A NOVEL BIOMETRIC APPROACH FOR AUTHENTICATION IN PERVASIVE COMPUTING ENVIRONMENTS

Rachappa[1], Divyajyothi M G [2] and Dr. D H Rao[3]

[1]Research Scholar, Department of Computer Science, Jain University, Bangalore
[2] Research Scholar, Department of Computer Science, Jain University, Bangalore
[3]Professor and Dean, S.G. Balekundri Institute of Technology, Belgaum India

ABSTRACT

The paradigm of embedding computing devices in our surrounding environment has gained more interest in recent days. Along with contemporary technology comes challenges, the most important being the security and privacy aspect. Keeping the aspect of compactness and memory constraints of pervasive devices in mind, the biometric techniques proposed for identification should be robust and dynamic. In this work, we propose an emerging scheme that is based on few exclusive human traits and characteristics termed as ocular biometrics, promising utmost security and reliability. Complex iris recognition and retinal scanning algorithms have been discussed which promises achievement of accurate results. The performance and vast applications of these algorithms on pervasive computing devices is also addressed.

KEYWORDS

Pervasive computing, Biometrics, Privacy, Security, Iris recognition, Advanced computing, Authentication

1. INTRODUCTION

A lot of computing devices have already started assisting people in their day to day activities. Embedded sensors are already part of cars and home appliances and will soon find widespread application in the whole environment where all the surrounding objects will be smart to assist users each possessing computing capability [4] [5]. So it's time to envision a future where the devices can comprehend with the picture of the real and virtual world. Though right now most devices have simple functionality, with not much knowledge about the people with whom they are communicating and interacting, it is highly essential to make the pervasive setup "human aware", so that the identity of the user in the proximity of the computing device is known. The usage of traditional authentication methods may not be feasible for pervasive environments, and needs an erudite identity recognition technology which is more accurate and non-forgeable. The efficient use of biometrics can serve the purpose of such identification and verification due to their prodigious ability of providing security in many applications. Keeping in mind the significant limitations of the previously proposed biometric schemes available in literature such as spoofing, back end and input level attacks, hill climbing attacks, designing multimodal biometric systems is essential. [1] [6] [8]. The multimodal biometric systems should encompass innovative tools and methods that can deal with most of these attacks. In this work we discuss the technique of iris and retinal scanning as a promising model for authentication for a pervasive computing environment, keeping in mind the ease of use, cost effectiveness and computation speed. Although the usage of biometric identifiers in pervasive domain in the future for authentication is upbeat, it also gives rise to interesting research problems for inventing

DOI:10.5121/acii.2016.3202

appropriate innovative techniques and algorithms that can fit into various pervasive application realms.

1.1. Related Work

A periocular biometric iris recognition scheme based on analysis of iris texture was designed that takes into account the shape of eyelids and even skin wrinkles promising improved performance [13]. NSF and Texas state university have proposed a reliable, more secure biometric approach which is three layered and is highly reliable[9] [10] [11] [12].

Though these results are not being discussed or applied on pervasive computing devices, it would be interesting to learn about their performance and functioning on the same. Speech and facial biometric identifiers have been deployed by the Australian market in the latest range of LED's and Television by Panasonic Company [15].

2. OCULAR BIOMETRICS

Accurate user and service provider authentication is a must in pervasive computing environments. The combination of iris scanning and retinal scanning is termed as ocular biometrics. Here both iris and retinal scanning being highly accurate serves as a strong candidate for authentication [2] [7].

Ocular biometric systems provide accurate results when compared to uni-modal biometric identifier and can be robust against spoofing attacks because multiple biometric traits are hard to fake.

2.1. Structural Background

The complexity of ocular biometric identifiers lies in the complex eye structure of an individual which is unique in every person. Also the movement of the eye takes different states depending on various provocations. There can be stable eye balls, centred ones, rotating ones or a combination of all these. For pervasive deployment cost of equipment used and accurate biometric results are very important. Using low cost image sensors can serve the purpose.

2.2. Iris

Iris recognition technique is one of the main reasons for the wide application of ocular biometry. The Indian government's UIDAI program is capable of matching 10000 billion iris patterns daily [18]. The acquisition techniques for a pervasive environment can be through sensor technology. The first region of interest to capture iris data is the region surrounding the pupil for which an appropriate edge detection algorithm has to be applied after which template matching can be done.

