes the methodology for real-time inspection of defects on the mouth part of the cases by image processing techniques.

The manuscript is organized as follows. In Section 2, related works are summarized. The detection methodology of defects is proposed in Section 3. Implementation of proposed methodology is described in Section 4. Finally, Section 5 concludes obtained results.

2. RELATED WORKS

In computer visual inspection systems, the defect detection algorithms are used to determine the defected products. Existing works use different algorithms to detect the defects on the different materials. The most common topic is related to textile materials. Kumar et al. [3] investigate various approaches for automated inspection of textured materials using Gabor wavelet features. Kumar [4] investigates different techniques for the detection of automated fabric defects. Chan and Pang [5] propose a method using Fourier transform to detect fabric defects.

There are many studies related to the detection of metallic surface defects in automated inspection systems. Choi et al. [6] present a real-time defect detection algorithm for high-speed steel bar in coil. Frayman et al. [7] present a camera based machine vision system for the automatic inspection of surface defects in aluminium die casting using genetic algorithm. Karimi and Asemani [8] compare and evaluate different defect detection algorithms using various performance parameters. In the literature, various image processing techniques were used to detect defects on different kinds of materials. This paper adopts and uses existing techniques to detect defects on cylindrical and metal objects in real-time.

Following studies are related to circle detection which can be used to detect the defects in the circularity of objects. To detect the circles with image processing techniques, different algorithms can be used. In [9], an algorithm for edge and segment detection was proposed. This algorithm can detect the circles in real-time images. In [10], a circle detection algorithm for automatic sign detection and recognition was proposed. The authors in [11] have proposed another algorithm to detect circles on images. In [12], a review study related to Hough algorithm was reported. An efficient Hough transform for circle detection was proposed in [13]. It was reported that, Hough is a popular algorithm to detect the circles. But to the best of our knowledge, there are no studies related to implementation of Hough algorithm to the moving cylindrical and metal objects. This paper uses Hough algorithm for checking the circularity to detect the defects in circles of real-time images of cylindrical and metal objects captured in a moving state.

3. MOUTH DEFECTS DETECTION METHODOLOGY

Different defects such as split, dent, etc. can occur in the mouth part of military cases (Fig. 2).

(a)   (b)   (c)

Figure 2. (a) Normal mouth, (b) mouth with split defect, (c) mouth with dent defect

The proposed methodology to detect the defects in the mouth part of the cases consists of the following stages:

• Preprocessing;
• Mouth processing;
• Split defect detection;
• Dent defect detection.

Block diagram of the entire defects detection methodology is shown in Fig. 3.

```
                        ┌──────────┐
                        │  Start   │
                        └──────────┘
                             │
                        ┌──────────┐
                        │ Captured │
                        └──────────┘
       ┌─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─│─ ─ ─ ─ ─ ─ ─ ─ ─ ─┐
       │                ┌──────────┐                │
       │                │ Cropping │                │
       │                └──────────┘                │
       │                     │                      │
       │              ┌───────────────┐             │
       │              │ Noise Reduction│            │
       │              └───────────────┘   Preprocessing
       │                     │                      │
       │              ┌──────────────┐              │
       │              │ Thresholding │              │
       │              └──────────────┘              │
       │                     │                      │
       │                ┌──────────┐                │
       │                │ Closing  │                │
       │                └──────────┘                │
       └─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─│─ ─ ─ ─ ─ ─ ─ ─ ─ ─┘
       ┌─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─│─ ─ ─ ─ ─ ─ ─ ─ ─ ─┐
       │                 ┌─────────┐               │
       │                 │ Circle  │               │
       │                 └─────────┘               │
       │                     │             Mouth   │
       │           ┌────────────────┐   Processing │
       │           │ Mouth detection│              │
       │           └────────────────┘              │
       │                     │                      │
       │           ┌────────────────┐              │
       │           │ Reconstruction │              │
       │           └────────────────┘              │
       └─ ─ ─ ─ ─ ─ ─ ─ ─ ─ ─│─ ─ ─ ─ ─ ─ ─ ─ ─ ─┘
                   ┌──────────────────────┐
                   │ Split defect detection│
                   └──────────────────────┘
```
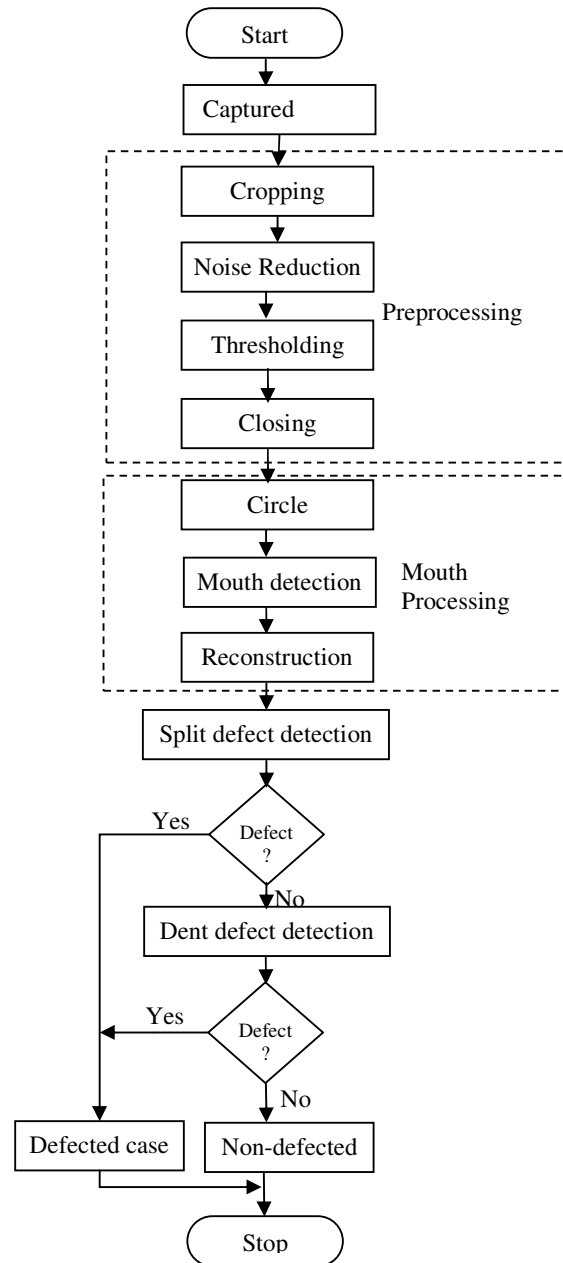
Figure 3. The block diagram of proposed defect detection methodology

3.1. Preprocessing

Preprocessing stage includes four steps: 1) cropping; 2) noise reduction; 3) thresholding and 4) morphological operations (closing).

3.1.1. Cropping

In real-time applications, the image processing performance should be optimized. For this, the size of captured raw images should be decreased. In other words, unnecessary part of raw images should be cropped.

3.1.2. Noise Reduction

Noise reduction is a process of removing noise from an image. Generally; every image has some noise that needs to be eliminated. Several techniques can be used to remove the noise from the image. Gaussian filter is widely used to reduce image noise.

3.1.3. Thresholding

Thresholding is a key step in defect detection process. The success of subsequence stages of methodology depends on the result of thresholding step [13, 14]. Mouth part of the captured image is glittered due to illumination. In order to get the glittered mouth in cropped image, bi-level thresholding should be used. At the result of bi-level thresholding, the glittered part of the mouth is denoted by white pixels and inside the mouth is filled by black pixels.

3.1.4. Morphological Operations

In order to improve the success, some morphological operations should be applied to the images. After thresholding, small discontinuities may appear. Closing operation can help eliminating such discontinuities.

3.2. Mouth Processing

Mouth processing stage includes three steps: 1) detection of the circle; 2) detection of the inner edge of the mouth and 3) drawing an edge of mouth.

3.2.1. Cycle Detection

Different algorithms can be used to detect the circle. Hough transform is a common algorithm used to detect geometry shape of the objects in image processing [15, 16]. At the results of Hough circle detection process, the center and the radius of the circle are defined. Center of the circle is denoted as $c(x, y)$ that is the pixel in the image. Radius is denoted as r.

3.2.2. Detection of Inner Edge of Mouth

First, the image obtained at thresholding step is scanned 360 degrees beginning from the center pixel of $c(x, y)$ toward to the inner edge of the mouth (Fig.4).

During scanning, 360 points detected on the inner edge of the mouth will be denoted as $C(X_\varphi, Y_\varphi)$. Here, X_φ and Y_φ are the coordinates of $C(X_\varphi, Y_\varphi)$ and calculated as follows:

$$X_\varphi = x + (i_\varphi * \cos(\varphi * pi \div 180))$$

(1)

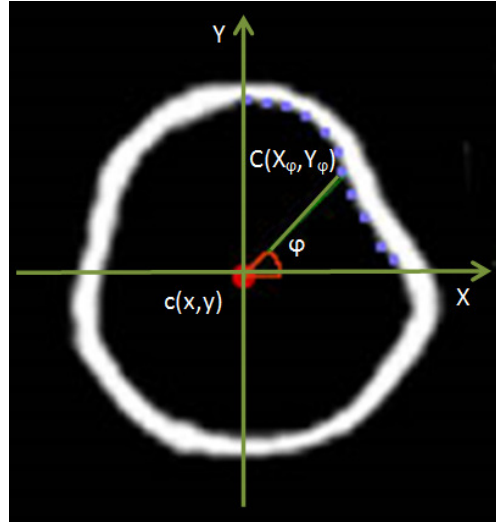$$Y_\varphi = y + (i_\varphi * \sin(\varphi * pi \div 180))$$

(2)

Figure 4. Detection of inner edge of mouth

where, φ $(\varphi = 1,2,...,360)$ is the degree of the 360 points of $C(X_\varphi, Y_\varphi)$ on the inner edge of the mouth. Next, the distance i_φ $(i_\varphi = 1,2,...,I)$ between $c(x,y)$ and $C(X_\varphi, Y_\varphi)$ is calculated. i_φ is defined as the minimum distance between $c(x,y)$ and $C(X_\varphi, Y_\varphi)$. Finally, $C(X_\varphi, Y_\varphi)$ and i_φ are stored as an array and used for the next step.

3.2.3. Drawing an Edge of Mouth

By using the array obtained in the previous step, the edge of the mouth is drawn by marking the black pixels on the white background.

3.3. Split Defect Detection

Euclidean distance is used to measure the distance between $C(X_\varphi, Y_\varphi)$ and $C(X_\varphi + 1, Y_\varphi + 1)$.

If the Euclidean distance is greater than Δ then the split defect on the mouth is present. Δ is the Euclidean distance for mouth of non-defected cases. If the Euclidean distance is less than Δ then it is necessary to go to the next stage of the methodology to detect the dent defect.

3.4. Dent Defect Detection

Dent defect detection stage includes three steps: 1) circle detection in the inner edge of the mouth; 2) calculation of the cumulative variance and 3) classification of the dent defect.

3.4.1. Circle Detection on Inner Edge of Mouth

Hough circle detection is applied to the inner edge of the mouth drawn in Section 3.2.3. The circle detected here is overlapped better with the mouth of the case with respect to the circle detected in Section 3.2.1. If Hough transform cannot detect any circle in the inner edge of the mouth, the circle detected in Section 3.2.1 is used.

3.4.2. Calculation of Cumulative Variance

The variance used for the detection and classification of the circular objects. Two different techniques are used to calculate the cumulative variance.

a) In the first one, central point $c(x, y)$ and radius r of the circle, detected in Section 3.2.1 by Hough algorithm, are used to calculate the cumulative variance. In order to calculate the cumulative variance of each degree of φ $(\varphi = 1,2,...,360)$, the Euclidean distance between the same points on the circle detected in Section 3.4.1 and the edge of the mouth drawn in Section 3.2.3 is calculated. The sum of all the square of Euclidean distance values for 360 degrees gives us the cumulative variance.

b) In the second technique, the average distance between the points on the edge of the mouth drawn in 3.2.3 and central point $c(x, y)$ is calculated. Then, the Euclidean distance between the points on the circle and the points on the edge of the mouth drawn in 3.2.3 is calculated. Finally, the sum of square of all 360 Euclidean distance values for 360 degrees gives us the cumulative variance.

3.4.3.   Classification of Dent Defects

When the mouth of the cases is fully circular, these kind of cases are classified as non-defected. If the calculated cumulative variance is less than δ then the cases are also classified as non-defected. On the other hand, if cumulative variance is greater than δ, the cases are classified as defected.

4. IMPLEMENTATION

All experiments were performed on platform with i7 2.4 GHz CPU, 8 GB RAM and Windows 7. All algorithms used in this study were coded in Visual Studio C++. All images were captured by PointGrey Flea 3 GigE 2.0 MP and Wordop 180 mm ring red colored led light was used to illuminate the cases.

According to the real-time conditions, five cases per second should be handled. So, each case should be processed during 200 milliseconds. Proposed algorithms should meet the real-time conditions.

A case inspection system was developed to capture images and to separate defected cases. An example of image captured on the conveyor band is shown in Fig. 5.
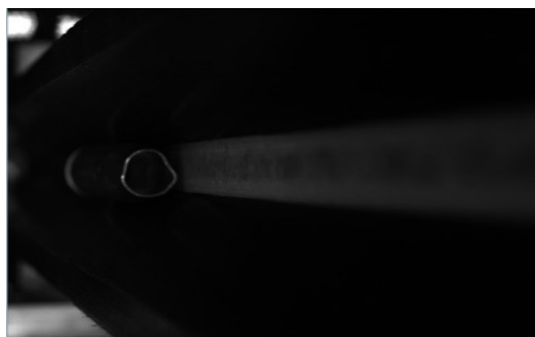

Figure 5. Original image

The implementation results of the proposed methodology on the real images are described below.

4.1. Preprocessing

The original image resolution is 1600x1200 pixels. After cropping, the image with resolution 350x350 pixels was obtained (Fig. 6).

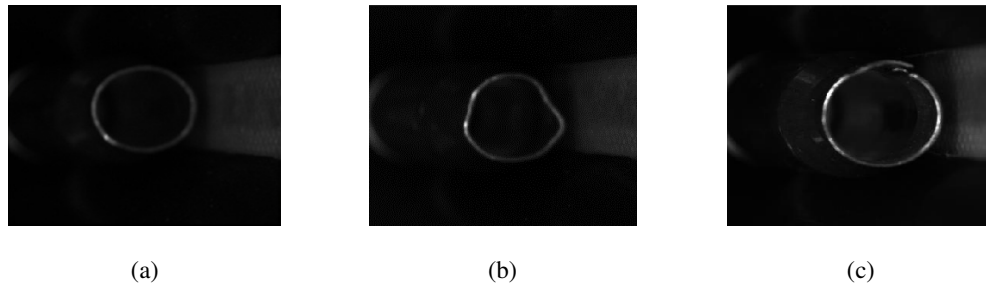(a)   (b)   (c)

Figure 6. Cropped mouth of non-defected case (a); dent defected case (b); and split defected case (c)

Gaussian filter was applied to the cropped images for noise reduction (Fig. 6).

Binary thresholding was done based on the Otsu threshold value. Following the thresholding, closing process was carried out and small discontinuities in the mouth of the case were closed (Fig. 7).
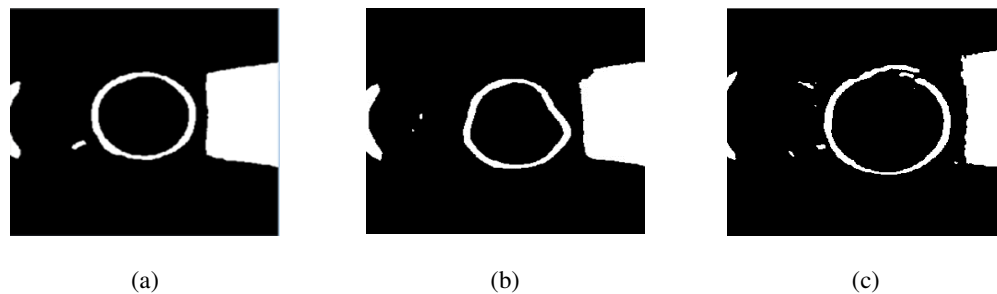

(a)   (b)   (c)

Figure 7. The results after thresholding and closing operation: non-defected mouth (a); dent defected mouth (b); and split defected mouth (c)

4.2. Mouth Processing

4.2.1. Circle Detection

Hough circle detection algorithm was used to detect the circle in the mouth of the case. The center and the radius of circle were found using this algorithm. The red circle was obtained in Fig. 8.

(a)   (b)   (c)
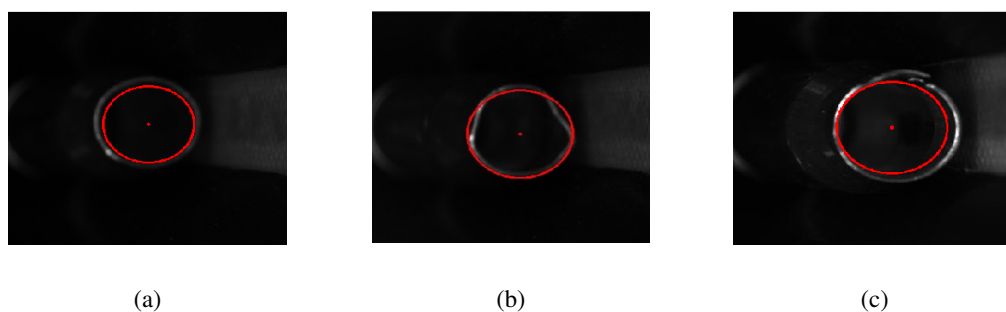
Figure 8. Detected circles of non-defected mouth (a); dent defected mouth (b); and split defected mouth (c)

4.2.2. Detection of Inner Edge of Mouth:

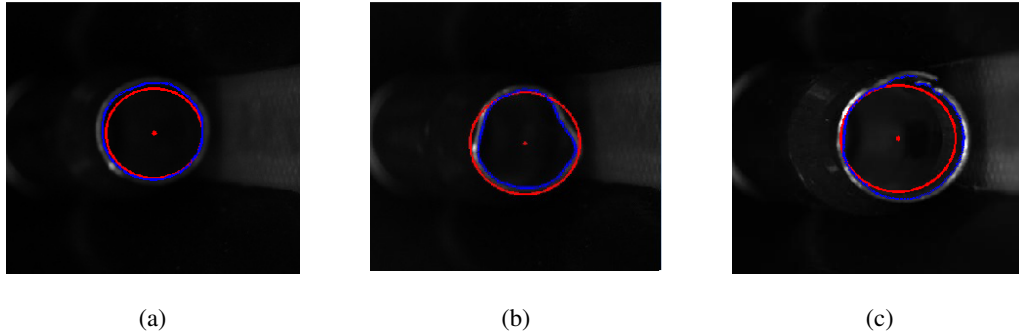Inner edge of the mouth was found and illustrated with blue color in Fig. 9.

(a)   (b)   (c)

Figure 9. Blue colored inner edge of non-defected mouth (a); dent defected mouth (b); and split defected mouth

4.2.3. Drawing the inner edge of mouth

The inner edge of mouth was reconstructed by marking the pixels of obtained array in Section 3.2.2 as black on the white background (Fig. 10).
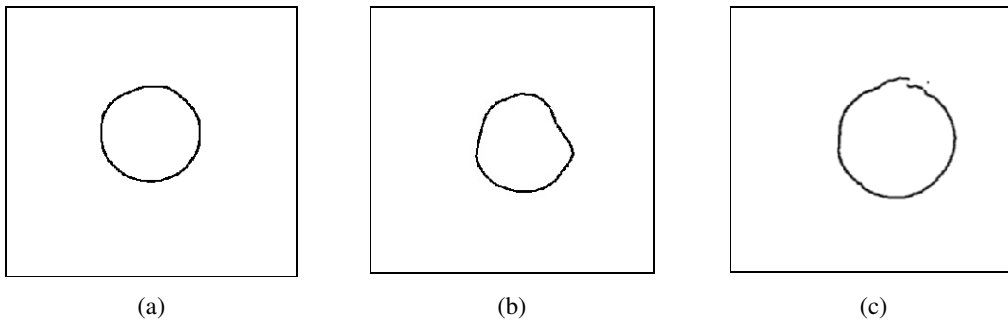

(a)   (b)   (c)

Figure 10. Reconstructed non-defected mouth (a); dent defected mouth (b); and split defected mouth (c)

4.3. Split Defect Detection

As seen from Fig. 9 (a) and (b), there is no interruption on the edge of the mouth. Suppose that $\Delta = 2$. The distance between neighbor pixels of mouth edge is calculated as 1-2. This means that the case is non-defected. On the other hand, there is an interruption on the edge of the mouth in Fig. 10 (c). For this case, the some distance was bigger than the value $\Delta = 2$ for split defected mouth. This means that the case is defected.

4.4. Dent Defect Detection

4.4.1. Hough circle detection on the inner edge of the mouth:

Fig. 11 shows the first (red) (Section 3.2.1) and second (yellow) (Section 3.4.1) circles obtained by Hough circle detection. The blue line is the inner edge of the mouth. During the second circle detection, the center of the mouth of the case was found more accurately.

4.4.2. Calculation of cumulative variance

The yellow line is perfect circle and the blue line is the mouth of the case. Cumulative variance was calculated between the yellow and the blue lines.

(a)   (b)

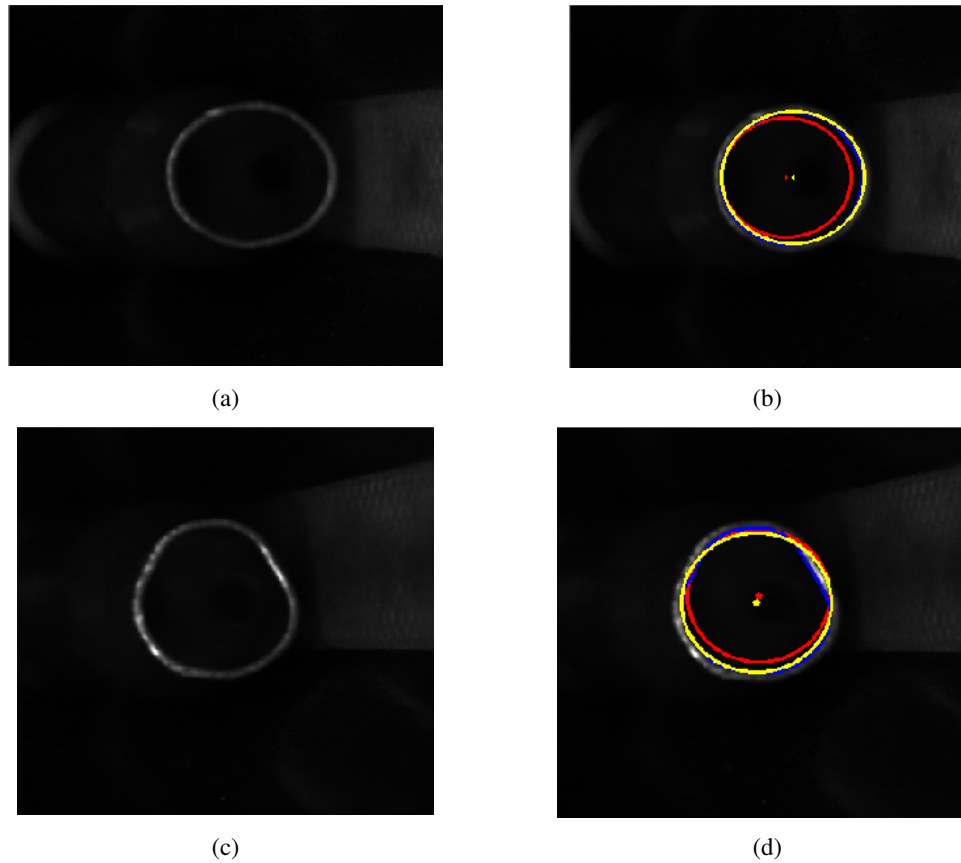(c)   (d)

Figure 11: Non-defected mouth (a); circles detected on non-defected mouth (b); dent defected mouth (c); circles detected on dent defected mouth (d)

4.4.3. Classification of dent defect

If the cumulative variance is bigger than determined value of the mouth, the case will be defined as defected. Otherwise the case will be defined as non-defected.

5. RESULTS

The results obtained were evaluated using confusion matrix theory [17, 18] which has four categories. True Positives (TP) mean the defected cases are detected as defected. False Positives (FP) mean the non-defected cases are detected as defected. True Negatives (TN) mean the non-defected cases are detected as non-defected. False Negatives (FN) mean the defected cases are detected as non-defected. The confusion matrix is shown in Table 1.

Table 1. Confusion matrix

		Result of algorithm	
		Defected	*Non-defected*
Actual military case	*Defected*	TP	FN
	Non-defected	FP	TN

The results are evaluated by error rate, recall, precision and F-measurement.

