STEGANALYSIS ALGORITHM FOR PNG IMAGES BASED ON FUZZY LOGIC TECHNIQUE

Jawaher alqahtani, Daniyal Alghazzawi [1] and Li Cheng [2]

[1]Department of Information Systems, King Abdulaziz University, Jeddah, Saudi Arabia
[2]Xinjiang Technical Institute of Physics & Chemistry, Chinese Academy of Sciences, China

ABSTRACT

Embedding a message in media files, also known as steganography, is a common approach to hide secret information. It has been exploited by some criminals to confidentially exchange messages. As a counter-measure, tools have been developed in order to detect hidden information form digital media such as text, image, audio or video files. However the efficiency and performance of previous approaches still have room for improvement. In this research, we focus on algorithm design for better efficiency of hidden message detection from PNG files. We employ three classic AI approaches including neural network, fuzzy logic, and genetic algorithm and evaluate their efficiency and performance in controlled experiments. Finally we introduce our message detection system for PNG files based on LSB approach and present its usability in different case scenarios.

KEYWORDS

Steganography, Steganalysis, Artificial Intelligence, fuzzy logic.

1. INTRODUCTION

In recent years, the rapid advancements in technologies and communication have generated an increase in the number of cyber-crimes cases. The biggest obstacle facing digital forensic examiners is the analysis and identification of hidden data in digital media (images, audio and video).

In digital forensics there are many indications which point to the use of hidden data in digital media in the planning for criminal activities [1]. Hiding information refers to the process of inserting and embedding information in digital content, such as, image, audio or video, without drawing attention to the change. This process is called Steganography, while trying to detect the hidden information is called steganalysis.

Every day there is a new steganography tool to hide data; however, steganalysis algorithms have difficulty in detecting the hidden data because the majority of it is based on rule-based techniques. In addition, the majority of steganography tools focus on hiding data inside images. The researcher found that there is little research on detecting hidden data in the PNG format. Therefore, there is a vulnerability to discover the hidden data on the PNG format.

Many crimes have been committed undetected by hiding and exchanging information between criminals in a confidential manner. The process of hiding information in any carrier is called Steganography. There are many algorithms that are used for this purpose and will be discussed in Section 1. In the opposite direction, there is a process known as steganalysis, which detects hidden data and it will be discussed in Section 2. Steganography can hide any data in any media,

DOI: 10.5121/ijnsa.2016.8501

therefore, we will focus on the image as a carrier in Section 3. In Section 4, we will discuss AI techniques that can be used to replace the traditional detection methods. Finally, the paper introduces the proposed system for detecting the hidden data. In the end, we conclude that the fuzzy logic system accomplished high performance in terms of classifying the clean and stego images in PNG images.

2. OVERVIEW OF STEGANOGRAPHY

The term steganography consists of two greek words: stegano which mean hidden or cover and grape which means writing [2]. Steganography was defined as "an ancient discipline which usually refers to hiding information within information"[3]. The purpose of this concealment process is to prevent a third party being aware of the existence of the information, thereby protecting it from reading, change or destruction by the third party [4].

Steganography has been used for a long time. In 480 BC a Greek man named Demaratus sent a message to the Spartans warning of possible invasion by Xerxes. Demaratus scraped the wax off a wooden table, wrote on the wood what Xerxes wanted to do and then cover the message with wax [5].

Many steganography techniques were used in World War II. For example, the United States Marines used Navajo "codetalkers." In addition, invisible ink was used to write secret messages while the paper appeared blank to the human eye. Extracting the secret message was done by heating a liquid such as vinegar or milk [2]. Steganography has grown rapidly and attracted more attention since ancient times. Various steganography techniques have been created and developed to hide information in different carriers [5].

The basic stenography model contains the cover (also known as a carrier), password and message (see Figure 1). The cover is a file used to hide the presence of information and the password or stego key ensures that only the recipient will be able to extract the hidden information. The stego key used to insert (embed) and extract a secret message on the cover. The message is the embedded information. The result of inserting the message into the cover file is called a stego file[6, 7].

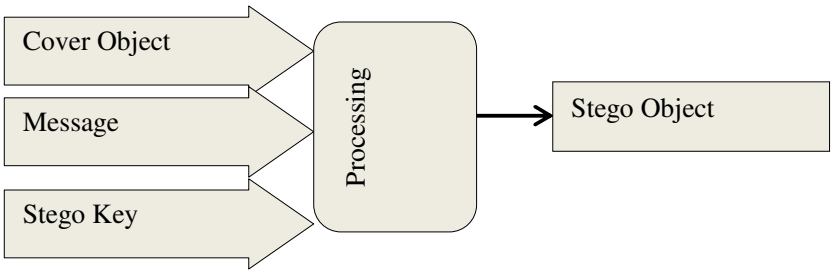

Figure 1. Steganography process

2.1. Steganography Vs. Cryptography

Information security has many disciplines such as steganography and cryptography (Figure 2). In some cases confusion arises between steganography and cryptography. Cryptography scrambles the information so that an unauthorised person can be aware of its existence but is unable to read or understand it [7]. Steganography secures the information, so that an unauthorised reader does not know if there is a message or not [7].