2.3. Periocular

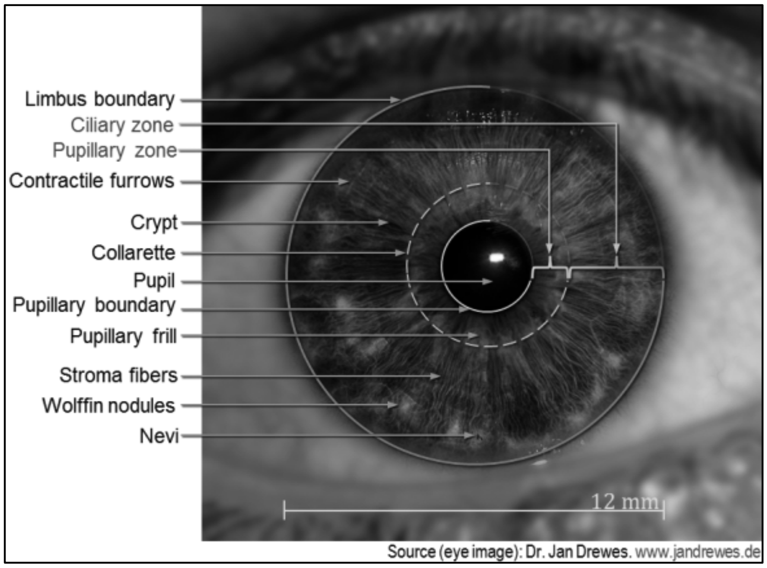
The portion of the face surrounding by the eyes is referred to as the periocular region. This can be used along with iris and retina to form a strong biometric identification trait, which in turn can form a basis to determine the age, gender, culture of various individuals.

2.4. Retina

Though a number of middleware solutions have been proposed for data, service management, owing to the wide heterogeneity of network resources involved in pervasive computing there are numerous coordination problems that exists in such computing environments. A secured single middleware solution is very much desirable in such environments.

3. IRIS RECOGNITION ALGORITHMS

The random structure of the iris can be absolutely reliable to determine a person's identity. Already it is being widely used in airports to authenticate / identify users. The iris patterns, as shown in the figure, have more uniqueness, randomness, come in different shapes and sizes, and can be a better contestant than face recognition or any other biometric identifiers.



Source (eye image): Dr. Jan Drewes. www.jandrewes.de

Figure 3.1: The Complex Iris Pattern

3.1. Daughman's Algorithm

The most widely used iris recognition algorithm [3]. The Daughman's Integro-Differential equation is as follows:

$$\max(r, x_o, y_o)\left|G_\sigma(r) * \frac{\partial}{\partial r}\oint_{r,x_o,y_o}\frac{I(x,y)}{2\pi r}ds\right|$$

Here, for each of the iris and pupil, r is the radius and (x_o,y_o) is the centre of the coarse circle. The algorithm is run twice, first to determine the iris contour followed by the pupil contour. The original image is given by I (x, y) and the Gaussian function is denoted by G_σ(r).

A number of studies have reported a zero failure rate on applying this algorithm for iris recognition. Given millions of possibilities, this algorithm can rightly determine an individual with a recognition rate of 98.4% [19] [20]. Thus iris recognition is considered to be a reliable biometric identifier in comparison with other technologies.

3.1.1 Enhanced Daughman's Algorithm

The algorithm mentioned above has a limitation that if there is maximum gradient received while scanning an image, then a bright spot can be mistaken. So the above equation needs to be modified. There needs to be a threshold value, beyond which all image pixels resulting in a circle has to be ignored.

3.1.2 Applicability in Pervasive Infrastructure

Owing to the complex iris structure and the fact that no two identical persons can have the same iris construction and due to its stable results for many years, Iris scanning techniques have many advantages to offer in comparison with many of the existing biometric identifiers.

Deployment in a pervasive domain demands optimum performance and it has been demonstrated that in less than 2 seconds a 2 GHz processor can compare around I million iris [17].

4. RETINAL SCANNING TECHNIQUES

Retina scanning based biometrics for identification and verification takes advantage of the complex structure of one's retinal blood vessel patterns which is unique for every individual. This technique is the least deployed as of now, as the retinal scanning algorithms work better with only high quality images.

Retinal patterns can be obtained by capturing a digital image of the eye while projecting an infrared light. This technique needs utmost cooperation from the subjects as they have to look at the lens in a specific alignment.