Error rate is defined as follows:

$$Err = \frac{FN + FP}{TP + FN + FP + TN} \tag{3}$$

Recall is defined as follows:

$$Rec = \frac{TP}{TP + FN} \tag{4}$$

Precision is defined as follows:

$$Pre = \frac{TP}{TP + FP} \tag{5}$$

F-measurement is defined as follows:

$$F = \frac{2 \times Rec \times Pre}{Rec + Pre} \tag{6}$$

50% non-defected and 50% defected images were used during experiments.

Table II shows the results obtained using the cumulative variance calculated on the base of the radius of the circle by Hough algorithm (Section 3.4.2 (a)).

Table 2. Results on the base of the radius value

		Result of algorithm	
		Defected	*Non-defected*
Actual defects of case	*Defected*	48%	2%
	Non-defected	10%	40%

Table III shows the results obtained using the cumulative variance calculated on the base of the average distance (Section 3.4.2 (b)).

Table 3. Results on the base of the average distance

		Result of algorithm	
		Defected	*Non-defected*
Actual defects of case	*Defected*	48%	2%
	Non-defected	8%	42%

Table IV shows the results of error rate, recall, precision, and F-measurement calculated by using Tables II and II and Eq. (3)-(6).

Table 4. Results of proposed methodology

	Error Rate	Recall	Precision	F-measurement
Radius	12%	96	82	88
Average	10%	96	85	90

As seen from Table IV, according to the values of metrics, the split and dent defects occurring on the mouth part of the case were detected with high accuracy in comparison with existing manual inspection system where the rates of the above listed metrics are very low. As seen from Tables II and III, the values of FN are 2% which means that very small number of defected cases is detected as non-defected. The other finding is related to FP which is calculated as 10% and 8%. This means that a small number of non-defected cases was defined as defected. By improving the quality of online images the values of these metrics can be increased.

3. CONCLUSION

This paper has proposed a methodology to detect defects in the mouth part of military cartridge cases. At all stages of the proposed methodology, special algorithms taking into account the challenges listed in introduction section were proposed.

The proposed methodology was implemented using real images. The results obtained showed that 96% of the defected cases were detected and separated in real-time. Experiment results have showed that the proposed algorithm guarantees the condition of the real-time processing and accuracy of detection.

In the future work, parallel programming techniques will be used to increase the accuracy rate and to decrease processing time.

ACKNOWLEDGEMENTS

REFERENCES

[1] MIL-STD-651, Military Standard-Visual Inspection Standards for 20mm Ammunition and Components, Department of Defense, USA, 18 October 1962.

[2] MIL-STD-636, Military Standard-Visual Inspection Standards for Small Arms Ammunition Through Caliber .50, Department of Defense, USA, 5 June 1958.

[3] A. Kumar, and G.K.H. Pang, (2002) "Defect Detection in Textured Materials Using Gabor Filters", IEEE Transactions On Industry Applications, Vol. 38, No. 2, pp425-440.

[4] A. Kumar, (2008) "Computer-Vision-Based Fabric Defect Detection: A Survey", IEEE Transactıons On Industrıal Electronıcs, Vol. 55, No. 1, pp348-363.

[5] C. Chan, and G.K.H. Pang, (2000) "Fabric Defect Detection by Fourier Analysis", IEEE Transactions On Industry Applications, Vol. 36, No. 5, pp1267-1276.

[6]   S. H. Choi, J.P.Yun, B Seo, Y. S Park, and S. W. Kim, (2007) "Real-Time Defects Detection Algorithm for High-Speed Steel Bar in Coil", World Academy of Science, Engineering and Technology, Vol. 25, pp66-70.

[7]   Y.Frayman, H. Zheng, and S. Nahavandi, (2006) "Machine Vision System for Automatic Inspection of Surface Defects in Aluminum Die Casting", Journal of Advanced Computational Intelligence and Intelligent Informatics, Vol. 10, No. 3, pp281-290.

[8]   M. H. Karimi, and D. Asemani, "Surface defect detection in tiling Industries using digital image processing methods: Analysis and evaluation", ISA Transactions, in press

[9]   C. Topal, and C. Akınlar, (2012) "Edge Drawing: A combined real-time edge and segment detector", J. Vis. Commun. Image R., Vol. 23, pp862–872.

[10]   H. Gündüz, S. Kaplan, S. Günal, and C. Akınlar, (2013) "Circular traffic sign recognition empowered by circle detection algorithm", 978-1-4673-5563-6/13.

[11]   B. Yuan, and M. Liu, "Power histogram for circle detection on images", Pattern Recognition, in press.

[12]   P. Mukhopadhyay, and B. B. Chaudhuri, (2015) "A survey of Hough Transform", Pattern Recognition, Vol. 48, pp 993-1010.

[13]   R. Samet, O.F. Bay, S. Aydin, S. Tural, A. Bayram, (2015) "Performance Analysis of GPU-based Parallel Image Segmentation using CUDA",   ICAT'15 (International Conference on Advanced Technology & Sciences), Antalya, Turkey.

[14]   R. Samet, O.F. Bay, S.Aydın, (2015) "Real-Time Image Processing Applications on Multicore CPUs and GPGPU", The 2015 International Conference on Parallel & Distributed Processing Techniques & Applications, Las Vegas USA.

[15]   L. Jiang, (2012) "Efficient randomized Hough transform for circle detection using novel probability sampling and feature points", Optik, Vol. 123, pp1834-1840.

[16]   R. Samet, A. Bayram, S. Tural, S. Aydin, (2016) "Primer Defects Detection on Military Cartridge Cases", NICOGRAPH International 2016. The 15th annual international conference, Hangzhou, China.

[17]   J.R. Parker, (2001) "Rank and response combination from confusion matrix data", Information Fusion, Vol. 1, No. 2, pp113-120.

[18]   G. Batista, R. C. Prati, M. C. Monard, (2004) "A study of the behavior of several methods for balancing machine learning training data", ACM SIGKDD Explorations Newsletter, Vol. 6, No. 1, pp20-29.

AUTHORS

Semra Aydin received her B.S. degree in Computer Systems Education from Gazi University, Turkey. She received the M.S. degree in Graduate School of Natural and Applied Sciences from Gazi University about distributed computing. She has been studying on the Ph.D. in Computer Science since 2010, at Gazi University. Her research interests focus on paralel computing, image processing, multicore processing and GPU programming.

Refik Samet received the BS and MS degrees in automation and control in technical systems from the National Technical University of Ukraine "Kyiv Polytechnic Institute" in 1983 and the PhD degree in computer science from the Institute of Control Sciences of Russian Academy of Sciences in 1992. He is professor in the Department of Computer Engineering, Ankara University. His current research interests include fault-tolerant systems analysis, parallel systems, image/video processing, mobile applications. He has been a member of the IEEE and the Computer Society since 2000.

Omer Faruk Bay received the B.Sc. degree in Electrical and Electronics Education from Gazi University, Turkey in 1985, M.Sc. and Ph.D. degrees in Electronics Engineering from Erciyes University, Turkey in 1992 and 1996 respectively. He is a full professor at the Department of Electronics and Computer Education in Gazi University. His research interests include artificial intelligence and their applications; control and instrumentation; intelligent systems, BCI for home automation and image processing. He has been worked at some national and international Projects as a manager and researcher. He has published more than 85 articles and published one book.
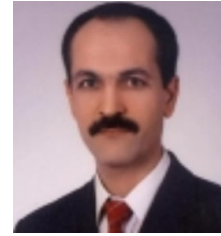
USING THE MANDELBROT SET TO GENERATE PRIMARY POPULATIONS IN THE GENETIC ALGORITHM AND REVERSE ORDER IN ORDER TO ENCRYPT THE IMAGE

Elaheh Aghamohammadi[1*], Zeinab Amani[1*], Maryam Rastgarpour[2]

[1]Ph.D. student Artificial Intelligence Computer Engineer,
Islamic Azad University E-Campus, Tehran, Iran
[2]Computer Engineering, Faculty Of Engineering,
Islamic Azad University, Saveh Branch, Saveh, Iran

ABSTRACT

Nowadays, finding a way to secure media is common with the growth of digital media. An effective method for the secure transmission of images can be found in the field of visual cryptography. There is a growing interest in the use of visual cryptography in security application. Since this method is used for secure transmission of images, many of the methods are developed based on the original algorithm proposed by Naor and Shamir in 1994. In this paper, a new hybrid model is used in cryptography of images which is composed of Mandelbrot algorithm and genetic algorithm. In the early stages of proposal, a number of encrypted images are made by using the Mandelbrot algorithm and the original picture and in the next stage, these encrypted images are used as the initial population for the genetic algorithm. At each stage of the genetic algorithm, the answer of previous iterations is optimized to get the best encoding image. Also, in the proposed method, we can achieve the decoded image by a reverse operation from the genetic algorithm. The best encrypted image is an image with high entropy and low correlation coefficient. According to the entropy and correlation coefficient of the proposed method compared with existing methods, it is observed that our method gets better results in both of them.

KEYWORDS

visual cryptography, genetic algorithm, Mandelbrot function, fractal, reversible genetic algorithm.

1. INTRODUCTION

With the rise of digital media, the need for methods to maintain such data seem necessary. Digital media sources link to the rich source of data which are offered by the internet and the range of the data are increasing day by day. These data can be simple text documents, images of people and so on. Internet provides an easy access to this required knowledge.

The field of visual cryptography is developed during the past few years. The main method was initially proposed by Naor and Shamir for binary images. This method offers a secure system in which secret messages are parts that are separately similar to random noise, but when they are properly placed on each other, their messages can be decrypted only by using the human visual system. While this method provides security for text and binary images, growth of digital media requires the development of these techniques to provide security for color and greyscale images. Through the development of the original method, visual cryptography provides a secure method to store and transfer text, binary images, gray and color images. Since the original method was developed in 1994, many changes and improvements were added to the available collection of visual encryption techniques. Many digital services require reliable security for the transfer and storage of digital images. Due to the rapid growth of the Internet in today's digital world, security of image has attracted a lot of attention. Prevalence of multimedia technologies in our society is caused digital images play a substantial role compared to the old texts which calls for serious protection of users' privacy is for all applications. Digital images' encryption techniques are very important that should be protected against unauthorized access attacks.

Digital images are exchanged on various types of networks that often a large part of these data is confidential or private. Encryption is a preferred technique to protect the transmitted data. There are various encryption systems to encrypt and decrypt data image. Today, images can be regarded as one of the usable forms of information. Image Encryption has various applications in different fields such as internet communications, multimedia systems, medical imaging, telemedicine and military communications and therefore, providing effective and secure protection for image files is one of the main concerns.

In proposed method, at first, the input images are combined with Mandelbrot fractal image then in terms of the size of the images, a series of random numbers is generated and in the next stage, pixel is selected with the use of these numbers in both of the rows and combined dual-point operation is performed on them. And finally, by using random numbers generated in the second step, the row of image pixels of previous step is dislocated that this act is similar to the mutation function in the genetic algorithm and in this way the encrypted image is obtained and if input images to be colorful, these acts are done on all three color components. In the decode step, at first the mutation function conducted at the encryption step is carried out inversely then, the two point combined action is also performed inversely. Finally, in order to achieve the original image, the Mandelbrot fractal image is subtracted from the generated image.

2. ENCRYPT IMAGES

The need for image encryption to securely transfer images across communication channels, such as Internet and wireless communications networks, is increasing, and due to the large amount of video and image data of traditional cryptographic algorithms, they do not have the required efficiency in this area. In this dissertation, a new method is proposed based on the integration of the Mandelbrot fractal image and genetic operators, which has the ability to encode images with a minimum correlation coefficient and maximum entropy.

Frectal

In mathematics, the object itself is exactly or nearly identical to that of itself. For example, a shape has the form of someone like its own parts or parts.

Many real-world objects, such as coastlines, are statistically similar, with some of them showing the same statistical characteristics on many scales. Stable on a scale or scale is a precise form of self-similarity. So that at each magnification there is a smaller piece of object that is geometrically similar or similar to the general one. Instead, one side of the snowflake, which is both symmetrical and stable, can grow steadily without change in shape.

A compact space with its topology X is the same if there is a set of bounded Ss that shows a disjoint cluster set. For If, we call ourselves the same as X if and only if the subgroup of Y is such that the equation is reserved for the above equation. In this case we have:

A self-constructed structure, such as a homogeneous one, may be a repeating function, which is the result of a repeating function system. A combination of functions of a monoidal algebraic structure creates. When the S set has only two factors, monoids are known as dynamic monoids. A dynamic monoid can be represented as infinite binary tree. In general, if the set p, S is a factor, the monoid may be represented as a p-adic tree. The Mandelbrot set is similar to its chihuahua points.

Self-similarity has important implications for the design of computer networks, and the typical network of traffic has its own characteristics. For example, in remote traffic engineering, packet switched data traffic patterns seem to be statistically similar. This means that the use of simple Poisson distribution models is inaccurate, and that networks that are designed to operate unexpectedly, regardless of self-similarity, are to some extent unexpected. Similarly, stock market volatility is defined as a self-similarity drama. For example, when they move from a special anchor conversion to a more detailed display, they appear as if they were. Many of their objects are like natural herbs. Real ferns are much closer to real self-similarity. Other plants, like flowers, are largely the same

Mandelbrot fractal model

Mandelbrot, when studying a study of the length of British coasts, concluded that when measured on a large scale this length is greater than that at a smaller scale. This disorder caused the creation of a mathematical branch of the disorder theory called fractal. This term was first introduced in 1975 by the Polish mathematician, Bennett Mendel Brut. The term fractal is derived from the Latin Latin fractus or fractal meaning a broken or broken broken stone. The Dictionary of Persian and Farsi has approved the word bhakal for fractals. Fractals are the forms that, unlike the Euclidean geometric forms, are not at all regular. These forms are, firstly, all irregular and, secondly, their degree of disorder is the same at all scales. In his explanation of his theory, Mandelbrot emphasized the choice of the phrase fractal on one of the main characteristics of this geometric form, which is due to the nature of the piece, fragmentation. In his opinion, the universe and all natural phenomena are somewhat fractal. He has stated that the clouds are not like Korea, the mountains are not like cones, the shores of the sea are not circular, the skin of the tree is not smooth, and the lightning does not move in a straight line. Observing the nature of the nature, it is clear that Euclidean geometry can not explain the complex and apparently

disorganized forms. Euclidean geometry (the full sphere of spheres, pyramids, cubes and cylinders) is not the best way to show natural elements. The clouds, the mountains, the coastline and the trunk of trees are all contradictory with Euclidean currents, and not smooth, but rugged, and this disorder brings in small scales, which is one of the most important features of fractals. This means that fractal geometry, in contrast to Euclidean geometry, is a better way of explaining and creating phenomena like nature. The language to which this geometry is expressed is called an algorithm that can be translated into simpler formulas and rules with compound objects. Fractals are elements whose spatial form is not smooth. Therefore, they are also called "irregular", and this irregularity is repeated geometrically and in a variety of scales within the pyramid. Every natural thing around us is essentially a fractal. Because straight lines and planes exist only in the ideal mathematical world. Along with this theory, any system that can be geometrically imagined and analyzed can be a fractal. The world in its general form of physical (material) is chaotic, irregular, irregular, but behind this initial mentality there is a coherent and conservative law that is based on order and has a clear combination. The best way to define a fractal is to pay attention to its attributes and symptoms. An "irregular" fractal means that there is no flat part in it. The fractal is "self-similar", which means that the "components" are similar to the whole. The fractal body is seen from far and near the same. In other words, it is similar. When we approach a fractal object, small pieces of it from the round are thought to be massive grains, they are physically depicted in a manner more or less like the image seen from the far side. In nature, there are many examples of fractals. Trees, clouds, mountains, rivers, the edges of the beaches, and bullets are all fractal objects. A small part of a tree whose branch is similar to the whole tree. This example can be used for clouds, bullets, thunderbolts and other fractal objects. Many artificial human hand elements are also fractal. Celican chips, the stock market volatility curve, the growth of cities, and finally the Sarpinsky triangle. The Serpinsky Triangle is an equilateral triangle, with the points in the middle of its side connected to each other. If this action continues within the triangles of the new trivial to infinite, triangles are always obtained that are similar to the first triangle. In mathematical science, fractal is a complex engineering complex with similar details in its structure on any scale. The degree of disorder is far from one and the same .

Mandelbrot, when studying a study of the length of British coasts, concluded that when measured on a large scale this length is greater than that at a smaller scale. This disorder caused the creation of a mathematical branch of the disorder theory called fractal. This term was first introduced in 1975 by the Polish mathematician, Bennett Mendel Brut. The term fractal is derived from the Latin Latin fractus or fractal meaning a broken or broken broken stone. The Dictionary of Persian and Farsi has approved the word bhakal for fractals. Fractals are the forms that, unlike the Euclidean geometric forms, are not at all regular. These forms are, firstly, all irregular and, secondly, their degree of disorder is the same at all scales. In his explanation of his theory, Mandelbrot emphasized the choice of the phrase fractal on one of the main characteristics of this geometric form, which is due to the nature of the piece, fragmentation. In his opinion, the universe and all natural phenomena are somewhat fractal. He has stated that the clouds are not like Korea, the mountains are not like cones, the shores of the sea are not circular, the skin of the tree is not smooth, and the lightning does not move in a straight line. Observing the nature of the nature, it is clear that Euclidean geometry can not explain the complex and apparently disorganized forms. Euclidean geometry (the full sphere of spheres, pyramids, cubes and cylinders) is not the best way to show natural elements. The clouds, the mountains, the coastline and the trunk of trees are all contradictory with Euclidean currents, and not smooth, but rugged, and this disorder brings in small scales, which is one of the most important features of fractals. This means that fractal geometry, in contrast to Euclidean geometry, is a better way of explaining

and creating phenomena like nature. The language to which this geometry is expressed is called an algorithm that can be translated into simpler formulas and rules with compound objects. Fractals are elements whose spatial form is not smooth. Therefore, they are also called "irregular", and this irregularity is repeated geometrically and in a variety of scales within the pyramid. Every natural thing around us is essentially a fractal. Because straight lines and planes exist only in the ideal mathematical world. Along with this theory, any system that can be geometrically imagined and analyzed can be a fractal. The world in its general form of physical (material) is chaotic, irregular, irregular, but behind this initial mentality there is a coherent and conservative law that is based on order and has a clear combination. The best way to define a fractal is to pay attention to its attributes and symptoms. An "irregular" fractal means that there is no flat part in it. The fractal is "self-similar", which means that the "components" are similar to the whole. The fractal body is seen from far and near the same. In other words, it is similar. When we approach a fractal object, small pieces of it from the round are thought to be massive grains, they are physically depicted in a manner more or less like the image seen from the far side. In nature, there are many examples of fractals. Trees, clouds, mountains, rivers, the edges of the beaches, and bullets are all fractal objects. A small part of a tree whose branch is similar to the whole tree. This example can be used for clouds, bullets, thunderbolts and other fractal objects. Many artificial human hand elements are also fractal. Celican chips, the stock market volatility curve, the growth of cities, and finally the Sarpinsky triangle. The Serpinsky Triangle is an equilateral triangle, with the points in the middle of its side connected to each other. If this action continues within the triangles of the new trivial to infinite, triangles are always obtained that are similar to the first triangle. In mathematical science, fractal is a complex engineering complex with similar details in its structure on any scale. The degree of disorder is far from one and the same.

3. IMAGE DECODING

In this section, all the processes and processes in the encryption section are reversed. First, the encoded image is loaded and the Fibonacci random string is created using the golden code, and then the image of the fractal is created. In the next step, based on the generated string, the mutation operation is reversed and the encryption section is applied to the encrypted image. Then the intersection operation is inversely applied to the pixel rows of the encrypted image. And these apply to all the pixels in the images. So, in order to achieve the original image, we need to subtract the image of Mendel Bert's fractal image from the encoded image, which is done by subtracting the pixel into the pixel and capturing the original image.

4. CRYPTOGRAPHY

Cryptography is the science of codes and ciphers and an ancient art and it is used for centuries to protect the messages that were exchanged between the commanders, spies, lovers and others to make their messages confidential. When data security is discussed, it is necessary to prove the identity of the sender and receiver of the message and also, to be sure not to change the content of the message. The three issues of confidentiality, authentication and integrity are at the heart of modern data communications security and can use encryption (8). This issue should be ensured that a message can only be read by those for whom the message was sent, and others are not allowed. Cryptography is the provider of this issue.

Cryptography is the art of writing in an encrypted format so that no one except the intended recipient cannot read the message content. Cryptography has two main components including algorithm and key. The algorithm is a converter with mathematical formula. The key is a string of binary digits (one and zero) which in itself is meaningless (7). Modern cryptography assumes that algorithm is known or can be discovered. It is the key that should be kept secret or varies at each stage of implementation. Decryption may use the same pair of algorithm and key or different pair (1, 2).

Areas of Cryptography
Issues related to the field of cryptography can be proposed and considered at different levels (7). At the first level, a number of the paradigm such as symmetric cryptography, asymmetric cryptography and mixture exist and at the second level, a number of algorithms such as RSA and DES exist and protocols and standards are established at the third level. At the fourth level, applications or other protocols are created on these protocols. Maybe algorithm to be good, the protocol to be well-defined and established, but at the level of implementation of the application not to be good. Therefore, every level requires a degree of quality, performance, and confidence and creating influence on the systems may naturally return to each of these levels (2).

The terms used in Cryptography

Cryptology: The science of the study of cryptography and decryption

Password device: a system that is created to encrypt and decrypt data.

Cryptography: It is the art and science of mathematical techniques related to the concepts of data security like confidentiality, data integrity, authentication, non-repudiation.

Decryption: The study of methods that are used to break the encryption techniques
Cryptographer: A person who is studying the systems and versions of encryption.

Decrytor: A person who is malicious at decoding and analysis of codes.

Cryptography: The encryption process of messages in a way that it's content to be hidden from foreigners.

Decryption: The process of recovering plaintext from the ciphertext.
Symmetric encryption algorithm: symmetric encryption algorithms or private key encryption use a key to encrypt and decrypt of data.

Asymmetric cryptography algorithm: Asymmetric Cryptography algorithm or public key cryptography algorithm uses different keys to encrypt and decrypt of data and decryption key cannot be derived from the encryption key (1,3).

DES, Triple-DES, SHA-1, RSA are the public key algorithm and RSA is the most famous public key algorithm that is used for encryption and digital signature. RSA calculations are done with integers $n = p * q$ for large prime numbers p and q. To encrypt the message of m, it reaches to the view of a public small view of e.

To decrypt, the receiver of cipher text of C = me (mod n), calculates reverse of d = e-1 (mod (p-1) * (q-1)) and obtains the amount of Cd = me * d. The private key includes m (mod n) e, q, n, p, d. The public key only includes e, n (1, 13).

Cryptographic Methods
Symmetric method: In this method both sender and receiver of information have a common key for encryption and decryption. In this state, the encryption and decryption of information are two reverse process. Key transition between each other by intranet or physically is somewhat safe. But its transmission by internet is not correct (4). In such systems, the keys for encryption and decryption are same or have very simple relationship with each other. Symmetric encryption is used to encrypt large amounts of data. When it is used with a digital certificate, the confidentiality of information is protected. When electronic signature is used, the message integrity is guaranteed (2).

Advantages: High speed during the encryption, key generated randomly and fast.

Disadvantages: a plurality of keys for the members of each connection, key distribution among communicating parties.

Asymmetric method: This method was created to solve the problem of key transfer in symmetric method. In this method, instead of a shared key a pair of public and private key is used. In this method, the public key is used for encryption of information. The one who intends to transfer information in an encrypted form, encodes information and sends to the person who is the owner of the key pair. The owner of key maintains the private key for himself in a confidential form. In this method, the encryption and decryption keys are distinct (2).

Advantages: No need to distribute and send key.

Disadvantages: low speed in high volume of data, the complexity of key generation.

The suggested process for image encryption in this method
The need for image encryption to securely transmit images over communication channels such as internet networks and wireless communications networks is increasing and due to the high volume of image and video data the traditional encryption algorithms do not enjoy the necessary efficiency in this regard (53).

In this study, a new method is proposed based on a combination of Mandelbrot fractal image and genetic operators with the ability to encrypt images with minimal correlation coefficient and maximum entropy. In Figure 1, the overall chart of image encryption stages of the proposed method is displayed. Then, the stages of image encryption system are completely explained.