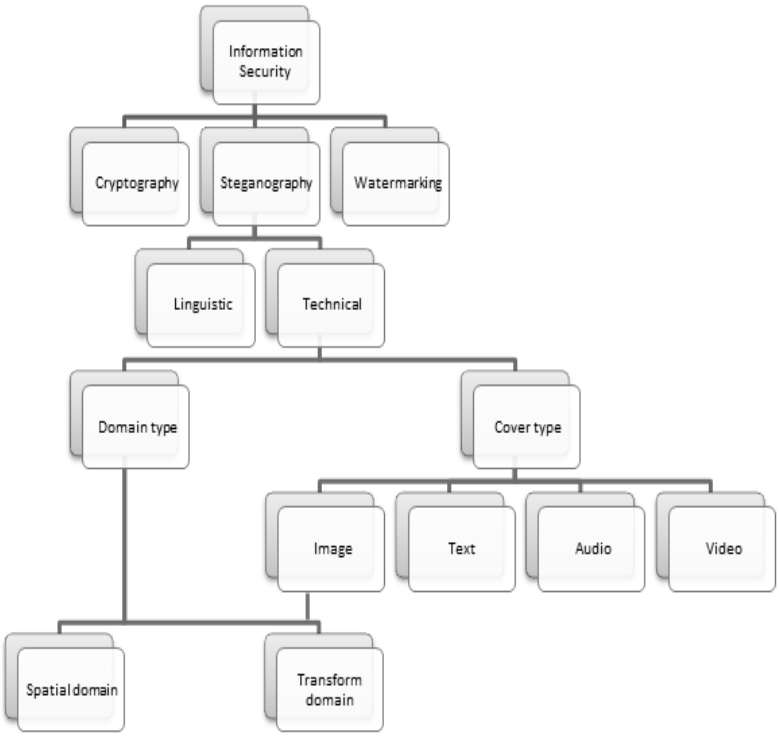

Figure 2. Information security sub-sections

The main differences between cryptography and steganography are summarised in Table 1. The process of attempting to discover the presence of hidden information, and read, change or delete bit is known as Steganalysis.

Table 1. Cryptography vs. Steganography

	Steganography	**Cryptography**
Definition	Depend on hiding the message existence	Depend on hiding the message meaning
Purpose	Keep communication secure.	Provide protection for data
Visibility	Never	Always
Failure	When discover the presence of a hidden message	When able to decrypt and read the message
Concern	Embedding capacity and detectability of cover object	Robustness against deciphering.
Carrier	Any type of digital media	Depend on text as a carrier
Key	Optional, but provide more security	Necessary

2.2. Steganography Classifications and Techniques

The classification of steganography presented in [8] is based on many standards, as shown in Figure 3. The spatial domain, [9] indicates the classifications of spatial domain image steganography techniques. These techniques are: least significant bit steganography, Pixel Value

Differencing steganography, RGB based steganography, Mapping based steganography, Speared spectrum steganography, Palette based steganography, Code based steganography and Collage based steganography. In the transform domain, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) are the most common techniques which are used for JPEG images [10].

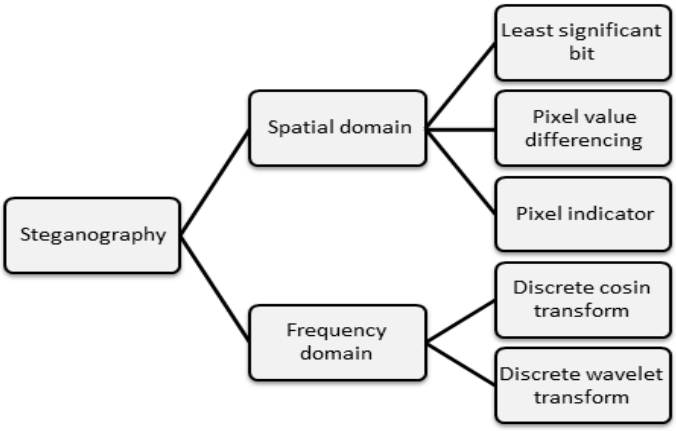

Figure 3. Steganography techniques

2.2.1. Spatial Domain Steganography Techniques

There are many techniques used for image steganography. According to [11] [11] the common effective techniques in image steganography are: Least Significant Bits substitution, Palette Modification and Blocking.

