INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

Retina based E-voting system using fuzzy logic and hamming distance

P. Abirami
abisathyadhoni95@gmail.com
Alagappa University, Karaikudi, Tamil Nadu

R. Anandha Jothi
ranandhajothi12@gmail.com
Alagappa University, Karaikudi, Tamil Nadu

Dr. V. Palanisamy
vpazhanisamy@yahoo.co.in
Alagappa University, Karaikudi, Tamil Nadu

ABSTRACT

Online E-Voting system is a convenient process to poll their votes easily for users. The online voting system is a very popular method but it has a lot of security issues. The major issue of this process is considered a user authentication and data storage. There are many secured passwords based securities are available in the last decades, but such kind of securities are not safe for user authentication it is easily hacked by the attackers. Hence, Biometric based E-voting system provide reliable security for the confidential E-voting system. The retina based E-voting has provided more reliable security for user authentication. In this work, the feature extraction process is done by the fuzzy logic and the matching process is done by the hamming distance and Manhattan distance to match frequent patterns in similarity measures between the retinal images and identifies detection probabilities in retina layers. Angular and radial partitioning techniques are used to detect the similarities of the blood vessels. This mechanism provides maximum security and achieves optimal results for the E-voting system.

Keywords: *Retina, E-Voting, Fuzzy systems, Blood vessels, Pattern, Manhattan points*

1. INTRODUCTION

Voting is a common process in all countries. It is an essential process for all countries. Hence the voting process implements high security, it is a major factor in this scheme and it changes everything in the voting process. In an Electronic Voting System, Voter availability is essential, but voter identification is the crucial part of this system. The online voting system leads to more advantage of voter because voter participates election in everywhere in the country, but some network security violations are the important factors in this system.

The conventional voting scheme is not a secure process and some irregular process is identified. It is a paper-based system, voter vote in a paper and collected on the ballot. If a voter is not voted correctly, there is no identification scheme is available and that vote is eliminated. This voting process has no security for voter identification because it is a human-based process and there is no electronically identification. Online voting scheme reduces these drawbacks from the conventional voting scheme. E-voting gives high security and reduces paperwork process.

The Biometric voting system is an online voting system that is implemented in elections and online surveys [12, 13]. It is highly secure and easily finds out results and voting process is on everywhere. Because the user implements a voting process electronically with biometric security. Biometric is a process of human-computer interaction with the identification of human biological identities, such as fingerprint, iris, and retina based identity. Biometric systems try to exchange Knowledge with features of an individual, such as an individual person's identity. These systems are implemented in low cost and implementation work is very less. Performance-wise implementation is very high in this system.

Biometric system limits the voting process in a certain time. Voters implement their vote in a specific period of time if the timer expires then it will log out. Voter confirmation process is in the biometric process. Voter's biological identity is already stored in the server. It will be matched to the voting process. After the successful match voter implements their voting process in online. The voting mechanism is always a private one that is each user vote is a secure one from others and it is not collapsed to another vote in databases. After completing the voting process, the system is logged out and logged in for the next voter.

Biometric secure e-voting system is implemented in characteristics of biological behaviors and converted into digital data. Comparing digital data to check details in the voting process is implemented by means of biometric reference data. Each user data are kept secret. And it is too difficult to share biometric identifiers because of identifiers and scanner devices. These problems are considered in a secure e-voting system.

In this work, we present a Retina-based biometric e-voting system and analyzes security issues in this system [1, 3, and 4]. This work implements the fuzzy logic matching process in retina future extraction. Hamming and Manhattan distances are identified to match frequent patterns in retina future samples.

© 2018, www.IJARIIT.com All Rights Reserved

2. RELATED WORK

Research work implements a skew tent map based symmetrical approach to encrypt the image. It uses the line map-based approach because it is applicable for any size of the image for the encryption. R, G, B components are encrypted at bit level and operation are performed at the same time to disturb the correlations. It does not need any sub-block complex processing so it can be implemented parallel. It is more secure.

Wang et.al discussed an improved gravity model and chaotic system based image encryption technique. First of all two chaotic sequences are generated based on the logistic map to shuffle the original image. After that, using an improved gravity model this shuffled image is di used. Finally to enhance the encrypted image with the help of changing one pixel on the plain image, chaotic system again di used.

Yushu et.al discussed a novel cryptosystem by a combination of time-varying delay and coupled map lattices. This approach basically overcomes the drawbacks in the previous methods based on the permutation diffusion architecture because the addition of pixel values of the original image basically used for the determination of the parameters of permutations and on the other hand cipher image used previously can be utilized in case of diffusion for the next time. So it is more efficient, reliable, practical and secured communication.