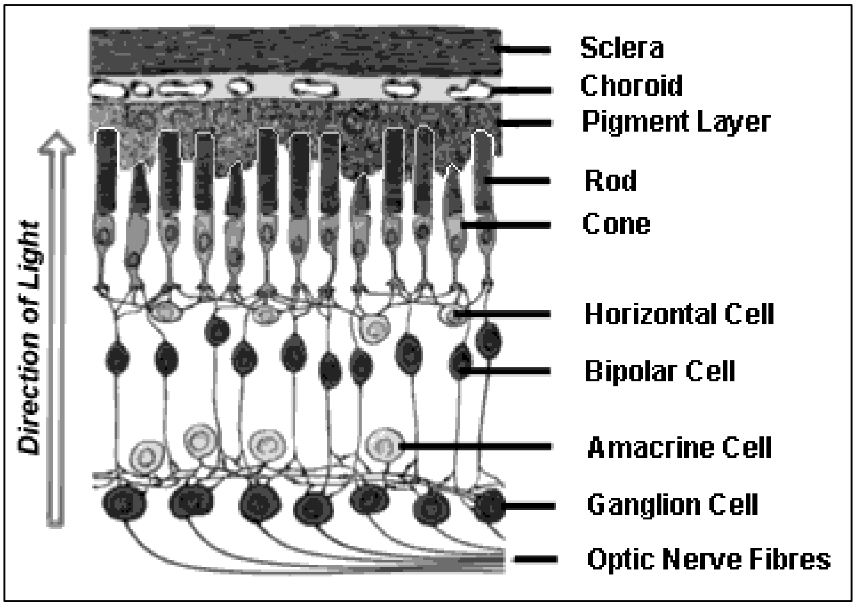


Figure 4.1: The Retina structure

4.1. Security Implications

Retina scan technology has a robust security implication due to its unique matching capabilities against a given identification database. The security of this technique comes from the fact that every individual has a unique retinal vasculature which is not possible to replicate.

The only constraint that applies here is the image quality. Retina scan identification algorithms work accurately only with high quality images.

4.2. Deployment in Pervasive Domain

Retina scanning devices can be embedded in the surrounding pervasive objects around the environment where a high degree of security, identification, verification and accountability is intended. Few areas to mention may be in governance and military management, Central Intelligence agencies, medical diagnostic examinations and chronic conditions, aeronautics and space applications, investigation agencies.

5. PERFORMANCE AND APPLICABILITY

For a pervasive environment and in its vast application, biometric authentication based on iris scanning followed by a retinal scanning can provide accurate results. Smart homes, PC webcam security systems, surveillance systems can make use of this authentication technique to identify users entering / leaving a house. The same applies to any computing device embedded with a camera and a scanning device. Military bases and nuclear reactors are already using retina scanners.

Due to the unique identifying traits, the performance of retinas scans is much more accurate than iris scans, and any other biometric identifiers [14]. In contrast, the refractive state of the eye and common corneal diseases does not affect iris scanning. But if there is a loss of corneal clarity, both the retinal and iris image results may vary radically.

In comparison with uni-modal biometric systems, future belongs to multimodal systems. They can improve the matching performance with their ability to integrate information at various levels. Several multimodal systems have been proposed by researchers. One such fusion model is shown in the figure. Here the feature extraction may differ based on the biometric trait one desires to capture. In the proposed paper, it is the iris and retina

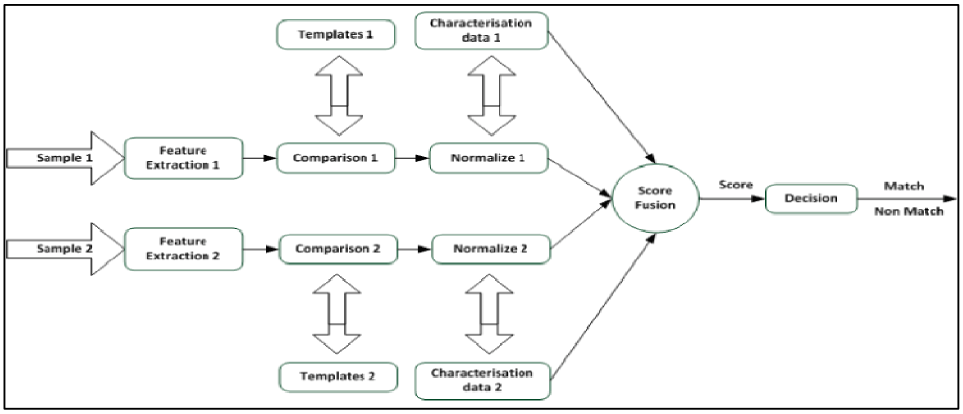


Figure 5.1: Example: Multimodal Fusion system [21]