LSB substitution refers to the process of modifying the least significant bit (lsb) of the carrier image's pixel. Palette modification replaces the unused colours within the carrier image's palette with colours that contain and represent the hidden information. Blocking breaks the image into blocks and uses the Discrete Cosine Transform (DCT). The block is divided into 64 DCT coefficients that approximate colour and luminance.

The least significant bits substitution is a method of inserting information in the selected cover image. The LSB modification is not usually detectable by the human eye because this technique causes minor changes in the colours [12]. The LSB is the simplest method of inserting secret information into the image. It is easy to understand and apply [13] . In December 2011, WetStone declared that about 70% of steganography tools are based on the LSB algorithm [14].
The LSB is the most effective technique for BMP and PNG images since their compression is lossless. In addition, grayscale GIF images can use the LSB algorithm while this algorithm would change the whole colour palette of a coloured GIF image at the beginning of the modification process.

The LSB method is based on substitution which can be done up to 4 least significant bits. It depends on replacing the embedding information at the least significant bit of each pixel in the cover images. The result of embedding is a stego image. This replacement does not change the image quality of human perception [15]. It is the most common method of steganography. It is simple and it can provide a high capacity by allowing information to be inserted into all of the pixels of the cover image, however, humans may notice when information is embedded in a smooth area of the image [16-18].

However, with the PVD approach, there is need to reference and compare the original image with the stego image. The inclusion of information in the cover image is done by replacing the difference values calculated from values of two consecutive pixels of the cover image with similar values in which bits of inserted information are included [17].

The PVD focuses on concealing information in the edge area to increase the security without considering the possibility of increasing the amount of hidden information [18]. The LSB method can provide more capacity while the PVD method can provide more security. These two techniques, PVD and LSB, can provide a high degree of security and capacity when it used together [9].

A new technique was proposed based on the security of PVD and capacity of LSB [18] This approach increased the amount of hidden information by inserting more in the pixels in the outer area and increased the security by inserting less in the smooth area.

2.2.2. Transform Domain Steganography Techniques

Discrete Cosine Transform steganography (DCT) is a technique used to transform domain images like JPEG. It can transform an image from the spatial to frequency domain. DCT separates the JPEG image into parts according to their importance. The image is separated into low frequency, middle frequency and high frequency components. The high frequency components are removed through noise attacks and compression while the most important visual parts are in the low frequency. The secret information is inserted by modifying the coefficients of the middle frequency without affecting image visibility [10].

Discrete Wavelet Transform steganography (DWT) is also used for JPEG images. It was introduced as highly flexible and efficient method of signals. A signal energy concentrates into wavelet coefficients. Wavelets can convert an image to a series of wavelets which can be stored in efficient way more than blocks of pixels [19].

3. STEGANALYSIS

Hiding information has been the objective of many researchers and scientists over the years as has its discovery or steganalysis [20]. Steganalysis is the process of detecting information hidden from a third party. Steganalysis aims to collect evidence about the existence of hidden messages. Steganalysis is used in computer forensics and criminal activities on the internet [21].

According to [22], steganalysis algorithms of image can be divided into: specific algorithms and blind (generic) algorithms. Blind (generic or universal) algorithms work independently of the algorithms used in steganography and require a high degree of statistical analysis and complex computations. They provide a good and improved result [20]. In the specific steganalysis, the algorithm used depend on the image format and the algorithm used in steganography [20, 22].

The audio steganalysis algorithms take advantage of variations in the features of the audio signal after embedding the secret message. The algorithm detects the gap phase, amplitude variations and changes in the non-perceptual and perceptual audio quality metrics after embedding messages. The video steganalysis algorithms which use temporal redundancies are more effective than those that depend on spatial redundancies [22].

[23] Presents a classification of steganalysis based on performance capacity. Steganalysis applied to individual images is small scale steganalysis, whereas steganalysis performed on a large number of images is large scale steganalysis. It is better to use small scale analysis when applying

it to social media where users can send many images daily. Universal steganalysis is used in large scale steganalysis for more efficiency.

3.1. Steganalysis Techniques

Steganalysis has two main types of techniques: Statistical analysis and Visual analysis [24, 25]. Visual analysis depends on human eyes. In visual analysis, human abilities are used to detect the presence of hidden information and secret communication. Visual inspection by eye can distinguish and succeed in detecting hidden messages, especially when secret information is embedded in the smooth area of an image [24, 25].

Statistical analysis is usually used to detect steganography. It can identify tiny modifications in the statistical properties of the image caused by steganography [24, 25].

In addition, Steganalysis techniques can be classified as belonging to the spatial domain or transform domain as in steganography [26]. A new steganalysis technique proposed by [1] uses Colour Model Conversion to distinguish between the stego image and the original image. This technique was tested on the stego-image generated by SIG tool (Stego-Image Generator) which use the least significant bit algorithm.