Combining the original image with the image of Mandelbrot
At this stage, the input images with Mandelbrot fractal image that have the same size are gathered pixel by pixel and the remaining pixel of original image with pixel of Mandelbrot image is calculated to number of 255 for each pixel of output image. And for color images, these actions are calculated for triple RGB colors.
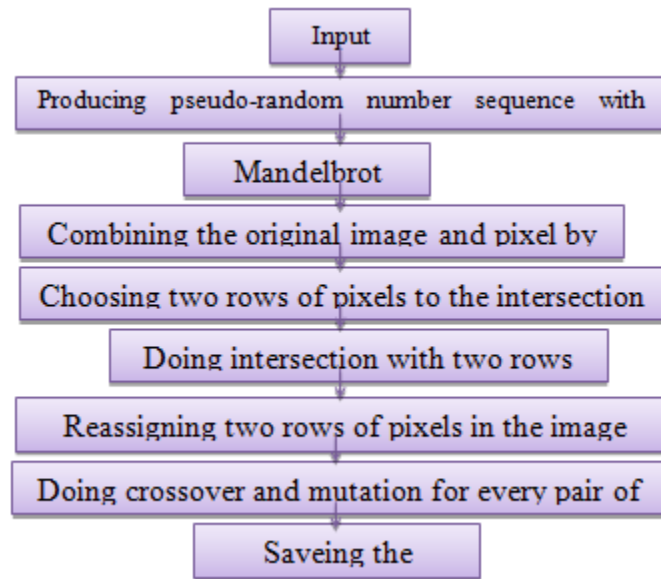
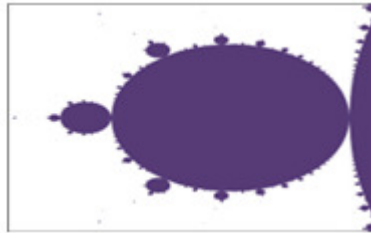Figure 1. The overall chart of the encryption system of the proposed system

Figure 2. Self-resemblance in Mandelbrot collection.

Numerical code generation for encryption and decryption
At this stage, a series of Fibonacci random numbers are produced in relation to the size of the input images and the golden key that these numbers are used in the later stages.

Fibonacci series
In mathematics, Fibonacci series are a sequence of numbers that are defined as follows:

$$F(n) := \begin{cases} 0 & \text{if } n = 0; \\ 1 & \text{if } n = 1; \\ F(n-1) + F(n-2) & \text{if } n > 1. \end{cases}$$

In which except the two prime numbers, the next numbers are obtained from sum of their previous two numbers. The first numbers of the series are: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, ... These numbers are named to the name of Italian mathematician Leonardo Fibonacci.

Double point crossover operator on rows of output images
At this stage, by using the code generated in previous stage, at first, two rows of pixels as two chromosomes become ready for crossover action and to determine the crossover pixel, at first, the number of row of each chromosome is divided to 255 and is multiplied in the number of pixel of

each row (the number of genes) and the number of pixel is achieved for double point crossover action. This is achieved for all pixel rows and for each three RGB color channels.

Mutation operator on the output images
At this stage, by using the code generated in the second stage, the row of pixels of images of previous step is dislocated and this is obtained for all row of pixels and for three RGB color channels. In Figure 3, an example of mutation operator is shown on the two rows of pixels of the image.
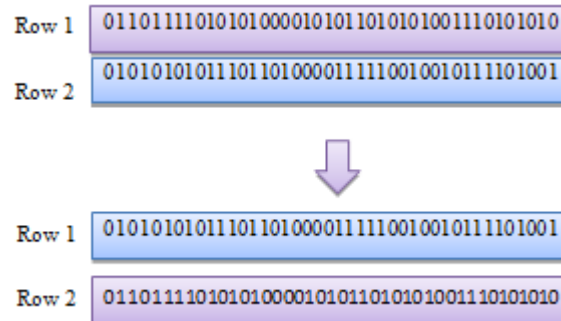
Figure 3. An example of mutation operator on two rows of pixels of the image

Finally, the encrypted image is created by using a combination of input images with Mandelbrot fractal image and operators of genetic algorithm. Figure 4 shows an example of the input image and the encrypted image

Figure 4. An example of the input image and the encrypted image

Decoding image
In this section, all the steps and processes in the encryption are performed inversely. At first, the encrypted image is loaded and the sequence of Fibonacci random numbers are created by using the golden code, then the Mandelbrot fractal image is created. In the next stage, based on the sequence of produced numbers, mutation operation is inversely applied and contrary to the encryption part on encrypted image. Then, the crossover practice is also applied in reverse form on pixel rows of encrypted image and this is applied to all the rows of pixels of the images. Finally, in order to achieve the main image the Mandelbrot fractal image should be subtracted from encrypted image and this action is done by pixel by pixel subtraction. Figure 5 shows the overall chart of steps involved in images decoding. In the following the details of each section are explained.
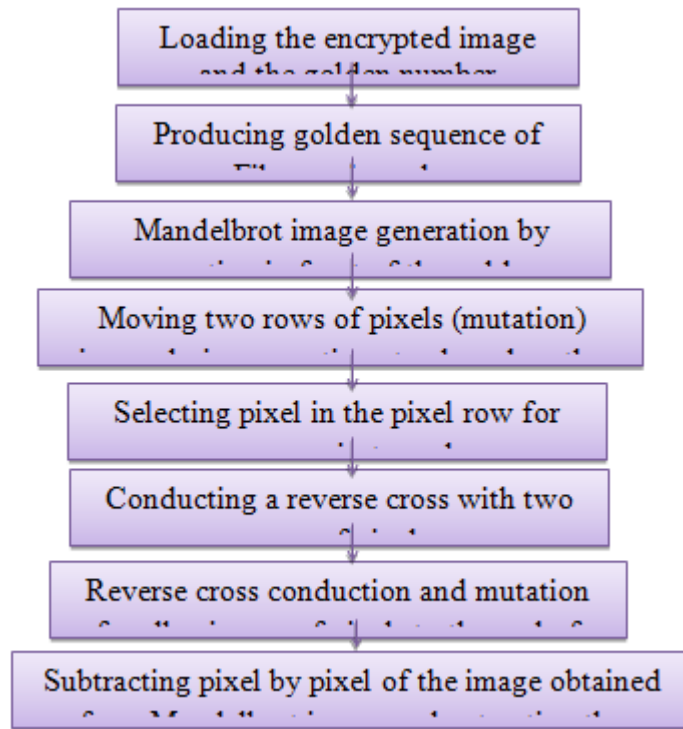
Figure 5. The overall chart of decoding system of the proposed system.

The production of the sequence of Fibonacci random numbers

At this stage, after loading the encrypted image and the golden number, such as the encryption section, the sequence of Fibonacci random numbers is produced.

Reverse mutation operator on encrypted images

At this stage, by using a series of randomly generated code, the pixels' row of encrypted images is displaced that this operation causes the row of pixels returns to its own true location. Also, this action is performed for all rows of pixels of images and for each of the three RGB color channels.

Reverse double point crossover operator on rows of encrypted images

By using randomly generated code sequence, at first, two rows of pixel as two chromosomes become ready for crossover action and in order to determine the crossover pixel, the number of row of each chromosome is initially divided to 255 and is multiplied in the number of pixel of each row (the number of genes) and the number of pixel is achieved for double point crossover action. This action is achieved for all rows of pixels and for each three RGB color channels.

Discretization of the original image from the Mandelbrot image

At this stage, the original image is subtracted from the Mandelbrot image that are at the same size and the decoded image is obtained by combining the Mandelbrot fractal image with genetic algorithm operators. Figure 6 displays an example of the encrypted image and decrypted image.
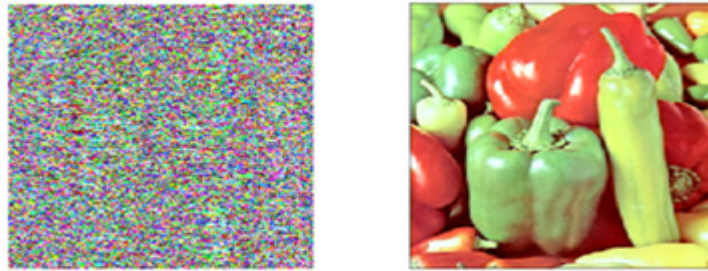
Figure 6. An example of the encrypted image and decrypted image

The performance and efficiency of proposed system are tested by using different parameters and criteria and the results obtained in each part are discussed and analyzed.

Collection of images

To evaluate and test the performance of the proposed system and also to compare with other methods the known images in this area are used. These images are being used in most of the articles and are suitable to evaluate the performance of systems. Images used in the gray area include Lena, Peppers, Baboon, House, Boat and Photographer and color images include Peppers, Baboon, Lena and Airplane. In Figure 7 the gray images used in the experiments of proposed system and in Figure 2 the color images are shown.

Figure 7. The gray images used in the experiments of proposed system

Evaluating the proposed system

Among the important criteria in images cryptographic operations can point to the calculation of the amount of entropy of encrypted images, correlation coefficient of the original image and encrypted image, the amount of PSNR original image and the decrypted image and also, histogram of the encrypted image. The proposed system is evaluated based on the mentioned criteria and on the gray and color images' levels. In the following the details of the results of the proposed system are presented.

Entropy of the encrypted images

Information entropy in theory of the information is in connection with the fact that a signal or a random event to what extent is random. In fact, information entropy reports the randomness rate

as a mathematical evaluation. One of the goals of the image encryption topic is data encryption in a way that the encrypted image contains maximum entropy. In other words, the more entropy amount, the more chaos or randomness of pixels of images. This causes the information of the original image not to be recognizable from encrypted image and access to the original image by using statistical analysis to be minimized. In Table 1, the entropy rate of encoded images is shown in the sample images.

Table 1. The results of the proposed system based on the selected criteria

Entropy	Input Image
7.8938	Peppers
7.9057	Lena
7.7937	house
7.8940	Baboon
7.8944	Boat
7.9004	Photographer

Correlation between the original image and encrypted image
The correlation coefficient is statistical tools to determine the relevance of a quantitative variable with another quantitative variable. The correlation coefficient is one of the criteria used to determine the correlation between two variables. It displays the intensity of correlation and this coefficient is between 1 and -1 and in the case of the lack of relationship between two variables is zero. The correlation coefficient of two images is used to investigate the relationship between the encrypted image and the original image. In our study, the aim is to reach a value close to zero and this proves the lack of connections and similarities between the two images. The correlation coefficient close to zero indicates that the encrypted images do not have the features of the original image and by using statistical analysis the original image data cannot be achieved. Table 2 displays the correlation coefficient data of the selected gray level images.

Table 2. Results of the proposed system based on selective criteria

Correlation Coefficient	Input Image
0.0010	Peppers
0.0198	Lena
0.0163	house
0.0111	Baboon
0.0097	Boat

Histogram Analysis

Histogram is a graphical representation of the number of pixels for each brightness level in the input image. For example, gray level images have 256 brightness levels, so each image pixel can have a value in the range of 0 to 255. In the histogram, the horizontal vector is 0 to 255 and that represents the intensity of the images pixels brightness and the vertical diagram showing the frequency of the intensity of the light and the amount depends on the input images. . In the context of the encryption of images, the purpose of encoding images is to not recover any image from the original images from the encrypted image. The histogram can also display the pixel data of the image. Hence the histogram of the encoded image and the original image must be different. The more histograms the encoded images have in a more uniform state, the less information is displayed and more suitable for this field. It is also worth noting that the uniformity of the histogram diagram and the entropy of the image have a direct proportion, hence, the more entropy the image is, the more the histogram of the image becomes even more smooth. The following diagrams show histograms for main images, encrypted images and decoded images.
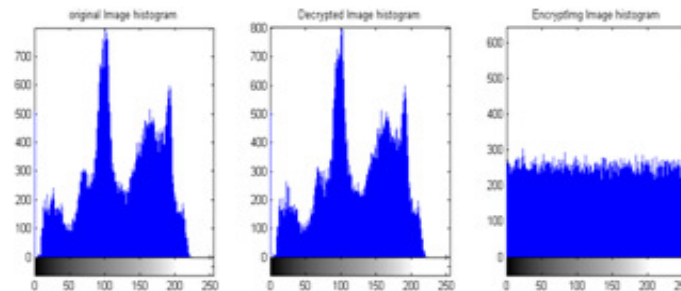
Figure (8): Histogram of the Peppers image, left histogram of the original image, decoded image and encoded image
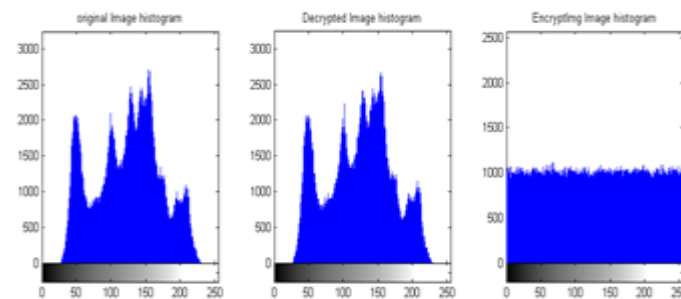
Figure (9): Histogram of the Lena image, left histogram of the original image, decoded image and encoded image.
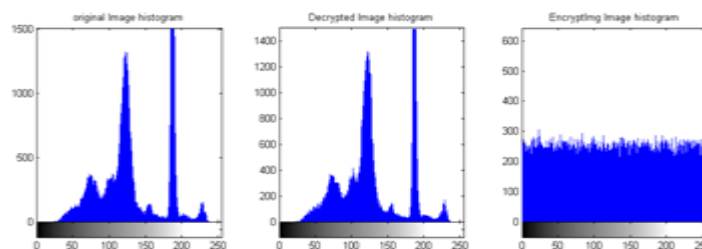
Figure (10): The histogram of the House image, from the left of the histogram of the original image, the decoded image and the encoded image
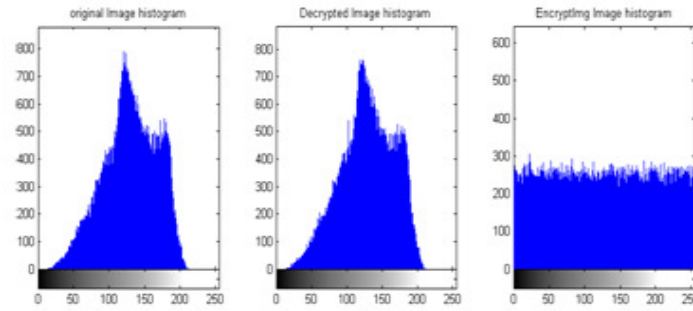
Figure (11): Histogram of the Baboon image, left histogram of the original image, decoded image and encoded image

As shown in the pictures, the histograms of the cropped images are uniform and smooth. In this case, no histogram of encrypted images can be recovered.

The simulation results

Finally, the outputs images of proposed system include encoded images and decoded images which are shown in Figure (12).
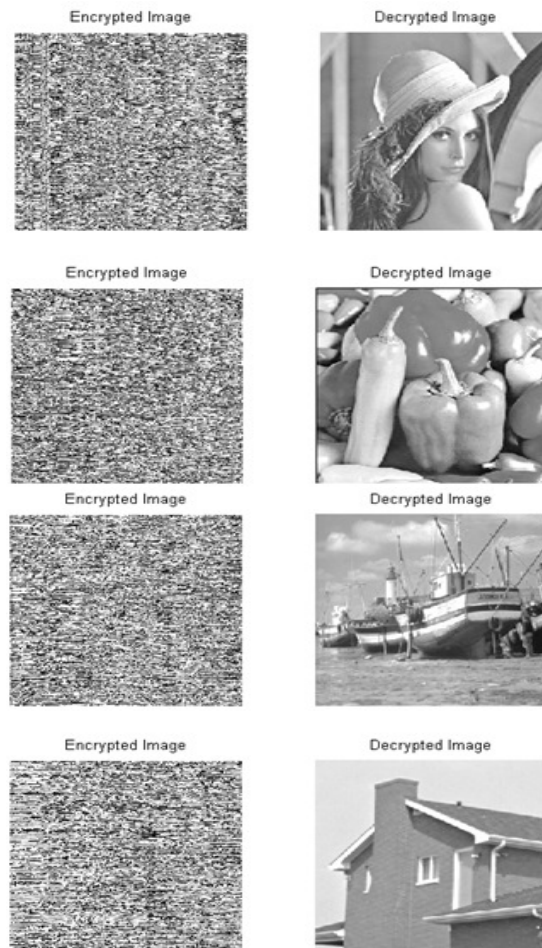

Figure 12. The outputs images of proposed system

A comparison of the proposed method and other methods

In order to investigate the tests results of the proposed system compared to the former provided systems, the test results of previous methods are obtained based on the listed criteria. The results of the proposed system and the system (35) are displayed in the Tables 3 and 4 according to the correlation coefficient and entropy for images of Lena and Baboon.

Table 3. The results of the proposed system and system based on the selected criteria on the Lena image

The method used	Correlation Coefficient	Entropy
The proposed method	0.0198	7.9057
Method (56)	0.0135	7.9822

Table 4. The results of the proposed system and system based on the selected criteria on the Peppers image

The method used	Correlation Coefficient	Entropy
The proposed method	0.0010	7.8938
Method (56)	0.0119	7.9873

As can be seen in Tables 5-3 to 5-4, the results of proposed system compared to the articles (56) and (57) have achieved better results in relation to the mentioned criteria.

1-5-1 Results of testing the proposed system on color images

The proposed system also has the ability to encode color images. There are three components of red, green, and blue color in the color images, each of which is a gray level image. In order to encode color images, the proposed algorithm applies to all three color components of the images and encodes the images. In Table 5, the proposed system results are displayed on Peppers, Baboon, Lena, and Airplane color images.

Table 5: Results of proposed system based on selected criteria on color images

Input Image	Entropy
Peppers	7.9368
Lena	7.8055
Airplane	7.9175
Baboon	7.7632

In Figures 13 and 14, histogram histograms are shown for the Lena and Baboon color images. In the form shown, the left histogram of the main images is displayed for all three color components, encoded images and decoded images. .
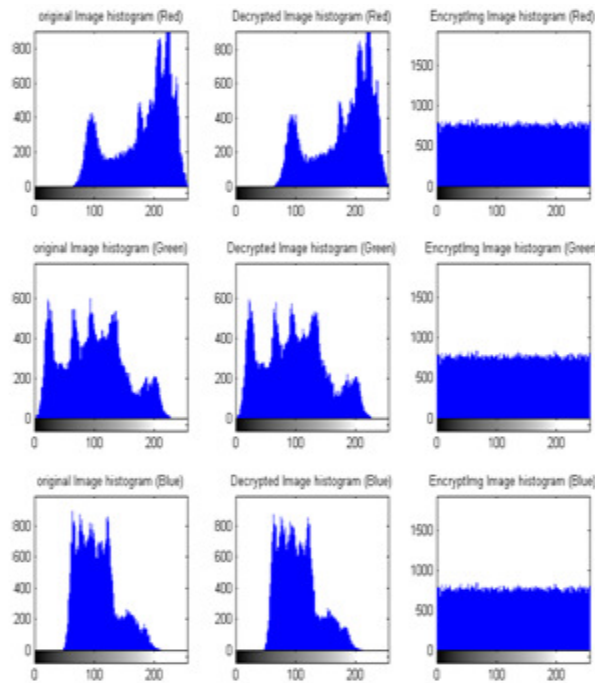

Figure 13: The histogram of the Lena color image, the left side of the main image histogram, the decoded image and the encoded image for each of the three color image components
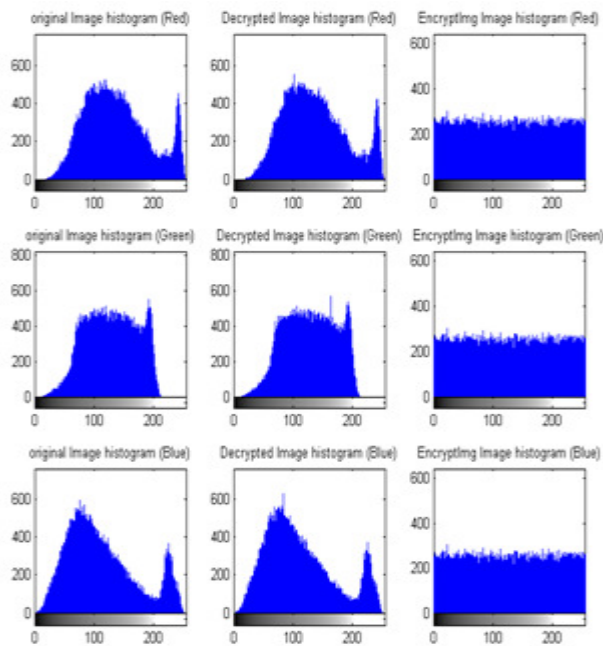

Figure 14: The Baboon color image histogram, from the left side of the main image histogram, the decoded image and the encoded image for each of the three color image components

Table 6 shows the selected color correlations correlation coefficient.

Table 6: Results of the proposed system based on the correlation coefficient on the components of color images

Input Image	Red	Green	Blue
Peppers	0.0034	−0.0037	−0.0019
Lena	−0.0043	−0.0056	−0.0037
Airplane	−0.0022	−7.6437e−04	4.2443e−04
Baboon	0.0032	−5.1269e-04	0.0017

In Figure 15, several examples of encoded and decoded color images are displayed
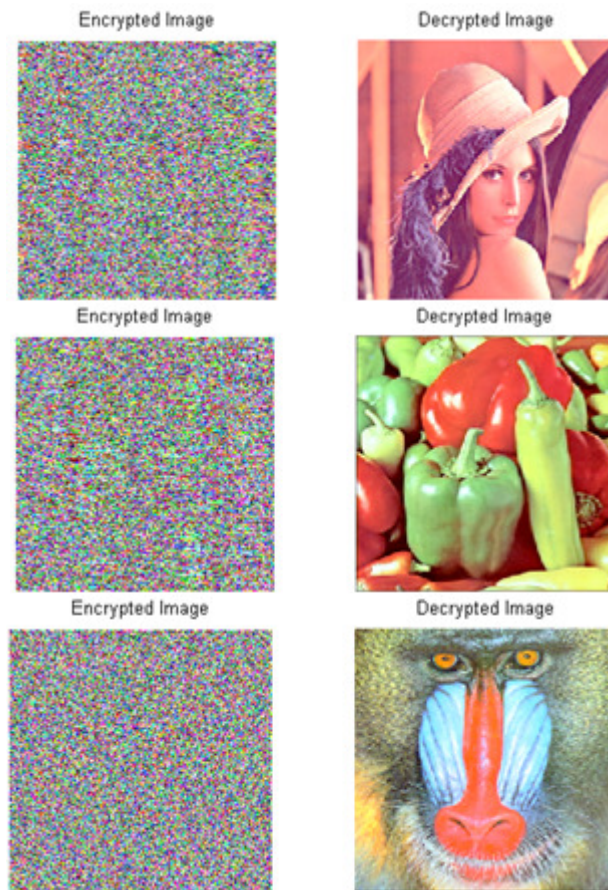
Figure 15: Output images of the proposed system on color images

5. CONCLUSION

In this paper, a method was presented based on fractal theory and operators of genetic algorithm to encrypt images. At first, in the proposed method the input images are combined with Mandelbrot fractal image then, according to the size of the images, a series of random numbers are generated that in the next stage, by using these numbers in each step two rows of pixel are selected and double point combined operations are performed on them. Finally, by using random numbers generated in the second stage, the row of pixels of the image of previous step is dislocated that this act is as mutation practice in genetic algorithm and the encrypted image is obtained in this way. If input images to be colored, this act is done on all three color components. In the decode step at first, the mutation practice conducted at the encryption step is done reversely then the double point combined operation is done in reverse form. Finally, in order to achieve the original image, Mandelbrot fractal image is subtracted from the generated image. The proposed system was evaluated by using the criteria used in these areas and also was compared with similar systems and according to various criteria, the proposed system can obtain the acceptable and appropriate values based on various criteria and compared with previous similar methods, the proposed method could also get better results based on the mentioned criteria.

REFERENCES

[1]   J. Weir, W. Yan, "A comprehensive study of visual cryptography", Transaction on DHMS V, LNCS, Springer, pp. 70-105, 2010.

[2]   C.M. Hu, W.G.Tzeng, "Cheating prevention in visual cryptography", IEEE Transactions on Image Processing 16(1), pp. 36–45, 2007.

[3]   A. Campbell, The Designer's Lexicon. Chronicle Books, San Francisco, 2000.

[4]   W. Qiao, H. Yin, H. Liang, "A Kind Of Visual Cryptography Scheme For Color Images Based On Halftone Technique", International Conference on Measuring Technology and Mechatronics Automation 978-0-7695-3583-8/09, pp. 393-395, 2009.

[5]   J. S. Lee, T. H. Ngan Le, "Hybrid (2, N) Visual Secret Sharing Scheme For Color Images", 978-1-4244-4568-4/09, IEEE, 2009

[6]   P. S. Revenkar, A. Anjum, W. Z. Gandhar, "Survey of visual cryptography schemes", International Journal of Security and Its Applications, Vol, 4, No. 2, 2010.

[7]   Wikipedia, "Mandelbrot Set", http://en.wikipedia.org/wiki/Mandelbrot_set.

[8]   R.J. Chen, W.K. Lu, J.L. Lai, "Image encryption using progressive cellular automata substitution and SCAN", In: IEEE international symposium on circuits and systems, 2005.

[9]   R. Enayatifar, "Image encryption via logistic map function and heap tree", Journal of the Physics Science, pp. 221–8, 2011.

[10] Z. Liu, L. Xu, C. Lin, J. Dai, S. Liu, "Image encryption scheme by using iterative random phase encoding in gyrator transform domains", Optics and Lasers in Engineering 49, pp.542–6, 2011.

[11] H. Li, Y. Wang, "Double-image encryption based on discrete fractional random transform and chaotic maps", Optics and Lasers in Engineering 49, pp.753–757, 2011.