6. CONCLUSION

In this paper we have discussed a multi-layer biometric authentication scheme that can be useful in authenticating users for varied pervasive computing applications. We have discussed in detail the iris and retina scanning techniques and algorithms and their performance issues. The statistics obtained from iris and retina scan can be consolidated to compute a new feature vector in a new hyperspace. This feature vector can perform best matching. Using this multi – modal scheme, each modal will generate a matching score which can be combined to sustain the claimed identity.

Ocular Biometrics is progressing rapidly [16], and promises acute security for various practical based applications. It facilitates several tools to carry out business transactions in a protected manner. The research effort continues from around the world to improve the efficacy and accuracy of this biometric domain. As the technology ripens further, one can expect increased user acceptance, applicability and credibility to the service providers.

With every innovative technology, comes a set of limitations. Careful system Design however can minimize these precincts. Every system must be designed with a cost-benefit analysis.

7. ACKNOWLEDGMENTS

We extend our thanks to our Prof. Dr. D. H. Rao for his discussions, time and ideas given during the course of our work.

8. REFERENCES

[1] Abdulmonam Omar Alaswad, "*Vulnerabilities of Biometric Authentication "Threats and Countermeasures*", International Journal of Information & Computation Technology. *ISSN 0974-2239 Volume 4, Number 10 (2014)*, pp. 947-958

[2] Prateek Verma, "*Daughman'S Algorithm Method For Iris Recognition-A Biometric Approach",* International Journal of Emerging Technology and Advanced Engineering, *Volume 2, Issue 6, June 2012.*

[3] Daugman, John G., PhD, "*How Iris Recognition Works*", IEEE Transactions on Circuits and Systems for Video Technology, *Vol. 14, No. 1, January 2004*, DOI 10.1109/TCSVT.2003.818350.

[4] Divyajyothi M G, Rachappa and Dr. D H Rao," *Techniques of Lattice Based Cryptography Studied On A Pervasive Computing Environment,"* International Journal on Computational Science & Applications (IJCSA), *Vol.5, No.4, August 2015.*

[5] Divyajyothi M G, Rachappa and Dr. D H Rao, “*A Scenario Based Approach for Dealing with Challenges in A Pervasive Computing Environment,”* International Journal on Computational Sciences & Applications (IJCSA), *Vol.4, No.2, April 2014.*

[6] David D. Zhang,” *Biometric Solutions: For Authentication in an E-World*”, Springer Science and Business.

[7] O. V. Komogortsev, A. Karpov. "*Automated Classification and Scoring of Smooth Pursuit Eye Movements in Presence of Fixations and Saccades*," Journal of Behavioral Research Methods, *v.45, 2013, p. 203*. doi:10.3758/s13428-012-0234-9

[8] O. V. Komogortsev, C. Holland, S. Jayarathna, A. Karpov. "*2D Linear Oculomotor Plant Mathematical Model: Verification and Biometric Applications*," ACM Transactions on Applied Perception, *v.10, 2013*. doi:10.1145/2536764.2536774

[9] Complex Eye Movement Pattern Biometrics: The Effects of Environment and Stimulus. "*Complex Eye Movement Pattern Biometrics: The Effects of Environment and Stimulus*," IEEE Transactions on Information Forensics and Security, *v.8, 2013, p. 2115*. doi:10.1109/TIFS.2013.2285884

[10] O. V. Komogortsev, A. Karpov, C. Holland.. "*Attack of Mechanical Replicas: Liveness Detection with Eye Movements*," IEEE Transactions on Information Forensics and Security, *v.10, 2015, p. 716*.

[11] O. V. Komogortsev, C. Holland, A. Karpov, L. R. Price. "*Biometrics via Oculomotor Plant Characteristics: Impact of Parameters in Oculomotor Plant Model*," ACM Transactions on Applied Perception, *v.11, 2014, p. 1*.