In order to detect hidden data using LSB steganography, [6] presents the following methods of steganalysis:

- Chi-squared which is the earliest method used to reveal LSB hidden in jpeg coefficients.
- Binary Similarity Measures.
- Regular/Singular (RS) scheme.
- Sample pair analysis.

The RS scheme and sample pair analysis are regarded as powerful LSB detection methods [6].

3.2. Steganalysis Tools

There are many steganalysis tools available to the public. Some of these tools designed to detect certain steganography algorithms, consider this as a weakness of the steganalysis tool [27]. An Experiment was done by [27] to compare the efficacy and response-time of StegalyzerAS and StegalyzerSS software. The researchers use JPEG and PNG images as the cover file and create the steganography by using open source applications like SecrtLayer, Openpuff, OpenStego, Steg, steganographyStudio and GhostHost. The results of detection are represented in Table2

Table 2. StegalyzerAS & StegalyzerSS detection

		Steganalysis tools	
		StegalyzerAS	**StegalyzerSS**
Steganography tool	SecretLayer		
	Openpuff	✔	
	OpenStego		
	Steg		
	SteganographyStudio	✔	
	GhostHost		✔

We have done an experiment to measure steganalysis tool detection. Our experiment was done by using three steganography tools (ImgStegano, Openpuff, OpenStego) to hide a secret message into PNG images. To detect the secret message, we have been using five steganalysis tools. The

result shows that there is no tool can detect the hidden message embedding by all three steganography tools (see Table 3).

Table 3. Result of testing steganalysis tools

		Steganalysis tools				
		StegSpy	**OpenStego**	**ImgStegano**	**StegoPNG**	**StegExpose**
Steganography Tool	ImgStegano	✔		✔		
	Openpuff	✔				
	OpenStego		✔			

According to our experiment and [27], there is no tool can detect the hidden data in PNG image embedded by any steganography tool.

4. IMAGE IN STEGANOGRAPHY AND STEGANALYSIS

Many digital mediums can be used to hide information, such as images, video and audio [15]. The image in the computer system is stored as an array of pixels, which can be coloured or grayscale. An array of the coloured image is a combination of the three basic colours: Red, Green and Blue. Each pixel in the coloured image is represented by 24 bits. In a grayscale image there is only one channel and 8 bits used to represent each pixel.

The image can be manipulated in the transform domain (frequency domain) or spatial domain [9, 28]. The spatial domain directly manipulates the pixel values of an image whereas the transform domain deals with the rate at which the values of the pixels are changing in the spatial domain. The transform domain is more complex than the spatial domain [26, 29].

Images have a set of formats which differ in their structures and features. The most popular formats are JPEG, GIF, BMP and PNG because of their broadband speeds, compatibility with browsers and users' needs [15].

4.1. JPEG Images

JPEG stands for Joint Photographic Experts Group. It is the most common image format. It can be manipulated under the transform domain. The common steganography tools that are available to embed information into jpeg image are JSteg-Shell, JSteg, Outguess and JPhide [20]. A steganalysis technique depends on the Discrete Cosine Transform (DCT) Proposed by [30] to detect steganography in JPEG images. The F5 steganalysis algorithm is used to discover information hidden in an image by an F5 steganography algorithm. After applying the F5 algorithm, the status of the image will change.

Applying the F5 algorithm for steganalysis to compare the stego image and cover image uses the DCT and analyses the histogram of both. The result of this comparison will show whether the image is a stego image or not [30].

4.2.GIF Images

The Graphics Interchange Format (GIF) was introduced in 1987 by CompuServe. Due to its huge support and portability, GIF is widely used on the World Wide Web [31]. Palette image steganalysis is used for GIF images. The LSB technique changes the 24bit RGB value of a pixel results [31].

4.3. BMP Images

BMP (known as bitmap image) is the native format of the windows platform. It acts as the parent format of JPEG and GIF. The BMP format does not usually allow for the compression of images. Raw image steganalysis is used for the BMP image and it has a lossless LSB plane. While embedding over the lossless LSB plane results in casting over two grayscale values. Statistical analysis over a BMP image shows the length of the hidden message[20].

4.4. PNG Images

PNG (Portable Network Graphics) was designed as an alternative to the GIF image format [12]. A PNG image is much larger than a GIF image and capable of sorting more transparency and colour depth than GIF. It has more efficient compression techniques than GIF [20]. PNG supports grayscale, true colour and indexed colours in addition to an optional alpha channel. It is robust, provides simple detection of transmission errors and fulfils integrity checking.

The PNG structure always starts with a signature which contains eight bytes. The decimal values of signature are: 137 80 78 71 13 10 26 10. A series of chunks follow the signature where each chunk contains four parts: chunk type/name, length and cyclic redundancy code which each contain four bytes. The fourth part is chuck data (length bytes).