[12] Z. J. Liu, Q. Guo, L. Xu, "Double image encryption by using iterative random binary encoding in gyrator domains", Optics Express 18, pp.12033–12043, 2010.

[13] J. Koljonen, "Comparison of nearest point algorithms by genetic algorithms", Expert Systems with Applications 38, pp.10303–10311, 2011.

[14] D. Ashlock, J. Alexander Brown, "Fitness functions for thee Mandelbrot set", IEEE Transaction, 2011.

[15] http://en.wikipedia.org/wiki/Fractal.

[16] A. H. Abdullah, R. Enayatifar, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," AEU - International Journal of Electronics and Communications, vol. 66, pp. 806-816, 10// 2012

Attachments images:
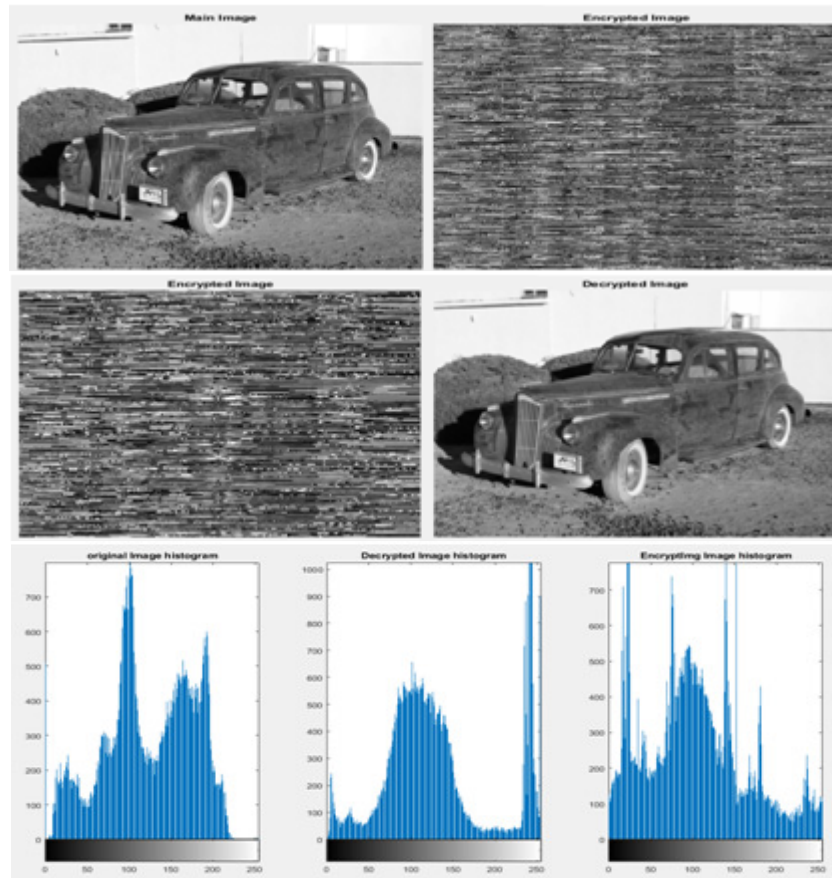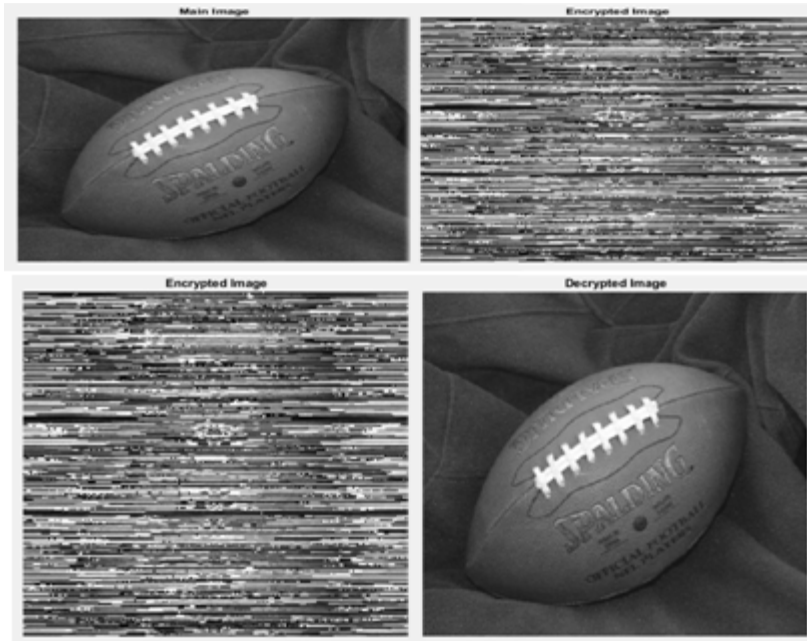
DISTRIBUTED KERNEL K-MEANS FOR LARGE SCALE CLUSTERING

Marco Jacopo Ferrarotti[1], Sergio Decherchi[1, 2]and Walter Rocchia[1]

[1]Istituto Italiano di Tecnologia, Genoa, Italy
[2]BiKi Technologiess.r.l, Genoa, Italy

ABSTRACT

Clustering samples according to an effective metric and/or vector space representation is a challenging unsupervised learning task with a wide spectrum of applications. Among several clustering algorithms, k-means and its kernelized version have still a wide audience because of their conceptual simplicity and efficacy. However, the systematic application of the kernelized version of k-means is hampered by its inherent square scaling in memory with the number of samples. In this contribution, we devise an approximate strategy to minimize the kernel k-means cost function in which the trade-off between accuracy and velocity is automatically ruled by the available system memory. Moreover, we define an ad-hoc parallelization scheme well suited for hybridcpu-gpustate-of-the-art parallel architectures. We proved the effectiveness both of the approximation scheme and of the parallelization method on standard UCI datasets and on molecular dynamics (MD) data in the realm of computational chemistry. In this applicative domain, clustering can play a key role for both quantitively estimating kinetics rates via Markov State Models or to give qualitatively a human compatible summarization of the underlying chemical phenomenon under study. For these reasons, we selected it as a valuable real-world application scenario.

KEYWORDS

Clustering, Unsupervised Learning, Kernel Methods, Distributed Computing, GPU, Molecular Dynamics

1. INTRODUCTION

Grouping unlabelled data samples into meaningful groups is a challenging unsupervised Machine Learning (ML) problem with a wide spectrum of applications, ranging from image segmentation in computer vision to data modelling in computational chemistry [1]. Since 1957, when k-means was originally introduced, a plethora of different clustering algorithms arose without a clear all-around winner.

Among all the possibilities, k-means as originally proposed, is still widely adopted mainly because of its simplicity and the straightforward interpretation of its results. The applicability of such simple, yet powerful, algorithm however is limited by the fact that, by construction, it is able to correctly identify only linearly separable clusters and it does require an explicit feature space (i.e. a vector space where each sample has explicit coordinates).

To overcome both these limitations one can take advantage of the well-known kernel extension of k-means [2]. Computational complexity and memory occupancy are the major drawbacks of

kernel k-means: the size of the kernel matrix to be stored together with the number of kernel function evaluations scales quadratically with the number of samples. This computational burden has historically limited the success of kernel k-means as an effective clustering technique. In fact, even though the potential of such approach has been theoretically demonstrated, few works in the literature [3] explore possibly more efficient approaches able to overcome the $O(N^2)$ computational cost.

We selected a real-world challenging application scenario, namely Molecular Dynamics (MD) simulations of biomolecules in the field of computational chemistry. Such atomistic simulations, obtained by numerical integration of the equations of motion, are a valuable tool in the study of biomolecular processes of paramount importance such as drug-target interaction [4]. MD simulations produce an enormous amount of data in the form of conformational frames (i.e. atoms positions at a given time step) that need to be processed and converted into humanly readable models to get mechanistic insights. Clustering can play a crucial role in this, as demonstrated by the success of recent works [1] and by the popularity of Markov state models [5]. We stress the fact that kernel k-means, without requiring an explicit feature space, is particularly suited for clustering MD conformational frames where roto-translational invariance is mandatory.

We introduce here an approximated kernel k-means algorithm together with an ad-hoc distribution strategy particularly suited for massively parallel hybrid CPU/GPU architectures. We reduce the number of kernel evaluations both via a mini-batch approach and an a priori sparse representation for the cluster centroids. As it will be clear, such twofold approximation is controlled via two straightforward parameters: the number of mini-batches B and the sparsity degree of the centroid representation s. These two knobs allow to finely adapt the algorithm to the available computational resources to cope with virtually any sample size.

The rest of the paper is organized as follow: in section 2, we briefly review the standard kernel k-means [2] [6] algorithm. In section 3 our approximate approach is introduced together with a detailed description of the proposed distribution and acceleration strategy. Section 4 contains the assessment of both the approximation degree and the performances on standard ML datasets and a real case MD scenario. A discussion section together with conclusions complete the work.

2. KERNEL K-MEANS

Given a set X of data samples $x_i \in \mathbb{R}^d, i \in [1, N]$, a non-linear transformation $\phi(x_i): \mathbb{R}^d \to \mathbb{R}^{d'}$ and said C the number of clusters to be found, the kernel k-means algorithms finds a set W of centroids $w_j \in \mathbb{R}^{d'}, j \in [1, C]$ in the transformed space, minimizing the following cost function:

$$\Omega(W) = \sum_{i=1}^{N} \sum_{j=1}^{C} \| \phi(x_i) - w_j \|^2 \, \delta(u_i, j) \tag{1}$$

Where u_i is the index of the closest prototype (i.e. the predicted label for sample i-th) obtained as:

$$u_i = \underset{j}{argmin} \| \phi(x_i) - w_j \|^2 \tag{2}$$

and $\delta(u_i, j)$ is the usual Kronecker delta.

A Gradient Descent (GD) procedure can be used in order to locally minimize the non-convex cost $\Omega(W)$ starting from an initial set of cluster prototypes $W_0 = \{w_{j,0}\}$ so that at the t-th iteration we have:

$$w_{j,t} = \frac{1}{|w_{j,t}|} \sum_{i=1}^{N} \phi(x_i) \delta(u_{i,t}, j) \tag{3}$$

where the j-th cluster cardinality is indicated as $|w_j| = \sum_{i=1}^{N} \delta(u_i, j)$.

A self-consistent update equation can be derived substituting Eq.3 into Eq.1:

$$
\begin{aligned}
u_{i,t+1} &= \arg\min_j \{\frac{1}{|w_{j,t}|^2}\sum_{m,n} K_{m,n}\delta(u_{m,t}, j)\delta(u_{n,t}, j) - \frac{2}{|w_{j,t}|}\sum_m K_{i,m}\delta(u_{m,t}, j)\} \\
&= \arg\min_j g_{j,t} - 2f_{(i,j),t}
\end{aligned}
\tag{4}
$$

Where the inner product in the transformed space $< \phi(x_m), \phi(x_n) >$ was replaced with a generic Mercer kernel $K(x_m, x_n) = K_{m,n}$ and where we introduced the cluster compactness and cluster average similarity respectively defined as:

$$
g_j = \frac{1}{|w_j|^2}\sum_{m,n} K_{m,n}\delta(u_m, j)\delta(u_n, j)
\tag{5}
$$

$$
f_{i,j} = \frac{1}{|w_j|}\sum_m K_{i,m}\delta(u_m, j)
\tag{6}
$$

It is therefore clear that the knowledge of the kernel matrix is sufficient to update the set of predicted labels up to convergence. Since an explicit form for $\phi(x)$ is not known in general, a medoid approximation can then be used in order to obtain an approximated estimate of the cluster prototypes:

$$
\begin{aligned}
\phi^{-1}(w_j) \approx m_j \quad &= \arg\min_{x_l \in X} \| \phi(x_l) - w_j \|^2 \\
&= \arg\min_{x_l \in X} K_{l,l} - 2\frac{1}{|w_j|}\sum_i K_{i,l}\delta(u_i, j) \\
&= \arg\min_{x_l \in X} K_{l,l} - 2f_{i,j}
\end{aligned}
\tag{7}
$$

As shown in [7], for the linear case, the kind of iterative algorithm described by Eq.4 almost surely converge to a local minimum, eventually reaching the stopping condition $u_{i,t+1} = u_{i,t}$, $\forall i \in [1, N]$.

We conclude this section with a final remark on the cluster compactness and the cluster average similarity (i.e. Eq.5-6). Indeed a kernel k-means reformulation in term of such quantities was originally proposed by Zhang and Rudnicky[6] in order to reduce the memory footprint of the kernel matrix allowing caching on disk. As we are going to show in the next section, the same formalism can be effectively used to design an efficient distribution strategy.

3. DISTRIBUTED MINI-BATCH KERNEL K-MEANS

We present in this section our contribution: a novel approximation for the kernel k-means algorithm together with an ad-hoc distribution and acceleration strategy well suited for nowadays heterogenous High Performance Computing (HPC) facilities.

Remark about the notation used: in the following a superscript eventually identifies a specific mini-batch quantity, when no superscript is used the quantity has to be intended as a global quantity. As an example w_j^i represents the j-th cluster prototype for the i-th mini-batch whereas w_j is the j-th global cluster prototype obtained combining the partial results of every mini-batches.

3.1. The Mini-batch Kernel K-Means

Our primary approach to reduce the $O(N^2)$ complexity coming from the kernel matrix evaluation consists of splitting the dataset in disjoint mini-batches that are processed one after the other. The procedure can be summarized by these steps:

1. Fetch one mini-batch at a time until all data is consumed.

2. Perform kernel k-means clustering on one minibatch and collect results with a proper initialization technique.

3. Merge together current minibatch results to global results with a proper strategy and go to step 1.

Fig.1 (a) shows a pictorial description of such algorithm highlighting its hierarchical structure. The entire procedure is detailed in the subsequent paragraphs.
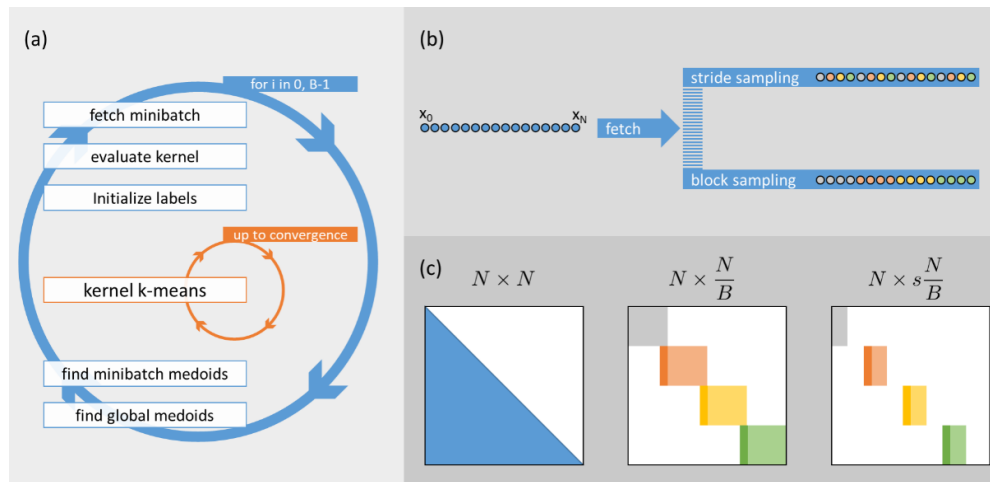
Fig.1 (a) Pictorial description of the algorithm. (b) Visualization of two possible sampling strategies to divide the dataset into mini-batches. (c) From left to right we visualize the effect of the two fold approximation proposed on the number of kernel matrix elements that need to be evaluated.

Mini-batch fetching: The first sensible choice to be made, regards the way in which the dataset is divided in B disjoint mini-batches of size $N^i, \forall i \in [0, B-1]$. Without loss of generality we will consider in the following $N^i = \frac{N}{B} \forall i \in [0, B-1]$. A variety of possibilities arise, we present here two common reasonable sampling strategies.

A stride sampling strategy can be used when the entire dataset is known beforehand and one wants to minimize the correlations among samples within the same mini-batch i.e. $X^i = \{x_{i+jB}\}, j \in [0, \frac{N}{B} - 1]$.

A block sampling strategy can be used instead to process a data stream in order to start the clustering procedure as soon as the first N^0 samples are received i.e. $X^i = \{x_{i\frac{N}{B}+j}\}, j \in [0, \frac{N}{B} - 1]$.

For the sake of clarity the two different sampling strategies presented are visualized in Fig.1(b).

Kernel evaluation and mini-batch initialization: Once a mini-batch is fetched, it is straightforward to evaluate the mini-batch kernel matrix K^i with a computational cost of $O\left(\frac{N^2}{B^2}\right)$. Let us now discuss how it is possible to initialize the i-th mini-batch labels. We distinguish two cases:

$i = 0$: during the first mini-batch the global cluster medoids have to be selected randomly or by means of some rational. We propose here to use a kernelized version of the popular k-means++ initialization scheme, where the medoids are picked at random with a distribution that maximize the distance among them. The interested reader can read the work in[8] where such initialization scheme is discussed in detail for the linear case.

$i \neq 0$: Starting from the second mini-batch the global cluster medoids $M = \{m_j \approx \phi^{-1}(w_j)\}$ obtained at the end of the previous iterations are used for the initialization. Simply applying Eq.2 we have:

$$u_l^i = \arg\min_j [K(x_l^i, x_l^i) - 2K(x_l^i, \tilde{x}_j)] \tag{8}$$

Such initialization step automatically allows to keep track of the clusters across different mini-batches. Indeed the global j-th medoid obtained at the end of the $(i-1)$-th iteration is used as initialization for the same j-th cluster of the i-th mini-batch. This avoids ambiguity also when the partial mini-batch result has to be merged with the global one. The mini-batch medoid m_j^i will be combined with the global centroid m_j having the same index j.

It should be understood that in order to evaluate the second term of Eq.8 one has to perform additional computations. One has to compute the kernel function for all the pairs (x_l^i, m_j) where x_l^i belongs to the i-th mini-batch and m_j its a global medoid coming from the $(i-1)$-th mini-batch. Thus, the initialization phase of each mini-batch requires the evaluation of the corresponding auxiliary kernel matrix $\tilde{K}^i$ of size $\frac{N}{B} \times C$.

Mini-batch inner GD loop: Given a mini-batch kernel matrix K^i and an initial set of labels U_0^i, equations Eq.2-5 are used to perform a GD optimization of the reduced cost function:

$$\Omega(W^i) = \sum_{x_j \in X^i} \sum_{l=1}^{C} \parallel \phi(x_j) - w_l^i \parallel^2 \delta(u_j^i, l) \tag{9}$$

A final set of labels U^i is obtained as a result of such optimization procedure. It is worth stressing the fact that at this point the set of mini-batch cluster prototypes is not knownin terms of explicit coordinates, but just in term of membership. As a solution, we propose the medoid approximation introduced in section 2. Using equation Eq.7, we set the cluster prototypes as:

$$w_j^i \leftarrow \phi(m_j^i): \quad m_j^i = \arg\min_{x_l \in X^i} \parallel \phi(x_l) - w_j^i \parallel^2 \tag{10}$$

More sophisticated approaches based, for instance, on a sparse representation of cluster centres are possible (e.g. see [9]). However, the inherent additional computational cost and the satisfactory results already obtained by means of the simple medoid approximation discouraged us to further investigate this possibility.

Full batch cluster centres update: We discuss now on how to merge the medoids M^i of the i-th mini-batch together with the global medoid set M. Let $\{w_j = \phi(m_j)\}$ be the global medoids at the

$(i-1)$-th iteration of the outer loop and let $\{w_j^i = \phi(m_j^i)\}$ be the cluster centres for the current i-thmini-batch. We propose to obtain the resulting global cluster prototypes as a convex combination of the two:

$$w_j \leftarrow (1-\alpha)\phi(m_j) + \alpha\phi(m_j^i) \tag{11}$$

Practically, since Eq.11 cannot be evaluated directly, we introduce a second medoid approximation as already done in the previous paragraph, so that:

$$w_j \leftarrow \phi(m_j): \quad m_j \leftarrow \arg\min_{x_l \in X^i} \parallel \phi(x_l) - (1-\alpha)\phi(m_j) - \alpha\phi(m_j^i) \parallel^2 \tag{12}$$

The choice of this convex combination stems from a simple but important observation; in order to choose the coefficient α let us consider the updating equation for the global cluster center w_j at the second iteration of the algorithm, when the first two mini-batches are merged in a single one (assuming this is the complete dataset):

$$
\begin{aligned}
w_j \quad &= \frac{1}{|w_j^0|+|w_j^1|}\sum_{x_i \in X^0 \cup X^1} \phi(x_i)\delta(u_i, j) \\
&= \frac{|w_j^0|}{|w_j^0|+|w_j^1|}\frac{1}{|w_j^0|}\sum_{x_i \in X^0} \phi(x_i)\delta(u_i, j) + \frac{|w_j^1|}{|w_j^0|+|w_j^1|}\frac{1}{|w_j^1|}\sum_{x_i \in X^1} \phi(x_i)\delta(u_i, j) \\
&= \frac{|w_j^0|}{|w_j^0|+|w_j^1|}w_j^0 + (1 - \frac{|w_j^0|}{|w_j^0|+|w_j^1|})w_j^1
\end{aligned}
\tag{13}
$$

We therefore set $\alpha = \frac{|w_j^i|}{|w_j^i|+|w_j|}$ so that, if each mini-batch is labelled correctly at the end of the GD minimization, we retrieve the correct result (i.e. same cluster medoids as for full batch kernel k-means).

Empty clusters: We close this subsection with a remark about empty-clusters. It is not guaranteed that along inner loop iterations there will be at least one data sample per cluster. This is a well-known k-means issue and several strategies to deal with such empty-clusters problem are possible e.g. randomly pick a new cluster prototype or reducing C. Here we propose the following: if a given cluster j is found to be empty at the end of the i-th mini-batch iteration then its global prototype will not be updated. It is worth noting that this kind of strategy is naturally embedded in the definition of α since for $|w_j^i| = 0$ we have $\alpha = 0$ and Eq.11 guarantee the correct behaviour.

3.2. Approximate Mini-batch Kernel K-Means

In the previous paragraph we introduced a simple yet powerful mini-batch approximation which allowed us to reduce the number of kernel evaluations down to $N\frac{N}{B}$. Here, we show how we can further reduce the complexity of the algorithm by means of an a priori sparse representation of the cluster centroids. This approach was first introduced by Chitta et al. and relies on the simple observation that the full kernel matrix is required at each iteration of the kernel k-means algorithm because the clusterscentres are represented as a linear combination of the entire dataset. However, the number of kernel elements to be evaluated can be drastically reduced if one restricts the cluster centres to a smaller sub space spanned by a small number of landmarks i.e. data samples randomly extracted from the dataset. A complete review of such approximation technique is out of the scope of this work, the interested reader can refer to [3] for further details.

We limit ourselves to illustrate here how we can reformulate the same idea within our algorithm. In order to do so we simply need to restrict the summation in Eq.3 on the subset $i: x_i \in L$ where $L = \{l_0, \ldots, l_{|L|}\}$ is a set of landmarks uniformly sampled from the mini-batch.

$$w_j = \frac{1}{|w_j|} \sum_{i \in L} \phi(x_i) \delta(u_i, j), j \in [1, C] \tag{14}$$

The self-consistent update equation for the minibatch labels will be:

$$u_i^{t+1} = \underset{j}{\text{argmin}}[\hat{g}(w_j^t) - 2\hat{f}(x_i, w_j^t)] \tag{15}$$

where $\hat{g}(w_j)$ and $\hat{f}(x_i, w_j)$ are the approximate mini-batch clusters compactness and mini-batch clusters similarity

$$\hat{g}(w_j) = \frac{1}{|w_j^t|^2} \sum_{m,n \in L} K_{m,n} \delta(u_m^t, w_j^t) \delta(u_n^t, w_j^t) \tag{16}$$

$$\hat{f}(x_i, w_j) = \frac{1}{|w_j^t|} \sum_{m \in L} K_{i,m} \delta(u_m^t, w_j^t) \tag{17}$$

It should be clear from Eq.16 and Eq.17 that the number of kernel evaluations needed to run such approximated algorithm is now $N|L| = sN\frac{N}{B}$, where the key parameter s is the fraction of data used for the cluster centres representation in each mini-batch defined as:

$$s = \frac{|L|}{N} B \tag{18}$$

In Fig.1(c) the reader can visualize the effects that B and s have on the number of kernel elements that needed to be evaluated in order to iterate the proposed algorithm. As already stated in the introduction, these two parameters act like knobs that control the degree of approximation of the procedure with respect to standard kernel k-means. Later, we will discuss on how to pick proper values for these parameters according to the available computational resources.

3.3. Heterogeneous HPC implementation strategy

We discuss here how the nature of the previously introduced algorithm is particularly suited to be implemented on both distributed systems and heterogeneous architectures where an accelerator (e.g. general-purpose GPU) is paired to a CPU.