Security is the important factor in biometric identity. Fingerprints are one among them [6,7]. It has the unique one from another finger and it is considered as a human identity. But which finger has to be selected is the main process and matching accuracy depends on fingerprints. Face recognition is another human identity in the biometric process. Human images are stored in the database and it is matched to the camera detected image. Iris-based identity is another biometric identity based on the human eye iris. Retina based identity is also a unique human future that is identified in Retina scanner.

William Wee analyzed retinal blood vessels and classified into three categories: the edge detection based, the segmentation based and the probing-based. The Edge detection method identifies edge points between retinal images. Segmentation method focuses single threshold to segments of a retinal image into the background and the vessel. The probing-based methods utilize a profile model to incrementally step forward along the inspected vessel and identify the vessel boundary during probing.

3. SECURITY MEASURES IN E-VOTING

Nowadays, E-voting System implements stronger security properties and this system implements the latest security technologies such as encryption/decryption algorithms. It is a more advanced methodology of the traditional voting system. Cryptographic techniques are the major security implementation in the e-voting system. To implement security of the E-voting system, the following security factors implement security.

A. Transparency

An E-voting system should be in transparent that is all process are in the system is an open system.

B. User trustability

E-voting system considers as central admin that implement the verification process.

C. Reliability

This system works for a specific period of time without affect hardware failures.

D. Mobility

This system is the online voting system that the election process is conducted in any location without any extra-work implementation.

E. Robustness

This system works on a different system if errors are obtained and recovered without affect continuity.

F. Fault-Tolerant

This system works on erroneous data and identifies whether data is right or wrong.

G. Scalability

This system adopts security features when data rising and it does not affect other security features with the central voting scheme.

4. RETINA SECURITY IN E-VOTING

Retina based E-voting security system provides high security in an E-voting system that mainly focuses on human identity and avoids malpractices. This provides a unique security feature keeps on electronically in central administrator and control security policies.

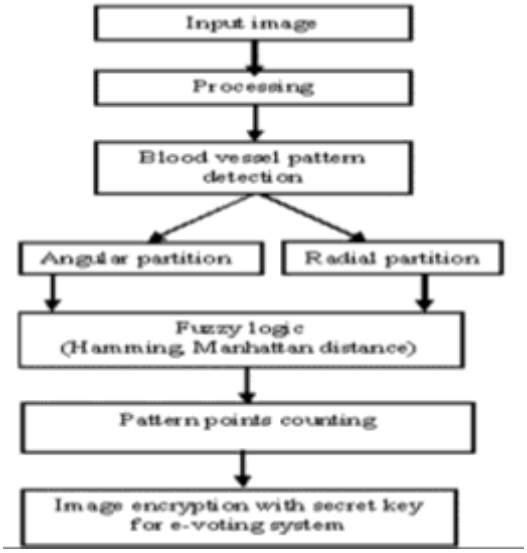


Fig. 1: Retina based E-voting feature extraction

The retina is a part of the human eye and unique one of human beings. It is changed very rarely throughout human life. This biometric identification system implements highly stable because blood vessels on Retina is a fixed one and cannot be changed throughout human life. In this method, the retina is implemented in recent trends.

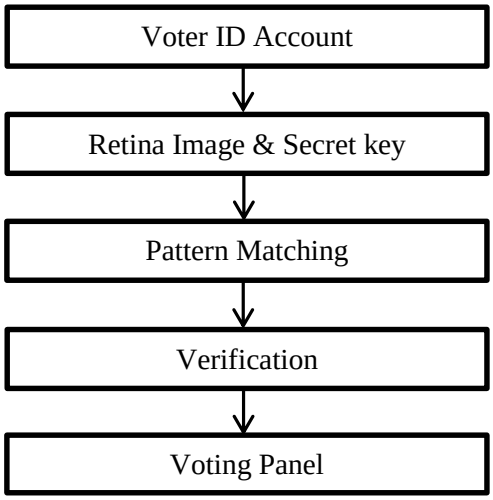


Fig. 2: Retina based E-voting system

© 2018, www.IJARIIT.com All Rights Reserved

Recent studies focus on Retina based identification but convert as image identification. Various technologies are implemented in Biometric security methods, but identifying process is so difficult in each method. Image-based retina detection affects various properties of Retina that image color schemes are categorized and patterned then matching Retina. The following diagram illustrates the retina based e-voting system process.