According to the image format, [32] introduced a review of steganalysis techniques. To avoid the loss of hidden data, JPEG use frequency domain steganalysis. The other formats (GIF, PNG, and BMP) use spatial domain steganalysis.

The steganalysis techniques for grayscale images are easier than the techniques for coloured images and can detect hidden information more accurately. Most steganalysis techniques are applied to JPEG and BMP images and there is insufficient research on GIF and PNG images. Hence, further research must be conducted on PNG steganalysis techniques. [15] concluded that the PNG image is the most suitable format for LSB steganography when the focus is on the amount of the information to be sent. The PNG image has the ability to hide a large amount of information.

When we take a screenshot on the iPhone, android and windows systems, the image is automatically saved as a PNG. PNG has many capabilities which make it superior to other image formats (Table 4). PNG compression is fully lossless, and restoring or resaving an image will not alter its quality unlike JPEG. PNG supports full transparency information unlike JPEG (for JPEG, there is no transparency). It supports up to 16bit grayscale or 48bit truecolour and it is more appropriate for images with few colours or images with a lot of sharp edges[33].

Table 4. Comparison between Image formats

	JPEG	TIFF	GIF	PNG
Transparency			✔	✔
Palette image		✔	✔	✔
Truecolor	✔	✔		✔
Best compression				✔
Web supporting	✔		✔	✔
Animation			✔	

With LSB steganography, the PNG image is the most suitable format when the focus is on the amount of information to be sent. The PNG image has the ability to hide a large amount of information.

5. ARTIFICIAL INTELLIGENCE IN IMAGE STEGANALYSIS

A few studies have been conducted on identifying how more advanced techniques could be applied and used to perform the intelligent processing of digital forensics. Automation approaches have been adopted into digital forensic processes to increase the speed and decrease the time required to identify a relevant evidence [34]. According to [35] it is necessary to enhance the use of the resources available. Intelligent techniques and tools could enhance the investigation in terms of efficiency and time when applied to digital investigations.

Most efforts focus on partially automating the processes of digital forensics to save time and resources. According to [36], computational intelligence has a strong chance of being applied successfully to a steganalytic system or steganasystem. Three major methods of computational intelligence have been identified to be useful in steganalysis: Bayesian, neural network, and genetic algorithm. These three techniques are applied in image steganalysis, audio steganalysis, and video steganalysis. The result of [36] and other studies discussed in this paper, shows that the application of computational intelligence methods has had a high effect on the performance of steganalysis.

The Automated Forensic Examiner is an approach proposed by [34] which aims to solve the problem of sorting and identifying relevant artefacts by applying artificial intelligence. A number of techniques used by AFE such as visualization and competency measure to provide and present an investigator with deeply understanding of cases.

The agent system will increase the speed and effectiveness and provide better results. [37] suggested a steganalysis technique based on statistics to discover the hidden information and used a Multi Agent System. MAS is capable of using all set agents to determine if the image contained hidden information or not, where each agent has a specific task to do. The main techniques of Artificial intelligence are: Neural Network, Fuzzy Logic and Genetic Algorithm.

5.1. Neural Network

Specific discovering provides highly accurate and more reliable results than general (universal) discovering. Approaches based the Neural Network are studied in [38] to measure its effectiveness in detecting hidden information. The most popular approaches are: visual detection, which is based on first order statistics, dual statistics methods that use spatial correlations in images and higher order statistics which is a general blind discovering.

The high degree of redundancy present in the image is used for performing steganography. [39] suggested a method based on the neural network and a random selection of pixels. This technique shows how a selection of different portions of the images increased the chances of hiding information in a more effective way. This technique reduces the chances of information detection. A detection system using an Artificial Neural Network (ANN) presented by [40] to classify the stego images and clean images. This system provide result with high accuracy rate because ANN is a blind classifier. The results are very good and have a lower misclassification rate than other ANNs.

5.2. Fuzzy logic

A multi-agent system for image steganalysis presented by [11]. This system is based on the paradigm of the community of polygenic bees using fuzzy logic. The system is designed to detect a file contain hidden data. The result presents accuracy rate of 89.37%, with 10.54% for false negative and 10.63% for false positive.

Also, [11] test a decision tree using entire dataset without polygenic multi agent system fuzzy clustering steganalysis. The result show accuracy rate of 72.45% with 26.92% for false negative and 27.23% for false positive. An accuracy rate of 56% for JPHide and Seek with Adaboost and 0.8% with OAASVM presented by[41].

5.3. Genetic Algorithm

The steganalysis process can be improved using genetic algorithms. The new approach for universal steganalysis proposed in [42] is based on the genetic algorithm (GA) and higher order statistics. This approach increases the accuracy of universal detection.