As already discussed in section 2, the whole iterative procedure to update the set of predicted labels minimizing the kernel k-means cost function can be expressed in terms of the average cluster similarity $f_i, j, \forall i \in 0, \ldots, \frac{N}{B}, j \in 0, \ldots, C-1$ and the cluster compactness $g_j \forall j \in 0, \ldots, C-1$. Both quantities can be expressed as partial summations of kernel matrix elements, where the elements to be summed are selected according to the labels via $\delta(u_i, j)$. From Eq.6 it should be clear that the summation to compute the i-th row of f runs just over the i-th row of K, this naturally suggest us a row wise distribution strategy. Considering a system with P nodes, the workload is divided so that each node p accounts for the computation of $K_{i,j}$ and $f_{i,l} \forall j \in [0, \frac{N}{B}), i \in [p\frac{N}{BP}, (p+1)\frac{N}{BP}), l \in [0, C)$.

The full data distribution scheme is presented in Fig.2(a) and the resulting algorithm is detailed via pseudo code in Alg.1. The advantage of such approach mainly consists in the reduced communication overhead. Indeed, for each iteration of the inner loop two communication steps are sufficient, involving a reduction of the cluster compactness g together with a gathering step

for the updated labels U. The kernel matrix elements always reside locally to the node and they never go through the network.

The memory footprint can be easily computed and amounts to $Q(\frac{N}{BP}(\frac{N}{B}+C)+\frac{N}{B}+2C)$ where Q is the size of variables expressed in Bytes, this is a central quantity because in a real application scenario once fixed the computational resources i.e. amount of memory available per processor R and the number of processors P, it allows us to compute the minimum number of mini-batches that can be used in order to process the entire dataset:

$$B_{min} = \frac{\frac{2N}{P}}{-(\frac{C}{P}+1)+\sqrt{(\frac{C}{P}+1)^2-8\frac{C}{P}+\frac{R}{Q}}} \tag{19}$$

An upper bound for the message size per node can also be easily given by $Q(\frac{N}{BP}+2C)$. This however represents a worst-case scenario, where the entire set of labels U are communicated at each step, instead of communicating just the ones that were actually updated.

The computational complexity of the proposed implementation grows as $O(\frac{N^2}{B^2P})$ and it is dominated by the kernel matrix evaluation step. It is worth stressing the fact that we decided not to exploit any kernel matrix symmetry because that would have resulted in the impossibility of pursuing our row-wise data distribution scheme and additionally it would have hindered the possibility of using non symmetric similarity functions. Moreover, exploiting the kernel matrix symmetry would have resulted in a non trivial addressing scheme, unsuitable for the limited memory addressing capabilities of accelerators such as general purpose GPUs; this increased memory footprint is largely compensated by the approximation strategy in performance terms.
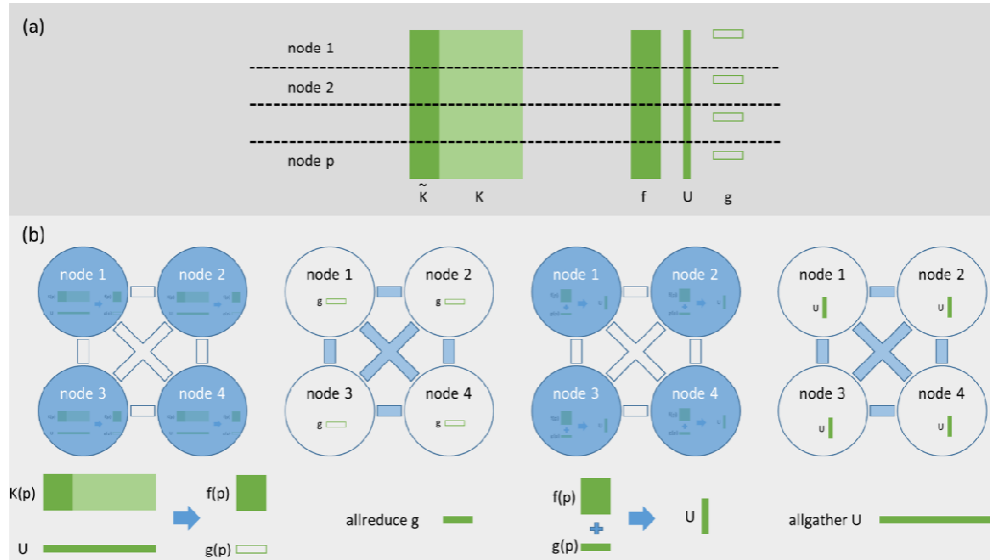

Fig. 2(a) Distribution scheme for the principal quantities needed to complete an inner loop iteration. Each node holds a set of entire rows for $\tilde{K}$, K, f and U. Each node holds a local copy of g. (b) From left to right the main steps of an inner loop iteration are illustrated. At first, each node is computing its portion of f together with a partial g starting from its K rows and U. Then, the global g is retrieved with an all-to-all reduction step. In the third stage each node uses that information together with its portion of f to compute its slice of U. As a final step an all-to-all gathering step spread the updated labels across the network.

input:	dataset X; number of clusters C; number of mini-batches B	
output:	medoids M	

1	**for** $i \leftarrow 1$ **to** B **do**	
2	$X^i \leftarrow$ samples fetched from $X \setminus X^{j<i}$	
3	$K^i(p) \leftarrow$ precompute kernel matrix	
4	**if** $i == 0$	
5	$M^0 \leftarrow$ initialize according to kernel k-means++	
6	**end**	
7	$U^i(p) \leftarrow$ assigned according nearest neighbor medoid	
8	$t \leftarrow 0$	
9	**while** $U_t^i \mathrel{!=} U_{t+1}^i$	
10	**allgather** U_t^i	sync
11	$g^i(p) \leftarrow$ compute according to Eq.5	
12	$f^i(p) \leftarrow$ compute according to Eq.6	
13	**allreduce sum** g^i	sync
14	$U_{t+1}^i(p) \leftarrow$ assign accoding to Eq.4	
15	$t \leftarrow t + 1$	
16	**end**	
17	$M^i(p) \leftarrow$ medoid approximation according to Eq.10	
18	**allreduce min** M^i	sync
19	$M(p) \leftarrow (1 - \alpha)M + \alpha M^i(p)$	
20	**allreduce min** M	sync
21	**end**	

Alg. 1Distributed mini-batch kernel k-means pseudocode for node p.

Starting from this observation we discuss now how the mini-batch structure of the algorithm can be exploited in order to design an effective acceleration strategy. In the following we will consider an offload acceleration model where host processor and target device have separate memory address spaces and communicate via a bus with limited bandwidth (e.g. PCIe) with respect to the processor-memory standard bus.

The evaluation of a large kernel matrix perfectly fits the massively parallel architecture of nowadays accelerators therefore it seems a reasonable choice to offload that portion of the computation. One of the key element for an efficient acceleration scheme however is the overlapping between the host and the target workload [10], so that a simple strategy where the CPU and the accelerator are alternatively in idle waiting for each other is not desirable.

Each iteration i-th of the outer loop depends on the previous one, namely the $(i-1)$-th, in order to initialize the set of labels U^i. This is what prevents the algorithm to be trivially parallel forcing to run just one mini-batch per time. However, if one considers the first two steps of each outer loop iteration i.e. mini-batch fetch X^i and kernel matrix evaluation K^i it is clear that they can be performed independently for each i. We exploit this feature, instructing the target device to compute the kernel matrix $K^{(i+1)}$ while the host processor executes the inner loop of the algorithm on the i-th mini-batch.

The offload procedure is detailed in Fig.3; the overall performance gain heavily depends on the accelerator side implementation of the kernel matrix evaluation which goes outside the scope of the proposed paper.
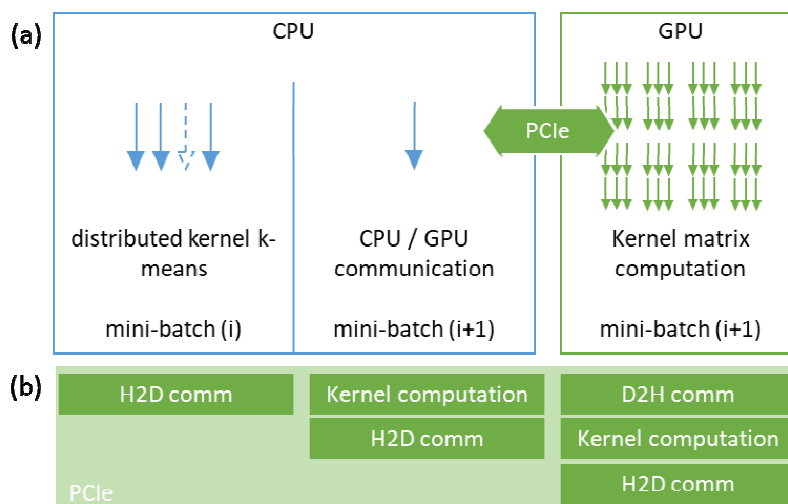
Fig. 3 (a) Pictorial description of the proposed acceleration scheme. The diagram is divided in two parts: a host processor side on the left, and a target device side on the right. We illustrate how multiple CPU threads can be used to overlap host and device workload. A CPU thread is bound to the device, it is responsible for data fetching from disk, for host-device data transfer and for device control. It instructs the device to compute the kernel matrix elements needed by the next $(i + 1)$-th iteration of the outer loop. All the other available threads cooperate and are responsible for the current i-th iteration consuming the kernel matrix elements provided by the accelerator. In this sense device and host work in a producer-consumer pattern. (b) We detailed how a 3-stage pipeline can be used on the device in order to overlap the kernel computation with the host to device (H2D) and device to host (D2H) slow communications needed to transfer the dataset on the device and the kernel matrix back to host.

4. EXPERIMENTS

We implemented the proposed method and we present here some tests against standard datasets in the ML field as well as against a 2D toy dataset in order to better asses both performances and the degree of approximation. Moreover, we present an applicative scenario in the Computational Chemistry realm.

2D Toy: Synthetic dataset containing 4 clusters of 10000 elements in a 2D feature space. Each cluster is generated by sampling a Gaussian distribution with center and width carefully selected in order to facilitate its visualization i.e. (σ=[0.2,0,2],μ=[0.25,0.75]), (σ=[0.2,0,2],μ=[0.75,0.75]) and (σ=[0.2,0,2],μ=[0.25,0.75]) .

MNIST: dataset of handwritten digits[11]. It is composed by a training set of 60000 samples and a test set of 30000 samples. 784-dimensional feature space with integer features.

RCV1: Reuters Corpus Volume I is a collection of manually labelled documents used as standard benchmark for classification in the domain of multilingual text categorization [12]. It is composed of 23149 training samples and 781265 test samples. Among the various formats available we used here its expression as normalized log TF-IDF (i.e. logarithmic term frequency-inverse document frequency) vectors in a sparse 47236-dimensional feature space. As already proposed in [13] we pre-processed the dataset removing samples with multiple labels and categories with less than 500 samples. After doing this we obtained a dataset of 193844 samples all coming from the test samples which we arbitrarily divided in 188000 training samples and 5844 test samples to maintain the original ratio. Moreover, to deal with the sparsity of the feature space we performed a dimensionality reduction step via random projection on a dense 256-dimensional space.

Noisy MNIST: generated by starting from MNIST and adding uniform noise on 20% of the features. Each sample in the training set is perturbed 20 times in order to obtain a final dataset of 1200000 samples in a 784-dimensional normalized feature space.

MD trajectory: As previously anticipated, we used Molecular Dynamics as an appealing clustering scenario in which to leverage the features of the proposed algorithm. Microsecond-long trajectories of the binding mechanism of a drug, specifically a transition state analogue named DADMe-immucillin-H, to the Purine Nucleoside Phosphorylase (PNP) enzyme were employed [14]. Those long trajectories well represent a good and relatively novel application domain for clustering and machine learning in general.

When possible, we compared the clustering labels coming from the proposed procedure with the training labels. We will consider mainly two standard quality measures:

Clustering accuracy: Let u_i be the set of labels obtained as a clustering result and let y_i be the set of the actual classes given as training or test. The clustering accuracy is defined as $\mu(y, u) = \sum_{i=0}^{N-1} \frac{\delta(\psi(y_i), u_i)}{N}$. Where $\psi(u_i)$ is a mapping function which maps each clustering label to an actual training or test class. We propose here the use of a simple majority voting scheme to obtain such a mapping.

Normalized Mutual Information: Let now be $n_i = \sum_{j=0}^{N-1} \delta(u_i, j)$, $m_i = \sum_{j=0}^{N-1} \delta(y_i, j)$ and $o_{i,j} = \sum_{k=0}^{N-1} \delta(u_k, i)\delta(y_k, j)$ the normalized mutual information is a quality measure defined as $NMI(y, u) = \frac{\sum_{i,j} o_{i,j} \log(\frac{No_{i,j}}{n_i m_j})}{(\sum_i n_i \log(\frac{n_i}{N}))(\sum_i m_i \log(\frac{m_i}{N}))}$

We tested our implementation on a variety of different platforms in order to better describe the versatility and the potential impact of the proposed algorithm:

IBM-BG/Q - Cineca/FERMI: Cluster of 10240 computing nodes equipped with two octacore IBM PowerA2, 1.6 GHz processors each, for a total of 163840 cores. The available memory amounts to 16 GB / core and the internal network features a 5D toroidal topology.

IBM NeXtScale - Cineca/GALILEO: Cluster of 516 computing nodes equipped with two octacore Intel Haswell 2.40 GHz processors for a total of 8256 cores. The available memory amounts to 8 GB / core and the internal network features Infiniband with 4x QDR switches.

State-of-the-art Workstation: Modern desktop machine equipped with two Intel E-6500 esacore processors and 64 GByte of memory.

4.1. Explanatory 2D toy model

As a first step to assess the proposed clustering algorithm we consider the 2D Toy dataset. We aim at better illustrating and helping the visualization of the evolution of the cluster centres along with the iterations of the outer loop. Incidentally, we want to highlight the consequences of a poor sampling strategy (concept-drift) and to give a rationale for understanding its quality.

In figure 4(a)-(b) the evolution of the cluster centres is followed for two different sampling strategies i.e. (a) stride sampling and (b) block sampling. Even though the final set of labels is the same for such simple dataset it should be clear that the stride sampling strategy is superior in representing the structure of the dataset within each mini-batch. The underlying question is how could one assess the quality of the sampling strategy in a real case scenario where direct visualization is not possible. In Fig.4(c) we try to answer by looking at the behaviour of the

cluster center displacement. We can comment that if such quantity is constantly small with respect to the average cluster size, the mini-batches can be regarded as good representative of the entire dataset structure. In contrast, high values or spikes in the same quantity may reflect a poor sampling strategy.

Observing Fig.4(d) we note that the inner loop of the proposed algorithm, i.e. the minimization of the partial cost $\Omega(W^i)$, does indeed help in minimizing the global objective function $\Omega(W)$.
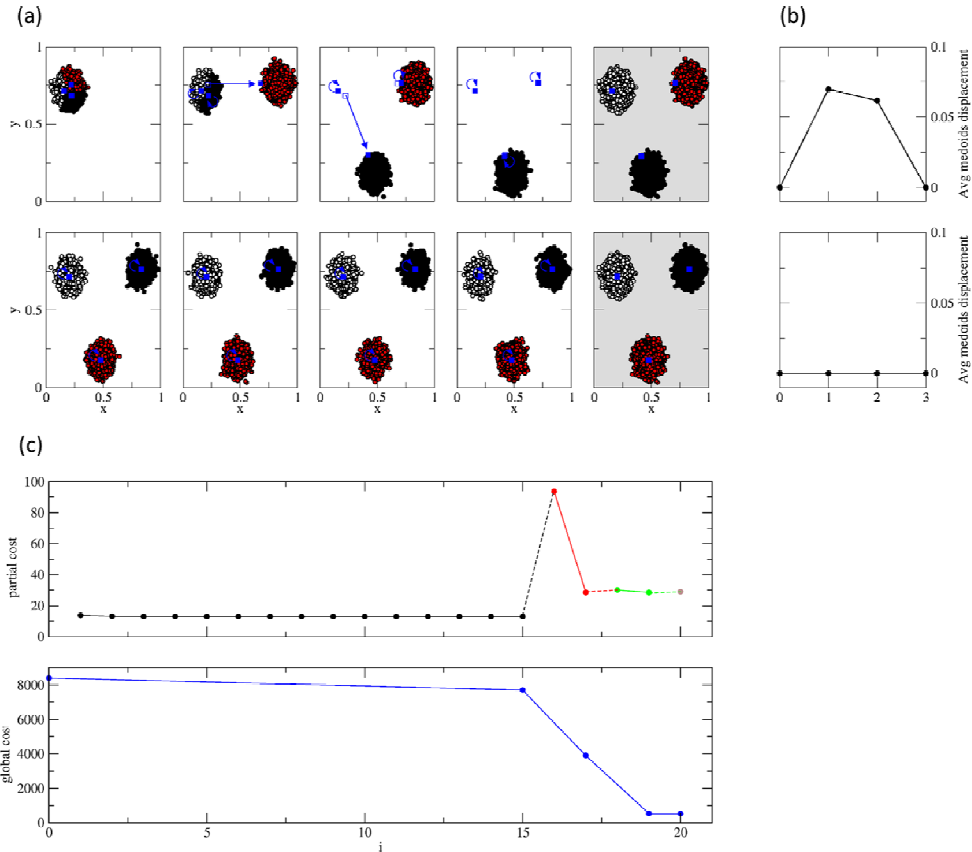

Fig. 4 (a-top row) From left to right the evolution of the cluster centres across different iterations of the outer loop in the case of a poorly designed block sampling strategy. (a-bottom row) From left to right the evolution of the cluster centres across different iterations of the outer loop in the case of a proper stride sampling strategy where each mini-batch correctly captures the underlying structure of data. (b) Average cluster centres displacement vs outer loop iterations for the two different sampling strategies illustrated in (a), we propose this as a control observable to assess the quality of the sampling when direct visualization is not feasible. (c-top panel) Partial cost function $\Omega(W^i), \forall i \in [0, B = 3]$ vs number of iterations, different colors represent different mini-batches. (c-bottom panel) Global cost function $\Omega(W)$ vs number of iterations. It is worth noting how the inner loop iterations within each mini-batch help to bring down the global cost function.

4.2. Assessing the degree of approximation

We consider now the MNIST dataset in order to assess the degree of approximation introduced by the mini-batch approach and by the a priori sparse representation of the cluster centres. We ran our algorithm on the 60000 training samples of MNIST with $B = [1,2,4,8]$, $s \in [0.025,1.0]$ and we monitored the resulting clustering centres against the 10000 test samples in order to compute the clustering accuracy μ. Results as well as execution times are presented in Fig.5. We observe

that the algorithm is generally robust across a wide range of the two parameters. The clusteringaccuracy slightly decreases when the number of mini-batches increase and once$B$ is fixed it decreases almost monotonically with $s$dropping to low values when $s < 0.2$. As expected, this suggests us to position ourselves to the top-left part of the graph i.e. few mini-batches and $s \approx 1$.

Both B and s are trade-off parameters that have to be fixed. The strategy we suggest here is to fix a desired execution time on a given compute architecture. The available memory for the execution can lead to a first value for B using Eq.19. As a starting point, the value of s can be fixed at its maximum. This set of parameters i.e. $(B_{min}, 1.0)$. should be optimal for the computational resources available i.e. minimum number of mini-batches without sparse representation of the cluster centroids. One can evaluate the expected execution time for the algorithm running it on a single mini-batch, if the expected execution time does not match the initial requirements then one can first slowly decrease s and, if this is not sufficient (i.e. expected execution time too high for $s < 0.2$), then increase the number of mini-batches. The approximation degree introduced can be self consistently checked using a single mini-batch and taking as reference the results obtained for the optimal set of parameters $(B_{min}, 1.0)$.

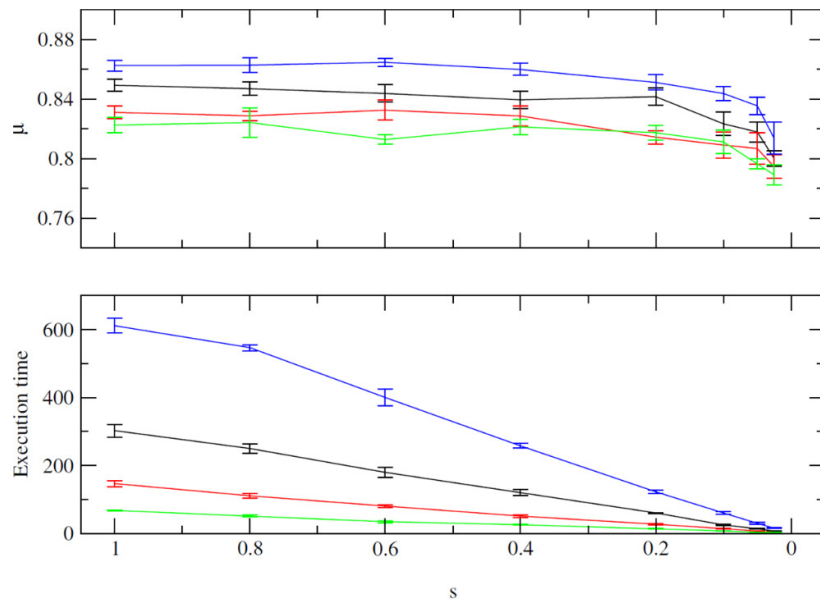This rationale should guide the user to finely tune the trade-off parameters also on a very large dataset.

Fig. 5(top panel) Cluster accuracy vs s. (bottom panel) Execution time vs s. Clustering performed on 60000 MNIST training samples evaluated against the 10000 provided test samples. Different colors represent different values of $B = [1,2,4,8]$. As described in the main text this graph can help understand how to perform model selection for the set of newly introduced parameters (B, s) picking a target execution time and looking at the clustering accuracy for the compatible sets of parameters.

4.3. Scaling behaviour

We aim here at assessing the quality of the ad-hoc distribution strategy that we proposed in the previous section. In order to do so we tested our algorithm both on the IBM BG/Q and on the IBM NeXtScale machines above described, against the standard MNIST dataset.

We decided to set $B = 1$in order to run the code in single batch mode since, as already explained, our distribution strategy does not involve the outer loop of the proposed method i.e. increasing the

number of mini-batches would have only added a multiplicative constant to the execution time equal to B.

In Fig.6 the strong scaling plot for both machines is showed, the algorithm exhibits near to perfect scaling for a wide range of P i.e. $16 \rightarrow 1024$ on IBM BG/Q and $16 \rightarrow 256$ on IBM NeXtScale. The discrepancy from the ideal behaviour outside this range can be ascribed to the portion of code intrinsically serial (e.g. fetching and initialization phases) which becomes a prominent cost as described by Amdahl's law.
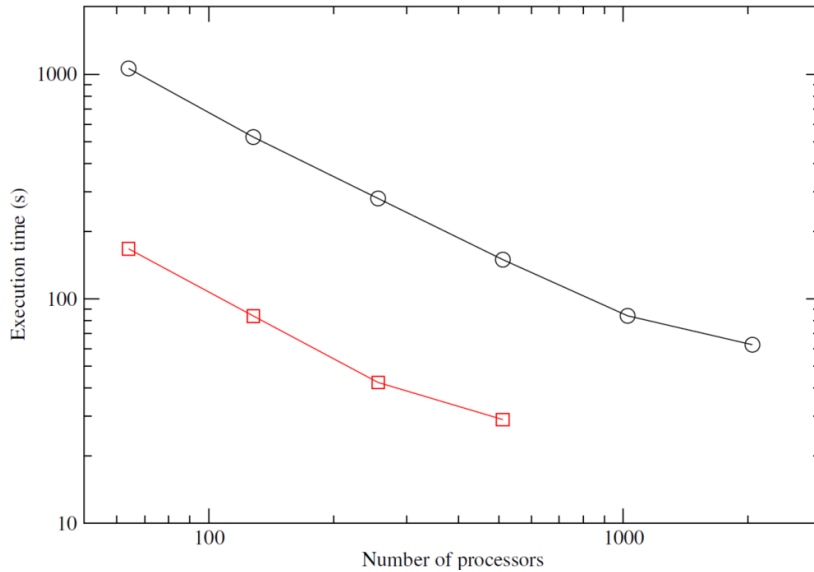

Fig. 6 Execution time vs P for two different distributed architectures. IBM BG/Q in black/circles and IBM NeXtScale in red/squares.

4.4. Standard datasets analysis

We present here the tests we performed on a state-of-the-art workstation over standard datasets coming from the Machine Learning community. We show how even a large dataset with up to 10^6 elements in 784 dimensions can be processed via a kernel approach on a desktop machine in a reasonable amount of time. The considered datasets are MNIST (60000 samples in 784 dimensions), RCV1 (188000 samples in 256 dimensions) and noisy MNIST (1000000 samples in 784 dimensions).The results are collected respectively inTab.1-3.

For all the experiments, we used the strided sampling technique, set $s = 1$, selected the number of clusters automatically via the elbow criterion and set $\sigma = 4d_{max}$ in order to mimic a linear kernel behaviour. As a baseline comparison for the clustering accuracy and the normalized mutual information we used a standard python implementation of k-means from the scikit-learn package [15]. Results coming from RCV1 are also compared with that appearing in the literature [13].