Human retina's blood vessels do not change throughout human life. It may change rarely because of any issues in human beings like operation in the eye. The retina is not changed by physical properties such as daily work activities, but fingerprint may change in routine activities. Retina has not directly identified by people that prevent malicious activities and detection process is highly accurate. The Retina based identification system in e-voting measures two types, one is user's retina images are stored already and perform the matching process and another one matching retina through retina scanner. It implements a faster identification process.

There are some limitations in retina based identification. Sometimes this identification process has not efficient one because human diseases such as eye diseases affect the retina. At that time the retina scanning process may not accurately and gives some false detection. The age factor is also affecting the retina because aged people may have a lot of diseases such as sugar, pressure, etc. these diseases affect retina patterns and may be inaccurate.

5. SECURE MODEL IN RETINA SCAN

The user positions his eye close to the unit's embedded lens, with the eye socket resting on the site. In order to a retinal representation to be acquired, the consumer must gaze straight into the lens and remain still, movement defeats the attainment process requiring another attempt. Retina Scan implements eye retina in a circular area in blood vessel pattern. It is reduced in 192 suggestion points before distilled into a digitalized 96-byte format and store in memory for verification purpose. It takes 3 to 5 images to ensure.

Retinal enlargement begins with the establishment of the eye fields mediate by Shh and Six3 with succeeding progress of the optic vesicles via Pax6 and Lhx2. The main uniqueness Pax6 was created Walter Gehring, showed the ectopic appearance of Pax6 can lead to eye development on Drosophila antennae, wings, and legs.

The retina has three structures: the neural retina, the retinal pigmented epithelium, and the optic stalk. First one has retinal progenitor cells (RPCs) that isolates retina cells from the other one. The individual difference starts with the retinal ganglion cells and concludes with the production of the Muller glia. It is reduced in 192 suggestion points before distilled into a digitalized 96-byte format and store in memory.

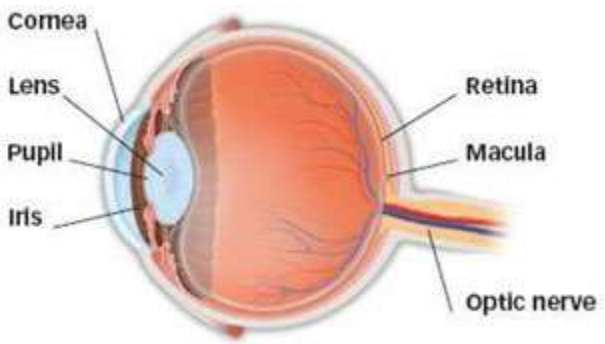


Fig. 3: Retina in Human Eye

The cues that determine an RPC daughter cell fate are coded by multiple transcription factor families, including the BHLH and home domain factors A retinal scanner uses infrared light for mapping. User views in retina scanner, then the retina circular path can be captured by using an invisible beam of low-energy infrared light. IR light captures the surrounding tissues in the retina circular path. Because of this, there is a variation in the intensity of the reflection. Retina scanner identifies various points in a retina circular path along with 320 points. It then assigns an intensity grade between zero and 4,095. The resultant statistics are compressed into an 80-byte computer code. This code can then be compared with patterns that have already been entered into the computer's database.

The deepest layers in the retina are located nearest the vitreous chamber, whereas the outermost layers are located adjacent to the retinal pigment epithelium and choroid. The most significant layers, succeeding from the outer to inner layers, are:

- The **retinal pigment epithelium**, which provides critical metabolic and supportive functions to the photoreceptors;
- The **receptor layer**, which contains the light-sensitive outer segments of the photoreceptors;
- The **outer nuclear layer**, which contains the photoreceptor cell bodies;
- The **outer plexiform layer**, where the photoreceptor, horizontal and bipolar cells synapse;
- The **inner nuclear layer**, which contains the horizontal, bipolar and amacrine cell bodies;
- The **inner plexiform layer**, where the bipolar, amacrine and retinal ganglion cells synapse;
- The **retinal ganglion cell layer**, which contains the retinal ganglion cell bodies; and
- The **optic nerve layer**, which contains the ganglion cell axons traveling to the optic disc.

Some of IR beam implements eye cornea, and various light beam passes in the retina globular pathway by reaching the light-sensitive portion of the photoreceptor; the outer segment in the receptor layer. Become aware of also in the region of the fovea wherever the image of the central visual field center is focused, the retina consists of fewer layers: thereby minimize the obstacles to forming a clear image on the fovea.