6. THE PROPOSED SYSTEM

Two basic stages represent the proposed system building process. The first stage focus on create a collection of stego images when texts and images are embedded into clean images as hidden data (See Figure 4) . OpenStego and Steganography Studio are the selected steganography tools, which support LSB (Least Significant Bit). The hiding ratio is between 11% and 20%. More than 600 images of people, animals, food, landscapes, buildings and interiors are used. The images file formats used PNG. Figure 5 and 6 show examples of the clean images and the hidden data.

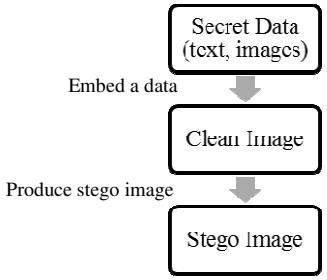

Figure 4. The process of creating stego images

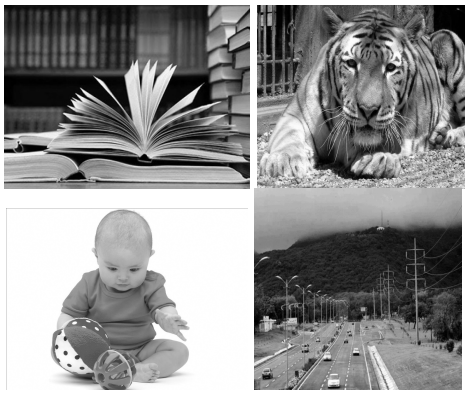

Figure 5. Example of the clean images

Figure 6. Example of hidden data

In the second stage , the focus on evaluating images set (stego and clean images) to detect hidden data by extracting a number of features from images and using fuzzy logic and neural network as AI techniques. Three cases are created based on the number of features as shown in Table 5.

Table 5. Three cases with different number of features

Case	**No. of Features**	**No. of Images**
Case 1	5 features	600 images
Case 2	30 features	600 images
Case 3	50 features	600 images

The proposed system for detection is depend on extracting a set of image features from stego and clean images and using fuzzy logic and neural network techniques to distinguish between clean an stego images. To train the proposed system to detect a hidden data in the images, it was set up a co-occurrence matrix for each image. Usefulness of this matrix is to provide valuable information about the neighboring pixels position in an image. From the created matrixes a number of features will be extracted. Different features will be selected for the three colour channels (Red, Green and Blue). These image features include correlation, contrast, colours variance, entropy and energy. Table 6 shows the five extracted features from clean image1 and its stego copy named stego image1.

The following are the steps of features extraction from images by using Matlab software :

- Using imread() function to read the image.
- Using graycomatrix() function to create co-occurrence matrix for the image.
- Using graycoprops() function to extract the correlation, homogeneity and entropy features from the created matrix.

Table 6. Values of the five features extracted from clean image1 and stego image1

Features name	Clean image 1	Stego image 1
Contrast	0.44698	0.44608
Correlation	0.91807	0.91823
Energy	0.11202	0.11208
Homogeneity	0.87812	0.87828
Entropy	7.56398	7.56370

For validation, the Fuzzy Logic (FL) is used to validate the results and the accuracies achieved by the system during the training and the testing phases. Takagi–Sugeno type of fuzzy inference method is used for this FL. The system divided the images into two sets. It used around 70% of the images for training and 30% for testing. The function xlsread() used to import the extracted features from Excel file and the function genfis2() is used to generate a fuzzy interface system.

The Multilayer Perceptron Neural Network (MLP) is also used to validate the results. The MLP were run 6 times for accuracy; the test automatically divided the images into two sets. It used around 70% of the images for training and 30% for testing. However, the MLP chose different images with each run for the training and the testing. Therefore, the results are not the same for each test.

7. DISCUSSION

As it known about fuzzy logic that it is more accurate methods of artificial intelligence techniques, successive tests have proved that the detection ratio of the clean images and the stego images increased respectively to the increased in the number of images and features.

We conclude that the fuzzy logic system achieved high overall accuracy during the testing phase for each case comparing to Multilayer Perceptron Neural Network. It is noticeable that in each test of MLP, the accuracy rate of detecting the stego images and the clean images was increased slowly relatively in each case than previous one, despite the increase in the number of features in each case as shown in figure 7. This reflects that the fuzzy logic system accomplished high performance in terms of classifying the clean and stego images.