Tab. 1 MNIST results and timings for different B values

B	Clustering accuracy	NMI	Execution time
Baseline	84.5 ± 0.62	0.693 ± 0.012	$-$
1	86.47 ± 0.37	0.737 ± 0.006	655.23 ± 82.92
4	82.63 ± 0.91	0.680 ± 0.011	133.63 ± 4.40
16	81.45 ± 0.653	0.670 ± 0.010	32.17 ± 2.48
64	78.39 ± 0.95	0.626 ± 0.015	9.51 ± 0.58

Tab. 2 RCV1 results and timings for different *B* values

B	Clustering accuracy	NMI	Execution time
Literature	16.59 ± 0.62	0.2737 ± 0.0063	−
Baseline	15.16 ± 0.81	0.091 ± 0.0052	−
4	17.41 ± 0.83	0.147 ± 0.006	797.65 ± 53.48
16	16.52 ± 0.74	0.145 ± 0.001	170.96 ± 4.94
64	16.15 ± 0.60	0.132 ± 0.001	77.20 ± 3.96

Tab. 3 Noisy MNIST (10^6 samples) results and timings for different *B* values

B	Clustering accuracy	NMI	Execution time
Baseline	−	−	−
32	64.19 ± 1.03	0.541 ± 0.005	2334.31 ± 25.63
64	60.97 ± 0.3	0.506 ± 0.001	1243.81 ± 23.43

4.5. Molecular dynamics trajectory clustering

In this section we analyze the behaviour of the clustering algorithm in terms of the quality of the obtained results in the MD domain. Basically, we compared the results obtained by the current implementation with respect to the results obtained in [1]. In that paper the binding process of a drug to its target was simulated and we used an in house clustering tool to get intermediate states of the protein/ligand complex formation along the binding routes. There, we employed the k-medoids algorithm and we were able to completely characterize the binding process.

Here we ran again the same kind of analysis systematically verifying that the same, or very similar, binding intermediates could be obtained. For the analysis of the structures, we extracted the medoids from each cluster. The same atoms as per [1] were used for the clustering.To define the number of clusters we used the elbow criterion as in [1] trying the clustering in the (4,40) range; in the end, we obtained 20 clusters as an optimal value.

For each run we initialized 5 times the algorithm with the k-means++ method and kept the solution with minimum cost. To assess the accuracy of the approximated algorithm we split the dataset in 4 mini-batches each comprising about 250000 samples, thus drastically limiting the kernel matrix size with respect to a full run. We used the strided sampling because data was batch available and when possible, this sampling should be always used. As previously anticipated, we evaluated the quality of the results by the capability of the solution to capture the key events of the simulations. In Fig.7(a) we summarize the meaning of the medoids in structural terms using the same naming conventions appeared in [1] and associate them with the respective cluster id.

Overall those medoids well recapitulate the binding process giving the same synthetic description obtained in [1] despite the mini-batch approximation. In particular, we show here, in Fig.7(b), the distance matrix computed across the medoids; we reordered the columns based on the manual classification induced by visual inspection. Results show clearly the three main macro-sections of the simulation namely the bound state, the entrance paths and the out unbound states.

(a)

(b)

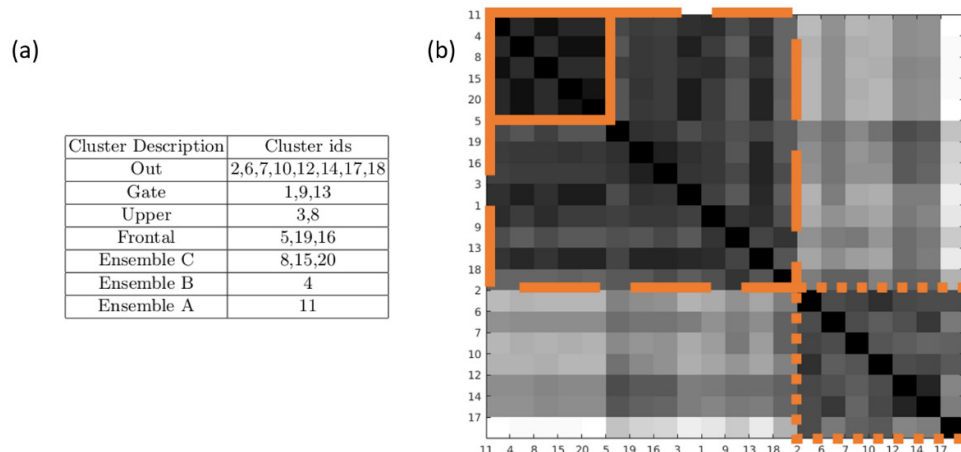| Cluster Description	Cluster ids
Out	2,6,7,10,12,14,17,18
Gate	1,9,13
Upper	3,8
Frontal	5,19,16
Ensemble C	8,15,20
Ensemble B	4
Ensemble A	11

Fig. 7 (a) Table summarizing medoids for MD data and their labelling (b) Medoids RMSD matrix. On the axes we indicate the medoid identifiers. On the upper left is well visible the macro-area of the bound states. Then, this area extends to the right including the entrance paths, and lastly, on the lower right corner, the unbound states

5. DISCUSSION

Mini-batch approaches are not new in the clustering community and encountered a great success when applied to standard k-means [9]. In his work, Sculley showed how a mini-batch Stochastic Gradient Descent (SGD) procedure converges faster than regular GD. He proposed to set the size of mini-batches to a rather small value, namely $\approx 10^3$, and to fix an a-priori number of iterations for the algorithm.

Our take here is quite different. The number of iterations is by construction equal to the number of mini-batches B in order to exploit the entire dataset. Moreover, a major difference with the SGD procedure proposed by Sculley is here represented by the inner loop. We actually believe that iterating each mini-batch up to convergence can lead to a better minimization of the cost function and to a less noisy procedure.

A comparison about the clustering accuracy achieved by the two algorithms for the original MNIST dataset is shown in Fig.8. It is worth noting that our proposed algorithm performs better as the number of mini-batches B decreases whereas the performances of the SGD procedure proposed by Sculley are almost constant. Moreover, and as expected, our algorithm is less sensitive to noise, indeed the clustering accuracy variance is much lower in comparison to that of the SGC procedure.

We stress also the fact that our parallelization approach is rather different when compared to what in literature is referred to as parallel patch clustering, see e.g. [16]. Indeed, we don't parallelize across mini-batches assigning one mini-batch per node. Instead, we parallelize the iterations within each mini-batch thus allowing the algorithm to cope with virtually any sample size.
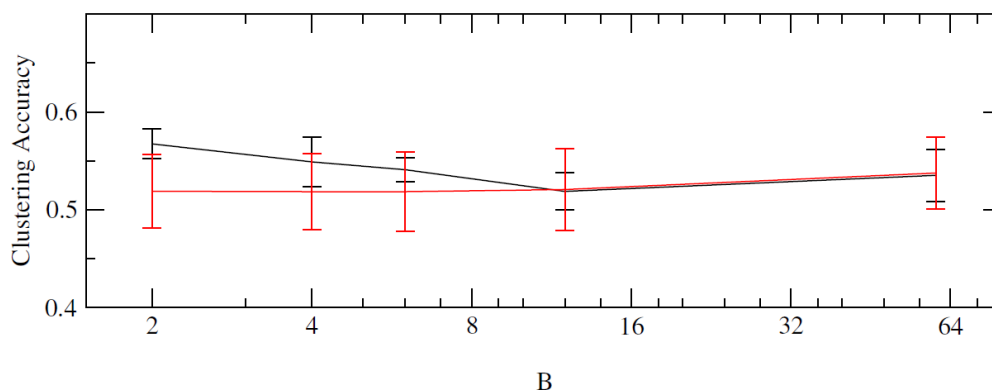
Fig. 8 Clustering Accuracy vs number of mini-batchs$B$ for the proposed algorithm (black line) and the SGD k-means procedure proposed by Sculley (red line). Comparison performed on the original MNIST dataset with $C = 10$, $\sigma = 4d_{max}$ to mimic a linear behaviour.

6. CONCLUSIONS

In this paper we presented a distributed and efficient approximation scheme for the kernel k-means algorithm. The approximation scheme applies an adaptive strategy based on the available memory resources together with the full exploitation of CPUs and GPUs capabilities. We obtained state of the art results in several application domains in terms of accuracy even in a heavily approximated regime; moreover, we got linear scaling in several different, distributed, computational architectures, something particularly useful in the big data era.

Next developments will deal with the full GPU porting of the algorithm exploiting GPU direct communications facilities of nVidia GPUs and the systematic application to the molecular dynamics domain, with particular attention to drug discovery, possibly proposing algorithmic extensions to best fit the field requirements.

REFERENCES

[1] Sergio Decherchi et al., (2015), "The ligand binding mechanism to purine nucleoside phosphorylase elucidated via molecular dynamics and machine learning." ,Nature communications, 6.

[2] Mark Girolami, (2002),"Mercer kernel-based clustering in feature space.", IEEE Transactions on Neural Networks, 13, 3, pp780–784.

[3] Radha Chitta, et al.,(2011),"Approximate kernel k-means: Solution to large scale kernel clustering", Proceedings of the 17th ACM SIGKDD international conference on Knowledge discovery and data mining, ACM, pp 895–903.

[4] Luca Mollica et al., (2015), "Kinetics of protein-ligand unbinding via smoothed potential molecular dynamics simulations.", Scientific Reports, 5.

[5] S Kashif Sadiq et al.,(2012),"Kinetic characterization of the critical step inHIV-1 protease maturation.",Proceedings of the National Academy of Sciences, 109, 50, pp 20449–20454.

[6] Rong Zhang and Alexander I Rudnicky. (2002), "A large scale clustering scheme for kernel k-means.", Pattern Recognition. Proceedings. 16th International Conference on,4, pp289–292.

[7] Leon Bottou and YoshuaBengio,(1995),"Convergence properties of the k-means algorithms." Advances in neural information processing systems, pp 585–592.

[8]   David Arthur and Sergei Vassilvitskii, (2007),"k-means++: The advantages of careful seeding.", Proceedings of the eighteenth annual ACM-SIAM symposium on Discrete algorithms. Society for Industrial and Applied Mathematics, pp 1027–1035.

[9]   David Sculley, (2010),"Web-scale k-means clustering.", Proceedings of the 19th international conference on World wide web, pp 1177–1178.

[10]   Jason Sanders and Edward Kandrot,(2010),"CUDA by example: an introduction to general-purpose GPU programming.", Addison-Wesley Professional.

[11]   Yann LeCun and Corinna Cortes,(1998),"The MNIST database of handwritten digits.".

[12]   David D Lewis et al.,(2004),"Rcv1: A new benchmark collection for text categorization research."Journal of machine learning research,5, pp 361–397.

[13]   Wen-Yen Chen et al.,(2011)."Parallel spectral clustering in distributed systems.", IEEE transactions on pattern analysis and machine intelligence, 33, 3, pp 568–586.

[14]   Meng-Chiao Ho, et al.,(2010),"Four generations of transition-state analogues for human purine nucleoside phosphorylase." Proceedings of the National Academy of Sciences, 107, 11, pp 4805–4812.

[15]   Fabian Pedregosa, et al.,(2011),"Scikit-learn: Machine learning in Python. Journal of Machine Learning Research", 12,pp 2825–2830.

[16]   Alex, N. and Hammer, B., (2008),"Parallelizing single patch pass clustering", ESANN, pp. 227-232.

AUTHORS

Marco Jacopo Ferrarotti

Graduated in Physics of Complex Systems in 2013 jointly from Politecnico di Torino and Paris-Sud University. Since 2014 he moved to theDrug Discovery and Development Department of the Italian Institute of Technology as PhD student working on study and developments of scalable Machine Learning methods applied to Molecular Dynamics simulations.

Sergio Decherchi

Graduated in Electronic Engineering in 2007 from Genoa University, Italy. Since 2005 he started collaborating with the Department of Biophysical and Electronics Engineering of Genoa University, where he completed a PhD inMachine Learning and Data Mining in 2010. His main research interests are computational byophisics and computational intelligence tools for drug discovery and virtual screening. He published more than 20 papers in refereed conferences and journals.
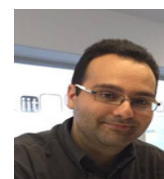
Walter Rocchia

Graduated in Electronic Engineering on July 1996. In February 2000, he got a PhD in Electronic Devices at the University of Trento. He then was a Research Scholar at the Biochemistry Department of the Columbia University. In 2008, he moved to the Drug Discovery and Development Department of the Italian Institute of Technology, working on computational approaches to ligand-protein binding free energy estimation. In late 2014, he created the Computational mOdelling of NanosCalE and bioPhysicalsysTems (CONCEPT) Lab.He is author of more than 50 publications including International Journals, book contributions and Proceedings.

Error Estimates for Multi-Penalty Regularization under General Source Condition

Abhishake Rastogi

Department of Mathematics
Indian Institute of Technology Delhi
New Delhi 110016, India

abhishekrastogi2012@gmail.com

Abstract

In learning theory, the convergence issues of the regression problem are investigated with the least square Tikhonov regularization schemes in both the RKHS-norm and the $\mathscr{L}^2$-norm. We consider the multi-penalized least square regularization scheme under the general source condition with the polynomial decay of the eigenvalues of the integral operator. One of the motivation for this work is to discuss the convergence issues for widely considered manifold regularization scheme. The optimal convergence rates of multi-penalty regularizer is achieved in the interpolation norm using the concept of effective dimension. Further we also propose the penalty balancing principle based on augmented Tikhonov regularization for the choice of regularization parameters. The superiority of multi-penalty regularization over single-penalty regularization is shown using the academic example and moon data set.

Keywords: Learning theory, Multi-penalty regularization, General source condition, Optimal rates, Penalty balancing principle.
Mathematics Subject Classification 2010: 68T05, 68Q32.

1 Introduction

Let X be a compact metric space and $Y \subset \mathbb{R}$ with the joint probability measure ρ on $Z = X \times Y$. Suppose $\mathbf{z} = \{(x_i, y_i)\}_{i=1}^m \in Z^m$ be a observation set drawn from the unknown probability measure ρ. The learning problem [1, 2, 3, 4] aims to approximate a function $f_{\mathbf{z}}$ based on $\mathbf{z}$ such that $f_{\mathbf{z}}(x) \approx y$. We define the regression function $f_{\rho} : X \to Y$ by

$$f_{\rho}(x) := \int_Y y d\rho(y|x) \tag{1}$$

which is the minimizer of the generalization error

$$\mathcal{E}(f) := \mathcal{E}_{\rho}(f) = \int_X \int_Y (f(x) - y)^2 d\rho(y|x) d\rho_X(x). \tag{2}$$

where $\rho(y|x)$ and $\rho_X(x)$ are conditional probability measure on Y and marginal probability measure on X respectively. Therefore our objective becomes to estimate the regression function f_{ρ}.

Single-penalty regularization is widely considered to infer the estimator from given set of random samples [5, 6, 7, 8, 9, 10]. Smale et al. [9, 11, 12] provided the foundations of theoretical analysis of square-loss regularization scheme under Hölder's source condition. Caponnetto et al. [6] improved the error estimates to optimal convergence rates for regularized least-square algorithm using the polynomial decay condition of eigenvalues of the integral operator. But sometimes, one may require to add more penalties to incorporate more features in the regularized solution. Multi-penalty regularization is studied by various authors for both inverse problems and learning algorithms [13, 14, 15, 16, 17, 18, 19, 20]. Belkin et al. [13] discussed the problem of manifold regularization which controls the complexity of the function in ambient space as well as geometry of the probability space:

$$f^* = \operatorname*{argmin}_{f \in \mathcal{H}_K} \left\{ \frac{1}{m} \sum_{i=1}^m (f(x_i) - y_i)^2 + \lambda_A ||f||^2_{\mathcal{H}_K} + \lambda_I \sum_{i,j=1}^n (f(x_i) - f(x_j))^2 \omega_{ij} \right\}, \qquad (3)$$

where $\{(x_i, y_i) \in X \times Y : 1 \le i \le m\} \bigcup \{x_i \in X : m < i \le n\}$ is given set of labeled and unlabeled data, λ_A and λ_I are non-negative regularization parameters, ω_{ij}'s are non-negative weights, $\mathcal{H}_K$ is reproducing kernel Hilbert space and $|| \cdot ||_{\mathcal{H}_K}$ is its norm.

Further, the manifold regularization algorithm is developed and widely considered in the vector-valued framework to analyze the multi-task learning problem [21, 22, 23, 24] (Also see references therein). So it motivates us to theoretically analyze this problem. The convergence issues of the multi-penalty regularizer are discussed under general source condition in [25] but the convergence rates are not optimal. Here we are able to achieve the optimal minimax convergence rates using the polynomial decay condition of eigenvalues of the integral operator.

In order to optimize regularization functional, one of the crucial problem is the parameter choice strategy. Various prior and posterior parameter choice rules are proposed for single-penalty regularization [26, 27, 28, 29, 30] (also see references therein). Many regularization parameter selection approaches are discussed for multi-penalized ill-posed inverse problems such as discrepancy principle [15, 31], quasi-optimality principle [18, 32], balanced-discrepancy principle [33], heuristic L-curve [34], noise structure based parameter choice rules [35, 36, 37], some approaches which require reduction to single-penalty regularization [38]. Due to growing interest in multi-penalty regularization in learning, multi-parameter choice rules are discussed in learning theory framework such as discrepancy principle [15, 16], balanced-discrepancy principle [25], parameter choice strategy based on generalized cross validation score [19]. Here we discuss the penalty balancing principle (PB-principle) to choose the regularization parameters in our learning theory framework which is considered for multi-penalty regularization in ill-posed problems [33].

1.1 Mathematical Preliminaries and Notations

Definition 1.1. Reproducing Kernel Hilbert Space (RKHS). For non-empty set X, the real Hilbert space $\mathcal{H}$ of functions from X to Y is called reproducing kernel Hilbert space if for any $x \in X$, the linear functional which maps $f \in \mathcal{H}$ to $f(x)$ is continuous.

For each reproducing kernel Hilbert space $\mathcal{H}$ there exists a mercer kernel $K : X \times X \to \mathbb{R}$ such that for $K_x : X \to \mathbb{R}$, defined as $K_x(y) = K(x, y)$, the span of the set $\{K_x : x \in X\}$ is dense in $\mathcal{H}$. Moreover, there is one to one correspondence between mercer kernels and reproducing kernel Hilbert spaces [39]. So we denote the reproducing kernel Hilbert space $\mathcal{H}$ by $\mathcal{H}_K$ corresponding to

a mercer kernel K and its norm by $||\cdot||_K$.

Definition 1.2. The sampling operator $S_{\mathbf{x}} : \mathcal{H}_K \to \mathbb{R}^m$ associated with a discrete subset $\mathbf{x} = \{x_i\}_{i=1}^m$ is defined by

$$S_{\mathbf{x}}(f) = (f(x))_{x \in \mathbf{x}}.$$

Then its adjoint is given by

$$S_{\mathbf{x}}^* \mathbf{c} = \frac{1}{m} \sum_{i=1}^m c_i K_{x_i}, \quad \forall \mathbf{c} = (c_1, \cdots, c_m) \in \mathbb{R}^m.$$

For each $(x_i, y_i) \in Z$, $y_i = f_\rho(x_i) + \eta_{x_i}$, where the probability distribution of η_{x_i} has mean 0 and variance $\sigma_{x_i}^2$. Denote $\sigma^2 := \frac{1}{m} \sum_{i=1}^m \sigma_{x_i}^2 < \infty$ and $\kappa := \sqrt{\sup_{x \in X} K(x, x)} < \infty$.

Learning Scheme. The optimization functional (3) can be expressed as

$$f^* = \operatorname*{argmin}_{f \in \mathcal{H}_K} \left\{ ||S_{\mathbf{x}} f - \mathbf{y}||_m^2 + \lambda_A ||f||_K^2 + \lambda_I ||(S_{\mathbf{x}'}^* L S_{\mathbf{x}'})^{1/2} f||_K^2 \right\}, \tag{4}$$

where $\mathbf{x}' = \{x_i \in X : 1 \leq i \leq n\}$, $||\mathbf{y}||_m^2 = \frac{1}{m} \sum_{i=1}^m y_i^2$, $L = D - W$ with $W = (\omega_{ij})$ is a weight matrix with non-negative entries and D is a diagonal matrix with $D_{ii} = \sum_{j=1}^n \omega_{ij}$.

Here we consider a more general regularized learning scheme based on two penalties:

$$f_{\mathbf{z},\lambda} := \operatorname*{argmin}_{f \in \mathcal{H}_K} \left\{ ||S_{\mathbf{x}} f - \mathbf{y}||_m^2 + \lambda_1 ||f||_K^2 + \lambda_2 ||Bf||_K^2 \right\}, \tag{5}$$

where $B : \mathcal{H}_K \to \mathcal{H}_K$ is a bounded operator and λ_1, λ_2 are non-negative parameters.

Theorem 1.1. *If $S_{\mathbf{x}}^* S_{\mathbf{x}} + \lambda_1 I + \lambda_2 B^* B$ is invertible, then the optimization functional (4) has unique minimizer:*

$$f_{\mathbf{z},\lambda} = \Delta_S S_{\mathbf{x}}^* \mathbf{y}, \ \ where \ \Delta_S := (S_{\mathbf{x}}^* S_{\mathbf{x}} + \lambda_1 I + \lambda_2 B^* B)^{-1}.$$

We can obtain the explicit form of $f_{\mathbf{z},\lambda}$ by taking the functional derivative of the expression:

$$||S_{\mathbf{x}} f - \mathbf{y}||_m^2 + \lambda_1 ||f||_K^2 + \lambda_2 ||Bf||_K^2 = \langle (S_{\mathbf{x}}^* S_{\mathbf{x}} + \lambda_1 I + \lambda_2 B^* B) f, f \rangle_K - 2\langle S_{\mathbf{x}}^* \mathbf{y}, f \rangle_K + ||\mathbf{y}||_m^2.$$

Define $f_{\mathbf{x},\lambda}$ as the minimizer of the optimization problem:

$$f_{\mathbf{x},\lambda} := \operatorname*{argmin}_{f \in \mathcal{H}_K} \left\{ \frac{1}{m} \sum_{i=1}^m (f(x_i) - f_\rho(x_i))^2 + \lambda_1 ||f||_K^2 + \lambda_2 ||Bf||_K^2 \right\} \tag{6}$$

which gives

$$f_{\mathbf{x},\lambda} = \Delta_S S_{\mathbf{x}}^* S_{\mathbf{x}} f_\rho. \tag{7}$$

The data-free version of the considered regularization scheme (5) is

$$f_\lambda := \operatorname*{argmin}_{f \in \mathcal{H}_K} \left\{ ||f - f_\rho||_\rho^2 + \lambda_1 ||f||_K^2 + \lambda_2 ||Bf||_K^2 \right\}, \tag{8}$$

where the norm $|| \cdot ||_\rho := || \cdot ||_{\mathscr{L}^2_{\rho_X}}$. Then we get the expression of f_λ,

$$f_\lambda = (L_K + \lambda_1 I + \lambda_2 B^* B)^{-1} L_K f_\rho \tag{9}$$

and

$$f_{\lambda_1} := \underset{f \in \mathcal{H}_K}{\operatorname{argmin}} \left\{ ||f - f_\rho||^2_\rho + \lambda_1 ||f||^2_K \right\}. \tag{10}$$

which implies

$$f_{\lambda_1} = (L_K + \lambda_1 I)^{-1} L_K f_\rho, \tag{11}$$

where the integral operator $L_K : \mathscr{L}^2_{\rho_X} \to \mathscr{L}^2_{\rho_X}$ is a self-adjoint, non-negative, compact operator, defined as

$$L_K(f)(x) := \int_X K(x,t) f(t) d\rho_X(t), \quad x \in X.$$

The integral operator L_K can also be defined as a self-adjoint operator on $\mathcal{H}_K$. We use the same notation L_K for both the operators.

Using the singular value decomposition $L_K = \sum_{i=1}^\infty t_i \langle \cdot, e_i \rangle_K e_i$ for orthonormal system $\{e_i\}$ in $\mathcal{H}_K$ and sequence of singular numbers $\kappa^2 \geq t_1 \geq t_2 \geq \ldots \geq 0$, we define

$$\phi(L_K) = \sum_{i=1}^\infty \phi(t_i) \langle \cdot, e_i \rangle_K e_i,$$

where ϕ is a continuous increasing index function defined on the interval $[0, \kappa^2]$ with the assumption $\phi(0) = 0$.

We require some prior assumptions on the probability measure ρ to achieve the uniform convergence rates for learning algorithms.

Assumption 1. (Source condition) *Suppose*

$$\Omega_{\phi,R} := \{ f \in \mathcal{H}_K : f = \phi(L_K)g \ and \ ||g||_K \leq R \},$$

Then the condition $f_\rho \in \Omega_{\phi,R}$ is usually referred as general source condition [40].