The optic disc is shaped by the retinal lump cell axons that are exiting the retina. It is located nasal to the fovea accordingly, it is the structural basis for the 'blind spot" in the image field.

According to the retina image in the pixel section, a particular pixel section X_i will be 1 for the following

$$i = (j+ V) \bmod K \text{ for } j, V = 0,1,2,\ldots k-1 \quad (1)$$

A number of edges pixels in each partition consider as a future. When the considered image rotates to 2μ/K radians, then its corresponding future vector shifts circularly.

Comparison of retina records includes calculation of a Hamming Distance (HD) that measures the detection probability where each scan absorbs and matches retina layers, as a measure of variation between the retina records recorded from the presented iris and each Retina Code recorded in the databases. Let Aj and Bj be two retina codes to be compared, the Hamming distance function can be calculated as:

$$HD= 1/E_j \sum (A_j \Theta B_j) \quad (2)$$

Denoting Exclusive - OR operator. (The exclusive-OR is a Boolean operator that equals one if and only if the two bits A_j and B_j are different).

© 2018, www.IJARIIT.com All Rights Reserved

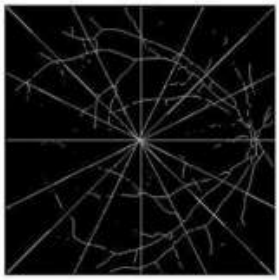
6. RESULTS AND DISCUSSION

This system describes the retina based security system in E-voting with high performance from the practical point of view. These techniques are:

- A method of evaluating the quality of an image in the image acquisition step and excluding it from the subsequent processing if it is not appropriate. Retina based details are stored in the database.
- Matching process based on Hamming distance function between the input code and the registered iris codes. The system out the recognition rate is about 92%.
- The following image identifies the retinal blood vessel detection in human eye.

After future extraction retinal pattern is analyzed and discovered using fuzzy logic distance identification

Angular partitioning process is implemented in this retinal pattern. In each pattern, Manhattan distance between two layers is identified. Using this distance detection probability between layers is also identified.



The following table illustrates the matching process detection probability with maximum probability.

Table 1: Comparative analysis

S. No.	Detection Probability count	Max Value Probability	Processing Time	Accuracy
1.	8	7	0.6232	89%
2.	5	5	0.4861	91%
3.	6	5	0.5391	93%
4.	3	4	0.3172	90%
5.	2	3	0.2817	91%

Retina based E-voting security system provides high security in large-scale systems because of its uniqueness. Retina blood vessels do not change in human beings that are effetely digitized in this security system. Its only drawback is retina scanners are expensive.

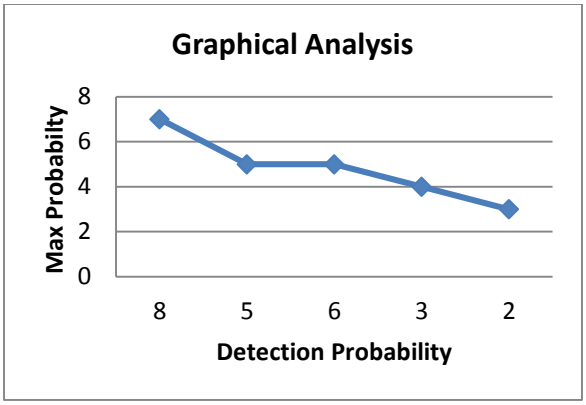


Fig. 4: Graphical analysis

This work analyses the Retina-based biometric e-voting system. And compares other biometric security features like fingerprint reorganization and iris reorganization. Both methods have some drawbacks compared to Retina security. The proposed work implements retina matching process in the e-voting system and analyses security features such as accuracy and efficiency.

7. CONCLUSIONS

The research work that is undertaken by me under the guidance of my supervisor/guide was aimed to develop complex biomedical biometric image processing algorithms for the recognition of human beings through the RETINA part of the human eye. This paper focuses on the retina based biometric security scheme and compares this scheme to other security mechanisms like Fingerprint security and online voting. In the research work consider a sincere attempt is ready to develop a simple and efficient method for retina recognition using hamming distance and Manhattan distance Algorithm by developing a GUI system for the retina Based Voting Machine integrated with RETINA recognition concept.

8. ACKNOWLEDGMENTS

This work was supported by the Department of Science and Technology- Promotion of University Research and Scientific Excellence (DST-PURSE)under the project number Phase-II /10815/2017. This support is gratefully acknowledged.