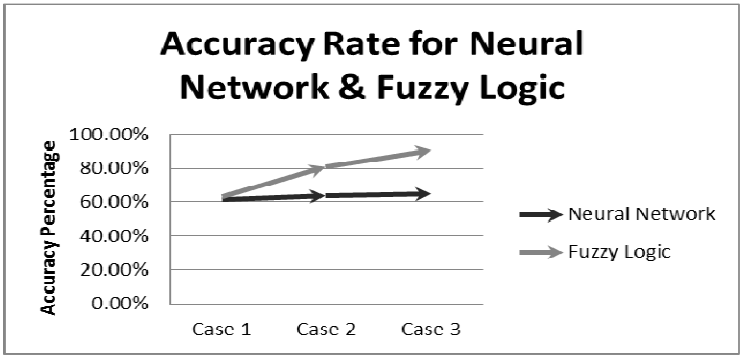

Figure 7. Accuracy rate of validation

8. FUTURE WORK

As it has been previously mentioned in this paper, genetic algorithm will be used as a third technique of AI to test the proposed system of detection. Genetic algorithm will be implemented

as a classifier to distinguish between stego and clean images. In addition, the accuracy of the genetic algorithm test will be compared to the results of fuzzy logic and neural network.

9. CONCLUSIONS

This paper presented a briefly review for the steganography and steganalysis definitions, categories, techniques and some related work. We concluded that the steganography field is developing rapidly and new methods and techniques are evolving to detect what is concealed by steganography techniques. One steganography technique is LSB steganography. The PNG image is the most suitable format for the LSB technique when the focus is on the amount of information to be sent. The PNG image has many capabilities which make it superior to other image formats and it requires further research.

There have been several attempts to incorporate artificial intelligence techniques in the steganalysis process. This combination is used to increase the accuracy and speed of detection.

The paper introduced the proposed detection system. OpenStego and Steganography Studio are the selected steganography tools to create the stego images. the proposed system depend on creating a co-occurrence matrix for images to extract set of image features. Fuzzy Logic (FL) and The Multilayer Perceptron Neural Network (MLP) used to validate these features. The fuzzy logic system achieved high overall accuracy.

ACKNOWLEDGEMENTS

I wish to express my sincere thanks to the supervisor Dr. Daniyal Alghazzawi, for supporting me and providing me with guidance and all the necessary facilities for the completion of this work.

REFERENCES

[1] P. Thiyagarajan, G. Aghila, and V. P. Venkatesan, "Steganalysis Using Color Model Conversion," arXiv preprint arXiv:1206.2914, 2012.
[2] R. Poornima and R. Iswarya, "An Overview of digital image Steganography," International Journal of Computer Science & Engineering Survey (IJCSES), vol. 4, pp. 23-31, 2013.
[3] S. Engle, "Current State of Steganography: Uses, Limits, & Implications," Retrieved March, vol. 12, p. 2012, 2003.
[4] S. A. Laskar and K. Hemachandran, "A Review on Image Steganalysis techniques for Attacking Steganography," in International Journal of Engineering Research and Technology, 2014.
[5] C. James, "Steganography Past, Present, Future," URL:http://www.sans.org/reaing_room/whitepapers/steganography/steganogaphy_past_present_future _552. pdf (12.12. 2009).
[6] B. Boehm, "StegExpose-A Tool for Detecting LSB Steganography," arXiv preprint arXiv:1410.6656, 2014.
[7] M. M. Amin, M. Salleh, S. Ibrahim, M. R. Katmin, and M. Shamsuddin, "Information hiding using steganography," in Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference on, 2003, pp. 21-25.
[8] R. Amirtharajan, V. Rajesh, P. Archana, and J. Rayappan, "Pixel indicates, standard deviates: A way for random image steganography," Res. J. Inform. Technol, vol. 5, pp. 383-392, 2013.
[9] G. Swain and S. K. Lenka, "Classification image steganography techniques in spatial domain: A study," Int J Comput Sci Eng Tech, vol. 5, pp. 219-32, 2014.
[10] S. Goel, A. Rana, and M. Kaur, "A Review of Comparison Techniques of Image Steganography," Global Journal of Computer Science and Technology, vol. 13, 2013.
[11] S. Azevedo, L. Gonçalves, and R. Rudson, Fuzzy Logic on a Polygenic Multi-Agent System for Steganalysis of Digital Images: INTECH Open Access Publisher, 2012.