Assumption 2. (Polynomial decay condition) *We assume the eigenvalues t_n's of the integral operator L_K follows the polynomial decay: For fixed positive constants α, β and $b > 1$,*

$$\alpha n^{-b} \leq t_n \leq \beta n^{-b} \quad \forall n \in \mathbb{N}.$$

Following the notion of Bauer et al. [5] and Caponnetto et al. [6], we consider the class of probability measures $\mathcal{P}_\phi$ which satisfies the source condition and the probability measure class $\mathcal{P}_{\phi,b}$ satisfying the source condition and polynomial decay condition.

The effective dimension $\mathcal{N}(\lambda_1)$ can be estimated from Proposition 3 [6] under the polynomial decay condition as follows,

$$\mathcal{N}(\lambda_1) := Tr\left((L_K + \lambda_1 I)^{-1} L_K \right) \leq \frac{\beta b}{b-1} \lambda_1^{-1/b}, \ \text{for } b > 1. \tag{12}$$

where $Tr(A) := \sum_{k=1}^\infty \langle Ae_k, e_k \rangle$ for some orthonormal basis $\{e_k\}_{k=1}^\infty$.

Shuai Lu et al. [41] and Blanchard et al. [42] considered the logarithm decay condition of the effective dimension $\mathcal{N}(\lambda_1)$,

Assumption 3. (logarithmic decay) *Assume that there exists some positive constant $c > 0$ such that*

$$\mathcal{N}(\lambda_1) \leq c \log\left(\frac{1}{\lambda_1}\right), \forall \lambda_1 > 0. \tag{13}$$

2   Convergence Analysis

In this section, we discuss the convergence issues of multi-penalty regularization scheme on reproducing kernel Hilbert space under the considered smoothness priors in learning theory framework. We address the convergence rates of the multi-penalty regularizer by estimating the sample error $f_{\mathbf{z},\lambda} - f_\lambda$ and approximation error $f_\lambda - f_\rho$ in interpolation norm.

Proposition 2.1. *Let $\mathbf{z}$ be i.i.d. samples drawn according to the probability measure ρ with the hypothesis $|y_i| \leq M$ for each $(x_i, y_i) \in Z$. Then for $0 \leq s \leq \frac{1}{2}$ and for every $0 < \delta < 1$ with prob. $1 - \delta$,*

$$||L_K^s(f_{\mathbf{z},\lambda} - f_{\mathbf{x},\lambda})||_K \leq 2\lambda_1^{s-\frac{1}{2}} \left\{ \Xi\left(1 + 2\sqrt{\log\left(\frac{2}{\delta}\right)}\right) + \frac{4\kappa M}{3m\sqrt{\lambda_1}} \log\left(\frac{2}{\delta}\right) \right\},$$

where $\mathcal{N}_{x_i}(\lambda_1) = Tr\left((L_K + \lambda_1 I)^{-1}K_{x_i}K_{x_i}^*\right)$ and $\Xi = \frac{1}{m}\sqrt{\sum_{i=1}^m \sigma_{x_i}^2 \mathcal{N}_{x_i}(\lambda_1)}$ for the variance $\sigma_{x_i}^2$ of the probability distribution of $\eta_{x_i} = y_i - f_\rho(x_i)$.

Proof. The expression $f_{\mathbf{z},\lambda} - f_{\mathbf{x},\lambda}$ can be written as $\Delta_S S_{\mathbf{x}}^*(\mathbf{y} - S_{\mathbf{x}}f_\rho)$. Then we find that

$$||L_K^s(f_{\mathbf{z},\lambda} - f_{\mathbf{x},\lambda})||_K \leq I_1 ||L_K^s(L_K + \lambda_1 I)^{-1/2}|| \ ||(L_K + \lambda_1 I)^{1/2}\Delta_S(L_K + \lambda_1 I)^{1/2}||$$

$$\leq I_1 I_2 ||L_K^s(L_K + \lambda_1 I)^{-1/2}||, \tag{14}$$

where $I_1 = ||(L_K + \lambda_1 I)^{-1/2}S_{\mathbf{x}}^*(\mathbf{y} - S_{\mathbf{x}}f_\rho)||_K$ and $I_2 = ||(L_K + \lambda_1 I)^{1/2}(S_{\mathbf{x}}^*S_{\mathbf{x}} + \lambda_1 I)^{-1}(L_K + \lambda_1 I)^{1/2}||$.

For sufficiently large sample size m, the following inequality holds:

$$\frac{8\kappa^2}{\sqrt{m}} \log\left(\frac{2}{\delta}\right) \leq \lambda_1 \tag{15}$$

Then from Theorem 2 [43] we have with confidence $1 - \delta$,

$$\begin{aligned} I_3 = ||(L_K + \lambda_1 I)^{-1/2}(L_K - S_{\mathbf{x}}^*S_{\mathbf{x}})(L_K + \lambda_1 I)^{-1/2}|| &\leq \frac{||S_{\mathbf{x}}^*S_{\mathbf{x}} - L_K||}{\lambda_1} \\ &\leq \frac{4\kappa^2}{\sqrt{m}\lambda_1} \log\left(\frac{2}{\delta}\right) \leq \frac{1}{2}. \end{aligned}$$

Then the Neumann series gives

$$\begin{aligned} I_2 &= ||\{I - (L_K + \lambda_1 I)^{-1/2}(L_K - S_{\mathbf{x}}^*S_{\mathbf{x}})(L_K + \lambda_1 I)^{-1/2}\}^{-1}|| \tag{16} \\ &= ||\sum_{i=0}^\infty \{(L_K + \lambda_1 I)^{-1/2}(L_K - S_{\mathbf{x}}^*S_{\mathbf{x}})(L_K + \lambda_1 I)^{-1/2}\}^i|| \leq \sum_{i=0}^\infty I_3^i = \frac{1}{1 - I_3} \leq 2. \end{aligned}$$

Now we have,

$$||L_K^s(L_K + \lambda_1 I)^{-1/2}|| \leq \sup_{0 < t \leq \kappa^2} \frac{t^s}{(t + \lambda_1)^{1/2}} \leq \lambda_1^{s-1/2} \text{ for } 0 \leq s \leq \frac{1}{2}. \tag{17}$$

To estimate the error bound for $||(L_K + \lambda_1 I)^{-1/2} S_\mathbf{x}^*(\mathbf{y} - S_\mathbf{x} f_\rho)||_K$ using the McDiarmid inequality (Lemma 2 [12]), define the function $\mathcal{F} : \mathbb{R}^m \to \mathbb{R}$ as

$$\begin{aligned}
\mathcal{F}(\mathbf{y}) &= ||(L_K + \lambda_1 I)^{-1/2} S_\mathbf{x}^*(\mathbf{y} - S_\mathbf{x} f_\rho)||_K \\
&= \frac{1}{m} \left|\left| (L_K + \lambda_1 I)^{-1/2} \sum_{i=1}^m (y_i - f_\rho(x_i)) K_{x_i} \right|\right|_K.
\end{aligned}$$

So $\mathcal{F}^2(\mathbf{y}) = \frac{1}{m^2} \sum_{i,j=1}^m (y_i - f_\rho(x_i))(y_j - f_\rho(x_j)) \langle (L_K + \lambda_1 I)^{-1} K_{x_i}, K_{x_j} \rangle_K$.

The independence of the samples together with $E_\mathbf{y}(y_i - f_\rho(x_i)) = 0$, $E_\mathbf{y}(y_i - f_\rho(x_i))^2 = \sigma_{x_i}^2$ implies

$$E_\mathbf{y}(\mathcal{F}^2) = \frac{1}{m^2} \sum_{i=1}^m \sigma_{x_i}^2 \mathcal{N}_{x_i}(\lambda_1) \leq \Xi^2,$$

where $\mathcal{N}_{x_i}(\lambda_1) = Tr\left((L_K + \lambda_1 I)^{-1} K_{x_i} K_{x_i}^*\right)$ and $\Xi = \frac{1}{m}\sqrt{\sum_{i=1}^m \sigma_{x_i}^2 \mathcal{N}_{x_i}(\lambda_1)}$. Since $E_\mathbf{y}(\mathcal{F}) \leq \sqrt{E_\mathbf{y}(\mathcal{F}^2)}$. It implies $E_\mathbf{y}(\mathcal{F}) \leq \Xi$.

Let $\mathbf{y}^i = (y_1, \ldots, y_{i-1}, y_i', y_{i+1}, \ldots, y_m)$, where y_i' is another sample at x_i. We have

$$\begin{aligned}
|\mathcal{F}(\mathbf{y}) - \mathcal{F}(\mathbf{y}^i)| &\leq ||(L_K + \lambda_1 I)^{-1/2} S_\mathbf{x}^*(\mathbf{y} - \mathbf{y}^i)||_K \\
&= \frac{1}{m}||(y_i - y_i')(L_K + \lambda_1 I)^{-1/2} K_{x_i}||_K \leq \frac{2\kappa M}{m\sqrt{\lambda_1}}.
\end{aligned}$$

This can be taken as B in Lemma 2(2) [12]. Now

$$\begin{aligned}
& E_{y_i}\left(|\mathcal{F}(\mathbf{y}) - E_{y_i}(\mathcal{F}(\mathbf{y}))|^2\right) \\
\leq\ & \frac{1}{m^2} \int_Y \left(\int_Y |y_i - y_i'|\ ||(L_K + \lambda_1 I)^{-1/2} K_{x_i}||_K d\rho(y_i'|x_i)\right)^2 d\rho(y_i|x_i) \\
\leq\ & \frac{1}{m^2} \int_Y \int_Y (y_i - y_i')^2 \mathcal{N}_{x_i}(\lambda_1) d\rho(y_i'|x_i) d\rho(y_i|x_i) \\
\leq\ & \frac{2}{m^2} \sigma_{x_i}^2 \mathcal{N}_{x_i}(\lambda_1)
\end{aligned}$$

which implies

$$\sum_{i=1}^m \sigma_i^2(\mathcal{F}) \leq 2\Xi^2.$$

In view of Lemma 2(2) [12] for every $\varepsilon > 0$,

$$\Prob_{\mathbf{y} \in Y^m} \{\mathcal{F}(\mathbf{y}) - E_\mathbf{y}(\mathcal{F}(\mathbf{y})) \geq \varepsilon\} \leq \exp\left\{-\frac{\varepsilon^2}{4(\Xi^2 + \varepsilon\kappa M/3m\sqrt{\lambda_1})}\right\} = \delta. \text{ (let)}$$

In terms of δ, probability inequality becomes

$$\Prob_{\mathbf{y} \in Y^m}\left\{\mathcal{F}(\mathbf{y}) \leq \Xi\left(1 + 2\sqrt{\log\left(\frac{1}{\delta}\right)}\right) + \frac{4\kappa M}{3m\sqrt{\lambda_1}}\log\left(\frac{1}{\delta}\right)\right\} \leq 1 - \delta.$$

Incorporating this inequality with (16), (17) in (14), we get the desired result. $\square$

Proposition 2.2. *Let* $\mathbf{z}$ *be i.i.d. samples drawn according to the probability measure* ρ *with the hypothesis* $|y_i| \leq M$ *for each* $(x_i, y_i) \in Z$*. Suppose* $f_\rho \in \Omega_{\phi,R}$*. Then for* $0 \leq s \leq \frac{1}{2}$ *and for every* $0 < \delta < 1$ *with prob.* $1 - \delta$,

$$||L_K^s(f_{\mathbf{z},\lambda} - f_\lambda)||_K \leq \frac{2\lambda_1^{s-\frac{1}{2}}}{\sqrt{m}} \left\{ 3M\sqrt{\mathcal{N}(\lambda_1)} + \frac{4\kappa}{\sqrt{\lambda_1}}||f_\lambda - f_\rho||_\rho + \frac{\sqrt{\lambda_1}}{6}||f_\lambda - f_\rho||_K \right.$$
$$\left. + \frac{7\kappa M}{\sqrt{m\lambda_1}} \right\} \log\left(\frac{4}{\delta}\right).$$

Proof. We can express $f_{\mathbf{x},\lambda} - f_\lambda = \Delta_S(S_{\mathbf{x}}^* S_{\mathbf{x}} - L_K)(f_\rho - f_\lambda)$, which implies

$$||L_K^s(f_{\mathbf{x},\lambda} - f_\lambda)||_K \leq I_4 \left\| \frac{1}{m}\sum_{i=1}^m (f_\rho(x_i) - f_\lambda(x_i))K_{x_i} - L_K(f_\rho - f_\lambda) \right\|_K.$$

where $I_4 = ||L_K^s \Delta_S||$. Using Lemma 3 [12] for the function $f_\rho - f_\lambda$, we get with confidence $1 - \delta$,

$$||L_K^s(f_{\mathbf{x},\lambda} - f_\lambda)||_K \leq I_4 \left(\frac{4\kappa||f_\lambda - f_\rho||_\infty}{3m} log\left(\frac{1}{\delta}\right) + \frac{\kappa||f_\lambda - f_\rho||_\rho}{\sqrt{m}} \left(1 + \sqrt{8log\left(\frac{1}{\delta}\right)}\right) \right). \quad (18)$$

For sufficiently large sample (15), from Theorem 2 [43] we get

$$||(L_K - S_{\mathbf{x}}^* S_{\mathbf{x}})(L_K + \lambda_1 I)^{-1}|| \leq \frac{||S_{\mathbf{x}}^* S_{\mathbf{x}} - L_K||}{\lambda_1} \leq \frac{4\kappa^2}{\sqrt{m}\lambda_1} \log\left(\frac{2}{\delta}\right) \leq \frac{1}{2}$$

with confidence $1 - \delta$, which implies

$$||(L_K + \lambda_1 I)(S_{\mathbf{x}}^* S_{\mathbf{x}} + \lambda_1 I)^{-1}|| = ||\{I - (L_K - S_{\mathbf{x}}^* S_{\mathbf{x}})(L_K + \lambda_1 I)^{-1}\}^{-1}|| \leq 2. \quad (19)$$

We have, $||L_K^s(L_K + \lambda_1 I)^{-1}|| \leq \sup_{0 < t \leq \kappa^2} \frac{t^s}{(t + \lambda_1)} \leq \lambda_1^{s-1}$ for $0 \leq s \leq 1$. $\quad (20)$

Now equation (19) and (20) implies the following inequality,

$$I_4 \leq ||L_K^s(S_{\mathbf{x}}^* S_{\mathbf{x}} + \lambda_1 I)^{-1}|| \leq ||L_K^s(L_K + \lambda_1 I)^{-1}|| \; ||(L_K + \lambda_1 I)(S_{\mathbf{x}}^* S_{\mathbf{x}} + \lambda_1 I)^{-1}|| \leq 2\lambda_1^{s-1}. \quad (21)$$

Let $\xi(x) = \sigma_x^2 \mathcal{N}_x(\lambda_1)$ be the random variable. Then it satisfies $|\xi| \leq 4\kappa^2 M^2/\lambda_1$, $E_x(\xi) \leq M^2 \mathcal{N}(\lambda_1)$ and $\sigma^2(\xi) \leq 4\kappa^2 M^4 \mathcal{N}(\lambda_1)/\lambda_1$. Using the Bernstein inequality we get

$$\operatorname*{Prob}_{\mathbf{x} \in X^m} \left\{ \sum_{i=1}^m \left(\sigma_{x_i}^2 \mathcal{N}_{x_i}(\lambda_1) - M^2 \mathcal{N}(\lambda_1)\right) > t \right\} \leq exp\left(-\frac{t^2/2}{\frac{4m\kappa^2 M^4 \mathcal{N}(\lambda_1)}{\lambda_1} + \frac{4\kappa^2 M^2 t}{3\lambda_1}} \right)$$

which implies

$$\operatorname*{Prob}_{\mathbf{x} \in X^m} \left\{ \Xi \leq \sqrt{\frac{M^2 \mathcal{N}(\lambda_1)}{m}} + \sqrt{\frac{8\kappa^2 M^2}{3m^2 \lambda_1} \log\left(\frac{1}{\delta}\right)} \right\} \geq 1 - \delta. \quad (22)$$

We get the required error estimate by combining the estimates of Proposition 2.1 with inequalities (18), (21), (22). □

Proposition 2.3. *Suppose* $f_\rho \in \Omega_{\phi,R}$*. Then under the assumption that* $\phi(t)$ *and* $t^{1-s}/\phi(t)$ *are*

nondecreasing functions, we have

$$||L_K^s(f_\lambda - f_\rho)||_K \leq \lambda_1^s \left(R\phi(\lambda_1) + \lambda_2 \lambda_1^{-3/2} M ||B^*B|| \right). \tag{23}$$

Proof. To realize the above error estimates, we decomposes $f_\lambda - f_\rho$ into $f_\lambda - f_{\lambda_1} + f_{\lambda_1} - f_\rho$. The first term can be expressed as

$$f_\lambda - f_{\lambda_1} = -\lambda_2 (L_K + \lambda_1 I + \lambda_2 B^*B)^{-1} B^* B f_{\lambda_1}.$$

Then we get

$$
\begin{aligned}
||L_K^s(f_\lambda - f_{\lambda_1})||_K &\leq \lambda_2 ||L_K^s(L_K + \lambda_1 I)^{-1}|| \, ||B^*B|| \, ||f_{\lambda_1}||_K \\
&\leq \lambda_2 \lambda_1^{s-1} ||B^*B|| \, ||f_{\lambda_1}||_K \leq \lambda_2 \lambda_1^{s-3/2} M ||B^*B||.
\end{aligned}
\tag{24}
$$

$$||L_K^s(f_{\lambda_1} - f_\rho)|| \leq R||r_{\lambda_1}(L_K) L_K^s \phi(L_K)|| \leq R\lambda_1^s \phi(\lambda_1), \tag{25}$$

where $r_{\lambda_1}(t) = 1 - (t + \lambda_1)^{-1} t$.

Combining these error bounds, we achieve the required estimate. □

Theorem 2.1. *Let $\mathbf{z}$ be i.i.d. samples drawn according to probability measure $\mathcal{P}_{\phi,b}$. Suppose $\phi(t)$ and $t^{1-s}/\phi(t)$ are nondecreasing functions. Then under parameter choice $\lambda_1 \in (0,1]$, $\lambda_1 = \Psi^{-1}(m^{-1/2})$, $\lambda_2 = (\Psi^{-1}(m^{-1/2}))^{3/2} \phi(\Psi^{-1}(m^{-1/2}))$ where $\Psi(t) = t^{\frac{1}{2} + \frac{1}{2b}} \phi(t)$, for $0 \leq s \leq \frac{1}{2}$ and for all $0 < \delta < 1$, the following error estimates holds with confidence $1 - \delta$,*

$$\Prob_{\mathbf{z} \in Z^m} \left\{ ||L_K^s(f_{\mathbf{z},\lambda} - f_\rho)||_K \leq C(\Psi^{-1}(m^{-1/2}))^s \phi(\Psi^{-1}(m^{-1/2})) \log\left(\frac{4}{\delta}\right) \right\} \geq 1 - \delta,$$

where $C = 14\kappa M + (2 + 8\kappa)(R + M||B^*B||) + 6M\sqrt{\beta b/(b-1)}$ and

$$\lim_{\tau \to \infty} \limsup_{m \to \infty} \sup_{\rho \in \mathcal{P}_{\phi,b}} \Prob_{\mathbf{z} \in Z^m} \left\{ ||L_K^s(f_{\mathbf{z},\lambda} - f_\rho)||_K > \tau (\Psi^{-1}(m^{-1/2}))^s \phi(\Psi^{-1}(m^{-1/2})) \right\} = 0.$$

Proof. Let $\Psi(t) = t^{\frac{1}{2} + \frac{1}{2b}} \phi(t)$. Then $\Psi(t) = y$ follows,

$$\lim_{t \to 0} \frac{\Psi(t)}{\sqrt{t}} = \lim_{y \to 0} \frac{y}{\sqrt{\Psi^{-1}(y)}} = 0.$$

Under the parameter choice $\lambda_1 = \Psi^{-1}(m^{-1/2})$ we have $\lim_{m \to \infty} m\lambda_1 = \infty$. Therefore for sufficiently large m,

$$\frac{1}{m\lambda_1} = \frac{\lambda_1^{\frac{1}{2b}} \phi(\lambda_1)}{\sqrt{m\lambda_1}} \leq \lambda_1^{\frac{1}{2b}} \phi(\lambda_1).$$

Under the fact $\lambda_1 \leq 1$ from Proposition 2.2, 2.3 and eqn. (12) follows that with confidence $1 - \delta$,

$$||L_K^s(f_{\mathbf{z},\lambda} - f_\rho)||_K \leq C(\Psi^{-1}(m^{-1/2}))^s \phi(\Psi^{-1}(m^{-1/2})) \log\left(\frac{4}{\delta}\right), \tag{26}$$

where $C = 14\kappa M + (2 + 8\kappa)(R + M||B^*B||) + 6M\sqrt{\beta b/(b-1)}$.

Now defining $\tau := C \log\left(\frac{4}{\delta}\right)$ gives $\delta = \delta_\tau = 4e^{-\tau/C}$. The estimate (26) can be reexpressed as

$$\Prob_{\mathbf{z} \in Z^m}\{||L_K^s(f_{\mathbf{z},\lambda} - f_\rho)||_K > \tau(\Psi^{-1}(m^{-1/2}))^s \phi(\Psi^{-1}(m^{-1/2}))\} \leq \delta_\tau. \tag{27}$$

$\square$

Corollary 2.1. *Under the same assumptions of Theorem 2.1 for Hölder's source condition $f_\rho \in \Omega_{\phi,R}$, $\phi(t) = t^r$, for $0 \leq s \leq \frac{1}{2}$ and for all $0 < \delta < 1$, with confidence $1 - \delta$, for the parameter choice $\lambda_1 = m^{-\frac{b}{2br+b+1}}$ and $\lambda_2 = m^{-\frac{2br+3b}{4br+2b+2}}$ we have the following convergence rates:*

$$||L_K^s(f_{\mathbf{z},\lambda} - f_\rho)||_K \leq Cm^{-\frac{b(r+s)}{2br+b+1}} \log\left(\frac{4}{\delta}\right) \text{ for } 0 \leq r \leq 1 - s.$$

Corollary 2.2. *Under the logarithm decay condition of effective dimension $\mathcal{N}(\lambda_1)$, for Hölder's source condition $f_\rho \in \Omega_{\phi,R}$, $\phi(t) = t^r$, for $0 \leq s \leq \frac{1}{2}$ and for all $0 < \delta < 1$, with confidence $1 - \delta$, for the parameter choice $\lambda_1 = \left(\frac{\log m}{m}\right)^{\frac{1}{2r+1}}$ and $\lambda_2 = \left(\frac{\log m}{m}\right)^{\frac{2r+3}{4r+2}}$ we have the following convergence rates:*

$$||L_K^s(f_{\mathbf{z},\lambda} - f_\rho)||_K \leq C\left(\frac{\log m}{m}\right)^{\frac{s+r}{2r+1}} \log\left(\frac{4}{\delta}\right) \text{ for } 0 \leq r \leq 1 - s.$$

Remark 2.1. The upper convergence rates of the regularized solution is estimated in the interpolation norm for the parameter $s \in [0, \frac{1}{2}]$. In particular, we obtain the error estimates in $||\cdot||_{\mathcal{H}_K}$-norm for $s = 0$ and in $||\cdot||_{\mathscr{L}_{\rho_X}^2}$-norm for $s = \frac{1}{2}$. We present the error estimates of multi-penalty regularizer over the regularity class $\mathcal{P}_{\phi,b}$ in Theorem 2.1 and Corollary 2.1. We can also obtain the convergence rates of the estimator $f_{\mathbf{z},\lambda}$ under the source condition without the polynomial decay of the eigenvalues of the integral operator L_K by substituting $\mathcal{N}(\lambda_1) \leq \frac{\kappa^2}{\lambda_1}$. In addition, for $B = (S_{\mathbf{x}'}^* LS_{\mathbf{x}'})^{1/2}$ we obtain the error estimates of the manifold regularization scheme (29) considered in [13].

Remark 2.2. The parameter choice is said to be optimal, if the minimax lower rates coincide with the upper convergence rates for some $\lambda = \lambda(m)$. For the parameter choice $\lambda_1 = \Psi^{-1}(m^{-1/2})$ and $\lambda_2 = (\Psi^{-1}(m^{-1/2}))^{3/2}\phi(\Psi^{-1}(m^{-1/2}))$, Theorem 2.1 share the upper convergence rates with the lower convergence rates of Theorem 3.11, 3.12 [44]. Therefore the choice of parameters is optimal.

Remark 2.3. The results can be easily generalized to n-penalty regularization in vector-valued framework. For simplicity, we discuss two-parameter regularization scheme in scalar-valued function setting.

Remark 2.4. We can also address the convergence issues of binary classification problem [45] using our error estimates as similar to discussed in Section 3.3 [5] and Section 5 [9].

The proposed choice of parameters in Theorem 2.1 is based on the regularity parameters which are generally not known in practice. In the proceeding section, we discuss the parameter choice rules based on samples.