9. REFERENCES

[1] Namita Tiwari and Dr.Madhu Shandilya, "Evaluation of Various LSB based Methods of Image Steganography", International Journal of Computer Applications Volume 6– No.2, September 2010.

[2] Hanan Mahmoud Hanan Saad Al-Hulaibah Sarah Ahmad Al-Naeem Suha, "Novel Technique for Steganography in Fingerprints Images: Design and Implementation" Sixth International Conference on Information Assurance and Security 2010.

[3] Sanjay Saini and Dr. Joydip Dhar, "An eavesdropping proof secure online voting model" International Conference on Computer Science and Software Engineering 2008.

[4] E.S. Shameem Sulthana and Dr. S.Kanmani, "Evidence-based Access Control over Web Services using Multi Security International Journal of Computer Applications March 2011.

[5] Alok Kumar Vishwakarma1 and Atul Kumar "A Novel Approach for Secure Mobile-Voting using Biometrics in Conjunction with Elliptic Curve Crypto-Stegano Scheme" International Journal of Technology and Engineering Systems, March 2011.

© 2018, www.IJARIIT.com All Rights Reserved

[6] R. Anandha Jothi, V. Palanisamy, "Performance Enhancement of Minutiae Extraction Using Frequency and Spatial Domain Filters" International Journal of Pure and Applied Mathematics Vol no-118 issue-7 page no-647-654 ISSN No-1314-3395.

[7] R.Ananadha Jothi and V.Palanisamy, "Analysis of Fingerprint Minutiae Extraction and Matching an Algorithm " International Journal of Advanced Research Trends in Engineering and Technology (IJARTET) Vol. 3, Special Issue 20, April 2016, PP: 398-410.

[8] Nabin Ghoshal, J. K. Mandal "A Steganographic Scheme for Colour Image Authentication (SSCIA)" IEEE-International Conference on Recent Trends in Information Technology, June 3-5, 2011.

[9] Masoud Afrakhteh and Subariah Ibrahim "Enhanced Least Significant Bit Scheme Robust Against ChiSquared Attack" Fourth Asia International Conference on Mathematical/Analytical Modeling and Computer Simulation 2010.

[10] Okediran O. O., Omidiora E. O. Olabiyisi S. O., Ganiyu R. A. and Alo O. O. (2011), A Framework for a Multifaceted Electronic Voting System, International Journal of Applied Science and Technology Vol. 1(4), pp 135 – 142.

[11] Howard, M. (2001) E-Government across the globe: How will "e" change government? Government Finance Review, Vol. 17(4), pp. 6-9.

[12] Olaniyi, O.M, O.T Arulogun, E.O, Omidiora, A Omotoso, Ogungbemi O.B. (2012), Design of A Secured Model For Electronic Voting System Using Stegano Cryptographic Approach , Proceedings of the 7th International Conference on ICT Applications, Application of ICT to Teaching, Research, and Administration (AICTTRA 2012), National Defense College Abuja, pp 84-89

[13] Linu P, and Anilkumar M. N. (2012), ―Authentication for Online Voting Using Steganography and Biometrics‖, International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) Vol. 5(10), pp. 26-32.

[14] Shafi'í, M, Adebayo, O. S, Damian, O., Mohammed, D. (2013). "The Design and Development of Real-Time EVoting System in Nigeria with Emphasis on Security and Result Veracity, International Journal of Network and Computer Security. MECS (http://www.mecs-press.org/) Vol. 5, pp 9-18

[15] Enokela, J. A. (2010), ―Security of Programs and Data for an Electronic Voting System, Pacific Journal of Science and Technology, Vol. 11(2), pp. 283-287.

[16] Gunjal B., and Mali S, (2013). ―Secure e-voting system with Biometric and Wavelet-Based Watermarking Technique in Ycgcb color space. IEEE International Conference on Information Technology, pp 1-6.

[17] Sable, S. and Bombale U. L. (2014), "Cryptography Based Secured E-voting System Using ARM for Cell Phone and Internet Application"

BIOGRAPHY

P. Abirami
M. Phil.
Department of Computer Applications
Alagappa University, Karaikudi, Tamil Nadu

R. Anandha Jothi
Ph.D. in Biometrics
Department of Computer Applications
Alagappa University, Karaikudi, Tamil Nadu

Dr. Palanisamy Vellaiyan
Professor and Head of the Department
Department of Computer Applications
Alagappa University, Karaikudi, Tamil Nadu

© 2018, www.IJARIIT.com All Rights Reserved