[12] W. W. Zin, "Message Embedding In PNG File Using LSB Steganographic Technique," International Journal of Science and Research (IJSR) Volume, vol. 2, 2013.
[13] T. Qiao, F. Retraint, R. Cogranne, and C. Zitzmann, "Steganalysis of JSteg algorithm using hypothesis testing theory," EURASIP Journal on Information Security, vol. 2015, pp. 1-16, 2015.
[14] J. Fridrich and J. Kodovský, "Steganalysis of LSB replacement using parity-aware features," in Information Hiding, 2013, pp. 31-45.
[15] V. L. Reddy, A. Subramanyam, and P. C. Reddy, "Implementation of LSB steganography and its evaluation for various file formats," Int. J. Advanced Networking and Applications, vol. 2, pp. 868-872, 2011.
[16] H.-W. Tseng and H.-S. Leng, "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number," Journal of Applied Mathematics, vol. 2013, 2013.
[17] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters, vol. 24, pp. 1613-1626, 2003.
[18] M. H. Mohamed, N. M. Al-Aidroos, and M. A. Bamatraf, "Innovative Multi-Level Secure Steganographic Scheme based on Pixel Value Difference."
[19] D. Gupta and S. Choubey, "Discrete Wavelet Transform for Image Processing," International Journal of Emerging Technology and Advanced Engineering, vol. 4, pp. 598-602, 2015.
[20] R. an Amirtharajan and J. Rayappan, "Steganography—time to time: A review," Research Journal of Information Technology, vol. 5, pp. 58-66, 2013.
[21] A. Ibrahim, "Steganalysis in computer forensics," in Australian Digital Forensics Conference, 2007, p. 10.
[22] N. Meghanathan and L. Nayak, "Steganalysis algorithms for detecting the hidden information in image, audio and video cover media," international journal of Network Security & Its application (IJNSA), vol. 2, pp. 43-55, 2010.
[23] R. P. S. Sruthi Das N, "A Survey on Different Image Steganalysis Techniques," International Journal of Modern Trends in Engineering and Research vol. 02, p. 5, 2015.
[24] K. Curran and J. Mc Devitt, "Image analysis for online dynamic steganography detection," Computer and Information Science, vol. 1, p. p32, 2008.
[25] H. Wang and S. Wang, "Cyber warfare: steganography vs. steganalysis," Communications of the ACM, vol. 47, pp. 76-82, 2004.
[26] S. O. Mundhada and V. Shandilya, "Spatial and Transformation Domain Techniques for Image Enhancement," International Journal of Engineering Science and Innovative Technology (IJESIT), vol. 1, pp. 213-216, 2012.
[27] J. Green, I. Levstein, C. R. J. Boggs, and T. Fenger, "Steganography Analysis: Efficacy and Response-Time of Current Steganalysis Software," J Comput Sci, vol. 9, pp. 236-44, 2015.
[28] R. Kumar, K. K. Saini, and S. Chand, "A New Steganography Technique Using Snake Scan Ordering Strategy," International Journal of Image, Graphics and Signal Processing (IJIGSP), vol. 5, p. 25, 2013.
[29] R. Singh and G. Chawla, "A Review on Image Steganography," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, pp. 686-689, 2014.
[30] S. Mehta, A. Maru, and P. K. Goel, "A Survey Paper on Steganalysis F5 Algorithm."
[31] A. Brown, "Graphics File Formats," ed, 2008.
[32] S. M. Badr, G. Ismaial, and A. H. Khalil, "A Review on Steganalysis Techniques: From Image Format Point of View," International Journal of Computer Applications, vol. 102, 2014.
[33] T. Boutell, "PNG (Portable Network Graphics) Specification Version 1.0," 1997.
[34] M. Al Fahdi, N. Clarke, and S. Furnell, "Towards An Automated Forensic Examiner (AFE) Based Upon Criminal Profiling & Artificial Intelligence," 2013.
[35] A. Irons and H. S. Lallie, "Digital Forensics to Intelligent Forensics," Future Internet, vol. 6, pp. 584-596, 2014.
[36] R. Din and A. Samsudin, "Computational intelligence in steganalysis environment," 2008.
[37] A. I. Bouguerne, B. H. F. Merouani, and C. N. Kobsi, "Multi Resolution Decomposition For A Passive Steganalysis Based On a Multi Agent System."
[38] N. Kobsi and H. F. Merouani, "Neural Network Based Image Steganalysis: A Comparative Study," in Neural Networks for Signal Processing [1994] IV. Proceedings of the 1994 IEEE Workshop, 2007, pp. 423-430.
[39] I. Khan, "An Efficient Neural Network based Algorithm of Steganography for image," International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume, vol. 1, pp. 63-67.

[40] C. Bergman and J. Davidson, "An artificial neural network for wavelet steganalysis," Final Report to Midwest Forensics Resource Center, 2005.
[41] S. Bakhshandeh, J. R. Jamjah, and B. Z. Azami, "Blind Image Steganalysis based on local information and human visual system," in Signal Processing, Image Processing and Pattern Recognition, ed: Springer, 2009, pp. 201-208.
[42] X. Y. Yu and A. Wang, "An investigation of genetic algorithm on steganalysis techniques," in Intelligent Information Hiding and Multimedia Signal Processing, 2009. IIH-MSP'09. Fifth International Conference on, 2009, pp. 1118-1121.

INTENTIONAL BLANK