3 Parameter Choice Rules

Most regularized learning algorithms depend on the tuning parameter, whose appropriate choice is crucial to ensure good performance of the regularized solution. Many parameter choice strategies

are discussed for single-penalty regularization schemes for both ill-posed problems and the learning algorithms [27, 28] (also see references therein). Various parameter choice rules are studied for multi-penalty regularization schemes [15, 18, 19, 25, 31, 32, 33, 36, 46]. Ito el al. [33] studied a balancing principle for choosing regularization parameters based on the augmented Tikhonov regularization approach for ill posed inverse problems. In learning theory framework, we are discussing the fixed point algorithm based on the penalty balancing principle considered in [33].

The Bayesian inference approach provides a mechanism for selecting the regularization parameters through hierarchical modeling. Various authors successfully applied this approach in different problems. Thompson et al. [47] applied this for selecting parameters for image restoration. Jin et al. [48] considered the approach for ill-posed Cauchy problem of steady-state heat conduction.

The posterior probability density function (PPDF) for the functional (4) is given by

$$
P(f, \sigma^2, \mu, \mathbf{z}) \;\; \propto \;\; \left(\frac{1}{\sigma^2}\right)^{n/2} \exp\left(-\frac{1}{2\sigma^2}||S_{\mathbf{x}}f - \mathbf{y}||_m^2\right) \mu_1^{n_1/2} \exp\left(-\frac{\mu_1}{2}||f||_K^2\right) \mu_2^{n_2/2}
$$

$$
\cdot \; \exp\left(-\frac{\mu_2}{2}||Bf||_K^2\right) \mu_1^{\alpha'-1} e^{-\beta'\mu_1} \mu_2^{\alpha'-1} e^{-\beta'\mu_2} \left(\frac{1}{\sigma^2}\right)^{\alpha'_o-1} e^{-\beta'_o\left(\frac{1}{\sigma^2}\right)}.
$$

where (α', β') are parameter pairs for $\mu = (\mu_1, \mu_2)$, (α'_o, β'_o) are parameter pair for inverse variance $\frac{1}{\sigma^2}$. In the Bayesian inference approach, we select parameter set (f, σ^2, μ) which maximizes the PPDF. By taking the negative logarithm and simplifying, the problem can be reformulated as

$$
\begin{aligned}
\mathcal{J}(f, \tau, \mu) \;\; = \;\; & \tau||S_{\mathbf{x}}f - \mathbf{y}||_m^2 + \mu_1||f||_K^2 + \mu_2||Bf||_K^2 \\
& + \beta(\mu_1 + \mu_2) - \alpha(log\mu_1 + log\mu_2) + \beta_o\tau - \alpha_o log\tau,
\end{aligned}
$$

where $\tau = 1/\sigma^2$, $\beta = 2\beta'$, $\alpha = n_1 + 2\alpha' - 2$, $\beta_o = 2\beta'_o$, $\alpha_o = n_2 + 2\alpha'_o - 2$. We assume that the scalars τ and μ_i's have Gamma distributions with known parameter pairs. The functional is pronounced as augmented Tikhonov regularization.

For non-informative prior $\beta_o = \beta = 0$, the optimality of a-Tikhonov functional can be reduced to

$$
\begin{cases}
f_{\mathbf{z},\lambda} = arg \min\limits_{f \in \mathcal{H}_K} \left\{||S_{\mathbf{x}}f - \mathbf{y}||_m^2 + \lambda_1||f||_K^2 + \lambda_2||Bf||_K^2\right\} \\
\mu_1 = \frac{\alpha}{||f_{\mathbf{z},\lambda}||_K^2}, \quad \mu_2 = \frac{\alpha}{||Bf_{\mathbf{z},\lambda}||_K^2} \\
\tau = \frac{\alpha_o}{||S_{\mathbf{x}}f_{\mathbf{z},\lambda} - \mathbf{y}||_m^2}
\end{cases}
$$

where $\lambda_1 = \frac{\mu_1}{\tau}$, $\lambda_2 = \frac{\mu_2}{\tau}$, $\gamma = \frac{\alpha_o}{\alpha}$, this can be reformulated as

$$
\begin{cases}
f_{\mathbf{z},\lambda} = arg \min\limits_{f \in \mathcal{H}_K} \left\{||S_{\mathbf{x}}f - \mathbf{y}||_m^2 + \lambda_1||f||_K^2 + \lambda_2||Bf||_K^2\right\} \\
\lambda_1 = \frac{1}{\gamma}\frac{||S_{\mathbf{x}}f_{\mathbf{z},\lambda} - \mathbf{y}||_m^2}{||f_{\mathbf{z},\lambda}||_K^2}, \quad \lambda_2 = \frac{1}{\gamma}\frac{||S_{\mathbf{x}}f_{\mathbf{z},\lambda} - \mathbf{y}||_m^2}{||Bf_{\mathbf{z},\lambda}||_K^2}
\end{cases}
$$

which implies

$$
\lambda_1||f_{\mathbf{z},\lambda}||_K^2 = \lambda_2||Bf_{\mathbf{z},\lambda}||_K^2.
$$

It selects the regularization parameter λ in the functional (5) by balancing the penalty with the fidelity. Therefore the term "Penalty balancing principle" follows. Now we describe the fixed point algorithm based on PB-principle.

Algorithm 1 Parameter choice rule "Penalty-balancing Principle"

1. For an initial value $\lambda = (\lambda_1^0, \lambda_2^0)$, start with $k = 0$.

2. Calculate $f_{\mathbf{z},\lambda^k}$ and update λ by

$$\lambda_1^{k+1} = \frac{||S_{\mathbf{x}} f_{\mathbf{z},\lambda^k} - \mathbf{y}||_m^2 + \lambda_2^k ||B f_{\mathbf{z},\lambda^k}||_K^2}{(1+\gamma)||f_{\mathbf{z},\lambda^k}||_K^2},$$

$$\lambda_2^{k+1} = \frac{||S_{\mathbf{x}} f_{\mathbf{z},\lambda^k} - \mathbf{y}||_m^2 + \lambda_1^k ||f_{\mathbf{z},\lambda^k}||_K^2}{(1+\gamma)||B f_{\mathbf{z},\lambda^k}||_K^2}.$$

3. If stopping criteria $||\lambda^{k+1} - \lambda^k|| < \varepsilon$ satisfied then stop otherwise set $k = k + 1$ and GOTO (2).

---

4 Numerical Realization

In this section, the performance of single-penalty regularization versus multi-penalty regularization is demonstrated using the academic example and two moon data set. For single-penalty regularization, parameters are chosen according to the quasi-optimality principle while for two-parameter regularization according to PB-principle.

We consider the well-known academic example [28, 16, 49] to test the multi-penalty regularization under PB-principle parameter choice rule,

$$f_\rho(x) = \frac{1}{10}\left\{ x + 2\left(e^{-8(\frac{4\pi}{3} - x)^2} - e^{-8(\frac{\pi}{2} - x)^2} - e^{-8(\frac{3\pi}{2} - x)^2} \right) \right\}, \quad x \in [0, 2\pi], \tag{28}$$

which belongs to reproducing kernel Hilbert space $\mathcal{H}_K$ corresponding to the kernel $K(x,y) = xy + \exp\left(-8(x - y)^2\right)$. We generate noisy data 100 times in the form $y = f_\rho(x) + \delta\xi$ corresponding to the inputs $\mathbf{x} = \{x_i\}_{i=1}^m = \{\frac{\pi}{10}(i - 1)\}_{i=1}^m$, where ξ follows the uniform distribution over $[-1, 1]$ with $\delta = 0.02$.

We consider the following multi-penalty functional proposed in the manifold regularization [13, 15],

$$\underset{f \in \mathcal{H}_K}{\operatorname{argmin}}\left\{ \frac{1}{m}\sum_{i=1}^m (f(x_i) - y_i)^2 + \lambda_1 ||f||_K^2 + \lambda_2 ||(S_{\mathbf{x}'}^* L S_{\mathbf{x}'})^{1/2} f||_K^2 \right\}, \tag{29}$$

where $\mathbf{x}' = \{x_i \in X : 1 \leq i \leq n\}$ and $L = D - W$ with $W = (\omega_{ij})$ is a weight matrix with non-negative entries and D is a diagonal matrix with $D_{ii} = \sum_{j=1}^n \omega_{ij}$.

In our experiment, we illustrate the error estimates of single-penalty regularizers $f = f_{\mathbf{z},\lambda_1}$, $f = f_{\mathbf{z},\lambda_2}$ and multi-penalty regularizer $f = f_{\mathbf{z},\lambda}$ using the relative error measure $\frac{||f - f_\rho||}{||f||}$ for the academic example in sup norm, $\mathcal{H}_K$-norm and $|| \cdot ||_m$-empirical norm in Fig. 1 (a), (b) & (c) respectively.

Now we compare the performance of multi-penalty regularization over single-penalty regularization method using the well-known two moon data set (Fig. 2) in the context of manifold learning. The data set contains 200 examples with k labeled example for each class. We perform experiments 500 times by taking $l = 2k = 2, 6, 10, 20$ labeled points randomly. We solve the manifold regularization problem (29) for the mercer kernel $K(x_i, x_j) = \exp(-\gamma||x_i - x_j||^2)$ with the exponential weights $\omega_{ij} = \exp(-||x_i - x_j||^2/4b)$, for some $b, \gamma > 0$. We choose initial parame-
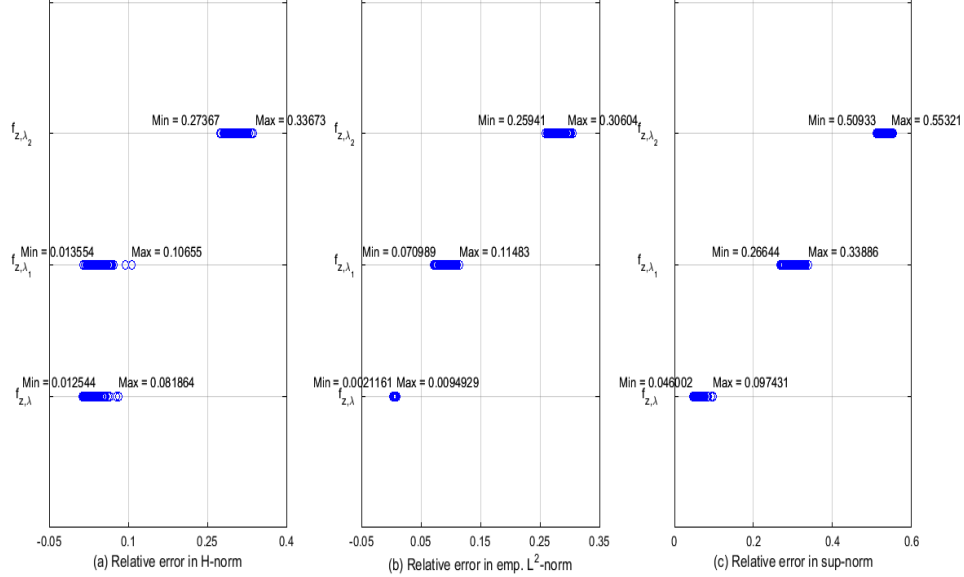
Figure 1: Figures show the relative errors of different estimators for the academic example in $||\cdot||_{\mathcal{H}}$-norm (a), $||\cdot||_m$-empirical norm (b) and infinity norm (c) corresponding to 100 test problems with the noise $\delta = 0.02$ for all estimators.

ters $\lambda_1 = 1 \times 10^{-14}$, $\lambda_2 = 4.5 \times 10^{-3}$, the kernel parameter $\gamma = 3.5$ and the weight parameter $b = 3.125 \times 10^{-3}$ in all experiments. The performance of single-penalty ($\lambda_2 = 0$) and the proposed multi-penalty regularizer (29) is presented in Fig. 2, Table 1.
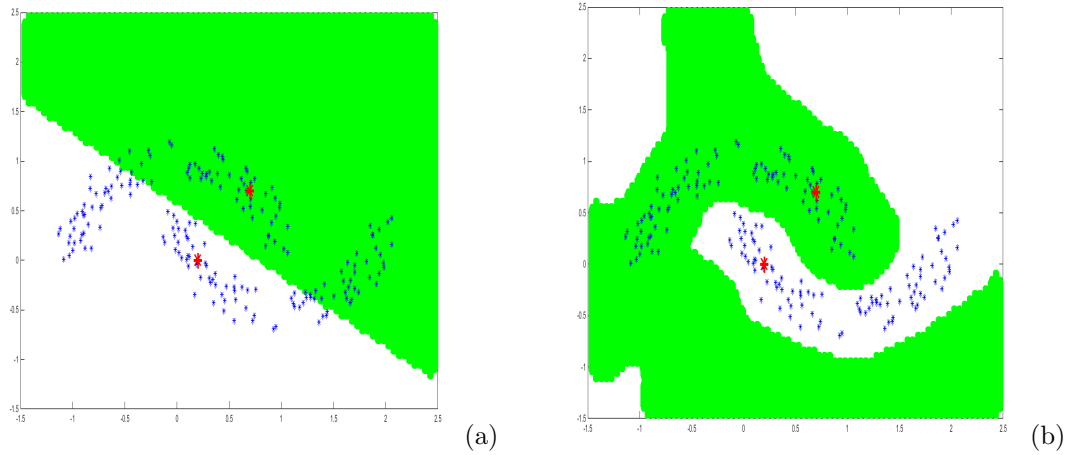
Figure 2: The figures show the decision surfaces generated with two labeled samples (red star) by single-penalty regularizer (a) based on the quasi-optimality principle and manifold regularizer (b) based on PB-principle.

Based on the considered examples, we observe that the proposed multi-penalty regularization with the penalty balancing principle parameter choice outperforms the single-penalty regularizers.

5   Conclusion

In summary, we achieved the optimal minimax rates of multi-penalized regression problem under the general source condition with the decay conditions of effective dimension. In particular,

	Single-penalty Regularizer			Multi-penalty Regularizer		
	(SP %)	(WC)	Parameters	(SP %)	(WC)	Parameters
$m = 2$	76.984	89	$\lambda_1 = 1.2 \times 10^{-14}$	100	0	$\lambda_1 = 1.1103 \times 10^{-14}$ $\lambda_2 = 5.9874 \times 10^{-4}$
$m = 6$	88.249	112	$\lambda_1 = 1.2 \times 10^{-14}$	100	0	$\lambda_1 = 9.8784 \times 10^{-15}$ $\lambda_2 = 5.7020 \times 10^{-4}$
$m = 10$	93.725	77	$\lambda_1 = 1.2 \times 10^{-14}$	100	0	$\lambda_1 = 1.0504 \times 10^{-14}$ $\lambda_2 = 7.3798 \times 10^{-4}$
$m = 20$	98.100	40	$\lambda_1 = 1.2 \times 10^{-14}$	100	0	$\lambda_1 = 1.0782 \times 10^{-14}$ $\lambda_2 = 7.0076 \times 10^{-4}$

Table 1: Statistical performance interpretation of single-penalty ($\lambda_2 = 0$) and multi-penalty regularizers of the functional

Symbols: labeled points (m); successfully predicted (SP); maximum of wrongly classified points (WC)

the convergence analysis of multi-penalty regularization provide the error estimates of manifold regularization problem. We can also address the convergence issues of binary classification problem using our error estimates. Here we discussed the penalty balancing principle based on augmented Tikhonov regularization for the choice of regularization parameters. Many other parameter choice rules are proposed to obtain the regularized solution of multi-parameter regularization schemes. The next problem of interest can be the rigorous analysis of different parameter choice rules of multi-penalty regularization schemes. Finally, the superiority of multi-penalty regularization over single-penalty regularization is shown using the academic example and moon data set.

References

[1] O. Bousquet, S. Boucheron, and G. Lugosi, "Introduction to statistical learning theory," in *Advanced lectures on machine learning*, pp. 169–207, Berlin/Heidelberg: Springer, 2004.

[2] F. Cucker and S. Smale, "On the mathematical foundations of learning," *Bull. Amer. Math. Soc. (NS)*, vol. 39, no. 1, pp. 1–49, 2002.

[3] T. Evgeniou, M. Pontil, and T. Poggio, "Regularization networks and support vector machines," *Adv. Comput. Math.*, vol. 13, no. 1, pp. 1–50, 2000.

[4] V. N. Vapnik and V. Vapnik, *Statistical Learning Theory*, vol. 1. New York: Wiley, 1998.

[5] F. Bauer, S. Pereverzev, and L. Rosasco, "On regularization algorithms in learning theory," *J. Complexity*, vol. 23, no. 1, pp. 52–72, 2007.

[6] A. Caponnetto and E. De Vito, "Optimal rates for the regularized least-squares algorithm," *Found. Comput. Math.*, vol. 7, no. 3, pp. 331–368, 2007.

[7] H. W. Engl, M. Hanke, and A. Neubauer, *Regularization of Inverse Problems*, vol. 375. Dordrecht, The Netherlands: Math. Appl., Kluwer Academic Publishers Group, 1996.

[8] L. L. Gerfo, L. Rosasco, F. Odone, E. De Vito, and A. Verri, "Spectral algorithms for supervised learning," *Neural Computation*, vol. 20, no. 7, pp. 1873–1897, 2008.

[9] S. Smale and D. X. Zhou, "Learning theory estimates via integral operators and their approximations," *Constr. Approx.*, vol. 26, no. 2, pp. 153–172, 2007.

[10] A. N. Tikhonov and V. Y. Arsenin, *Solutions of Ill-posed Problems*, vol. 14. Washington, DC: W. H. Winston, 1977.

[11] S. Smale and D. X. Zhou, "Shannon sampling and function reconstruction from point values," *Bull. Amer. Math. Soc.*, vol. 41, no. 3, pp. 279–306, 2004.

[12] S. Smale and D. X. Zhou, "Shannon sampling II: Connections to learning theory," *Appl. Comput. Harmonic Anal.*, vol. 19, no. 3, pp. 285–302, 2005.

[13] M. Belkin, P. Niyogi, and V. Sindhwani, "Manifold regularization: A geometric framework for learning from labeled and unlabeled examples," *J. Mach. Learn. Res.*, vol. 7, pp. 2399–2434, 2006.

[14] D. Düvelmeyer and B. Hofmann, "A multi-parameter regularization approach for estimating parameters in jump diffusion processes," *J. Inverse Ill-Posed Probl.*, vol. 14, no. 9, pp. 861–880, 2006.

[15] S. Lu and S. V. Pereverzev, "Multi-parameter regularization and its numerical realization," *Numer. Math.*, vol. 118, no. 1, pp. 1–31, 2011.

[16] S. Lu, S. Pereverzyev Jr., and S. Sivananthan, "Multiparameter regularization for construction of extrapolating estimators in statistical learning theory," in *Multiscale Signal Analysis and Modeling*, pp. 347–366, New York: Springer, 2013.

[17] Y. Lu, L. Shen, and Y. Xu, "Multi-parameter regularization methods for high-resolution image reconstruction with displacement errors," *IEEE Trans. Circuits Syst. I: Regular Papers*, vol. 54, no. 8, pp. 1788–1799, 2007.

[18] V. Naumova and S. V. Pereverzyev, "Multi-penalty regularization with a component-wise penalization," *Inverse Problems*, vol. 29, no. 7, p. 075002, 2013.

[19] S. N. Wood, "Modelling and smoothing parameter estimation with multiple quadratic penalties," *J. R. Statist. Soc.*, vol. 62, pp. 413–428, 2000.

[20] P. Xu, Y. Fukuda, and Y. Liu, "Multiple parameter regularization: Numerical solutions and applications to the determination of geopotential from precise satellite orbits," *J. Geodesy*, vol. 80, no. 1, pp. 17–27, 2006.

[21] Y. Luo, D. Tao, C. Xu, D. Li, and C. Xu, "Vector-valued multi-view semi-supervsed learning for multi-label image classification.," in *AAAI*, pp. 647–653, 2013.

[22] Y. Luo, D. Tao, C. Xu, C. Xu, H. Liu, and Y. Wen, "Multiview vector-valued manifold regularization for multilabel image classification," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 24, no. 5, pp. 709–722, 2013.

[23] H. Q. Minh, L. Bazzani, and V. Murino, "A unifying framework in vector-valued reproducing kernel Hilbert spaces for manifold regularization and co-regularized multi-view learning," *J. Mach. Learn. Res.*, vol. 17, no. 25, pp. 1–72, 2016.

[24] H. Q. Minh and V. Sindhwani, "Vector-valued manifold regularization," in *International Conference on Machine Learning*, 2011.

[25] Abhishake and S. Sivananthan, "Multi-penalty regularization in learning theory," *J. Complexity*, vol. 36, pp. 141–165, 2016.

[26] F. Bauer and S. Kindermann, "The quasi-optimality criterion for classical inverse problems," *Inverse Problems*, vol. 24, p. 035002, 2008.

[27] A. Caponnetto and Y. Yao, "Cross-validation based adaptation for regularization operators in learning theory," *Anal. Appl.*, vol. 8, no. 2, pp. 161–183, 2010.

[28] E. De Vito, S. Pereverzyev, and L. Rosasco, "Adaptive kernel methods using the balancing principle," *Found. Comput. Math.*, vol. 10, no. 4, pp. 455–479, 2010.

[29] V. A. Morozov, "On the solution of functional equations by the method of regularization," *Soviet Math. Dokl*, vol. 7, no. 1, pp. 414–417, 1966.

[30] J. Xie and J. Zou, "An improved model function method for choosing regularization parameters in linear inverse problems," *Inverse Problems*, vol. 18, no. 3, pp. 631–643, 2002.

[31] S. Lu, S. V. Pereverzev, and U. Tautenhahn, "A model function method in regularized total least squares," *Appl. Anal.*, vol. 89, no. 11, pp. 1693–1703, 2010.

[32] M. Fornasier, V. Naumova, and S. V. Pereverzyev, "Parameter choice strategies for multi-penalty regularization," *SIAM J. Numer. Anal.*, vol. 52, no. 4, pp. 1770–1794, 2014.

[33] K. Ito, B. Jin, and T. Takeuchi, "Multi-parameter Tikhonov regularization–An augmented approach," *Chinese Ann. Math.*, vol. 35, no. 3, pp. 383–398, 2014.

[34] M. Belge, M. E. Kilmer, and E. L. Miller, "Efficient determination of multiple regularization parameters in a generalized L-curve framework," *Inverse Problems*, vol. 18, pp. 1161–1183, 2002.

[35] F. Bauer and O. Ivanyshyn, "Optimal regularization with two interdependent regularization parameters," *Inverse problems*, vol. 23, no. 1, pp. 331–342, 2007.

[36] F. Bauer and S. V. Pereverzev, "An utilization of a rough approximation of a noise covariance within the framework of multi-parameter regularization," *Int. J. Tomogr. Stat*, vol. 4, pp. 1–12, 2006.

[37] Z. Chen, Y. Lu, Y. Xu, and H. Yang, "Multi-parameter Tikhonov regularization for linear ill-posed operator equations," *J. Comp. Math.*, vol. 26, pp. 37–55, 2008.

[38] C. Brezinski, M. Redivo-Zaglia, G. Rodriguez, and S. Seatzu, "Multi-parameter regularization techniques for ill-conditioned linear systems," *Numer. Math.*, vol. 94, no. 2, pp. 203–228, 2003.

[39] N. Aronszajn, "Theory of reproducing kernels," *Trans. Amer. Math. Soc.*, vol. 68, pp. 337–404, 1950.

[40] P. Mathé and S. V. Pereverzev, "Geometry of linear ill-posed problems in variable Hilbert scales," *Inverse problems*, vol. 19, no. 3, pp. 789–803, 2003.

[41] S. Lu, P. Mathé, and S. Pereverzyev, "Balancing principle in supervised learning for a general regularization scheme," *RICAM-Report*, vol. 38, 2016.

[42] G. Blanchard and P. Mathé, "Discrepancy principle for statistical inverse problems with application to conjugate gradient iteration," *Inverse problems*, vol. 28, no. 11, p. 115011, 2012.

[43] E. De Vito, L. Rosasco, A. Caponnetto, U. De Giovannini, and F. Odone, "Learning from examples as an inverse problem," *J. Mach. Learn. Res.*, vol. 6, pp. 883–904, 2005.

[44] A. Rastogi and S. Sivananthan, "Optimal rates for the regularized learning algorithms under general source condition," *Front. Appl. Math. Stat.*, vol. 3, p. 3, 2017.

[45] S. Boucheron, O. Bousquet, and G. Lugosi, "Theory of classification: A survey of some recent advances," *ESAIM: probability and statistics*, vol. 9, pp. 323–375, 2005.

[46] S. Lu and S. Pereverzev, *Regularization Theory for Ill-posed Problems: Selected Topics*, vol. 58. Berlin: Walter de Gruyter, 2013.

[47] A. M. Thompson and J. Kay, "On some choices of regularization parameter in image restoration," *Inverse Problems*, vol. 9, pp. 749–761, 1993.

[48] B. Jin and J. Zou, "Augmented Tikhonov regularization," *Inverse Problems*, vol. 25, no. 2, p. 025001, 2008.

[49] C. A. Micchelli and M. Pontil, "Learning the kernel function via regularization," *J. Mach. Learn. Res.*, vol. 6, no. 2, pp. 1099–1125, 2005.

AUTHOR INDEX