[12] I. Rigas and O. V. Komogortsev. "*Biometric Recognition via Probabilistic Spatial Projection of Eye Movement Trajectories in Dynamic Visual Environments*," IEEE Transactions on Information Forensics and Security, *v.9, 2014, p. 1743*.

[13] Proença H., “*Ocular biometrics by score-level fusion of disparate experts*”, IEEE Trans Image Process. 2014 Dec; *23(12):5082-93. doi: 10.1109/TIP.2014.2361285. Epub 2014 Oct 2*.

[14] Matthew Haughn, “*Retina Scan*” July 2014, Available at : http://whatis.techtarget.com/definition/retina-scan

[15] Steve Bell ,” *The invasion of biometrics”,* Security Expert at Bull Guard - Monday, *27 April 2015*, Available at : http://www.net-security.org/article.php?id=2260&p=1

[16] M. Vatsa, R. Singh, A. Noore, A. Ross, “*On the dynamic selection of biometric fusion algorithms*”, IEEE Transactions on Information Forensics and Security, *5 (3) (2010), pp. 470–479*

[17] Available : http://clinfowiki.org/wiki/index.php/Ocular_biometrics

[18] Unique Identification Authority of India, http://uidai.gov.in/

[19] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, S. McBride, “*A system for automated iris recognition”,* Proceedings IEEE Workshop on Applications of Computer Vision, *Sarasota, FL, pp. 121-128, 1994*

[20] S. Sanderson, J. Erbetta., “Authentication for secure environments based on iris scanning technology”, *IEE Colloquium on Visual Biometrics, 2000.*

[21] N. Celik[1*], N. Manivannan[1], W. Balachandran[1] and S. Kosunalp[2] “*Multimodal Biometrics for Robust Fusion Systems using Logic Gates”,* Biom Biostat 6:218, *doi: 10.4172/2155-6180.1000218*

Authors

Mr. Rachappa is currently working as Lecturer at the Department of Information Technology, Al Musanna College of Technology, Sultanate of Oman. His teaching interests include Computer Security, Pervasive Computing, E-Commerce, Computer Networks, Intrusion detection System, Network Security and Cryptography, Internet Protocols, Client Server Computing, Unix internals, Linux internal, Kernel Programming, Object Oriented Analysis and Design, Programming Languages, Operating Systems, Web Design and Development, etc. His most recent research focus is in the area of Security Challenges in Pervasive Computing. He received his Bachelor Degree in Computer Science from Gulbarga University, Master of Science Degree from Marathwada University and Master of Technology in Information Technology Degree from Punjabi University (GGSIIT). He has been associated as a Lecturer of the Department of Information Technology since 2006. He has worked as Lecturer at R.V. College of Engineering, Bangalore. He has guided many project thesis for UG/PG level. He is a Life member of CSI, ISTE.

Mrs DivyaJyothi M.G. is currently working as Lecturer at the Department of Information Technology, Al Musanna College of Technology, and Sultanate of Oman. Her teaching interests include Pervasive Computing, Firewalls and Internet Security Risks, E-Commerce, Computer Networks, Intrusion detection System, Network Security and Cryptography, Internet Protocols, Client Server Computing, Unix internals, Linux internal, Kernel Programming, Object Oriented Analysis and Design, Programming Languages, Operating Systems, Image Processing, Web Design and Development, etc. Her most recent research focus is in the area of Pervasive Computing. She received her Bachelor and Master Degree in Computer Science from Mangalore University, She bagged First Rank in Master's Degree at Mangalore University. She has been associated as a Lecturer of the Department of Information Technology since 2007. She has worked as Lecturer at ICFAI Tech., Bangalore, T John College for MCA, Bangalore, Alva's Education Foundation Mangalore. She has guided many project thesis for UG/PG level.

Dr. D H Rao is Currently working as Professor and Dean, S.G. Balekundri Institute of Technology, Belgaum. He has worked as a Dean, Faculty of Engineering, VTU, Belgaum. He was Principal at KLS Gogte Institute of Technology, Belgaum and Jain College of Engineering, Belgaum.

He is the Chairman, Board of Studies in E & C Engineering, VTU, Belgaum. He is a Member, Academic Senate, VTU Belgaum. He has over 100+ publications in reputed Journals and conferences. He obtained B.E. (in Electronics from B.M.S. College of Engineering), M.E. (from Madras University), M.S. (University of Saskatchewan, Canada) Ph.D. (Univ. of Saskatchewan, Canada).