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 authentication for E-voting system using MD5 algorithm

R. Suganya
suganyaraju2793@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

The electronic voting system is the easiest way for the election process. The E-Voting System is a digital electronic system. In this process, the user's data are collected in a digital manner. The stored data should be protected from unauthorized persons. The major issues of this process are the protection of stored data. The data security is considered as an important factor in an online voting system. Hence, the stored templates should be needed to prevent unauthorized users. In this work, explores unique retina features in a single can be existing in a binary format which can be quickly matched with the stored template to authorize identity. As biometric template are deposited in the database, owing to security threats biometric template may be altered by unauthorized persons. If the biometric template is altered authorized user will not be allowed to access the source. A box counting algorithms used to extract retina blood vessels from retina image. It analyzes and presents a high-level security and better image encryption using an MD5 algorithm which is implemented on high descriptor value in an image. The matching process is done by using a tree data structure. The experimental results show high accuracy for the matching process when applying more images and achieve optimal results in secure online E-voting system.

Keywords— *Image encryption, Blood vessels, Retina, MD5, Box counting algorithm*

1. INTRODUCTION

The Election process is a central administrative work in every country. It has a variety of processes implemented and all are human work. Now days voting process is converted in electronically and implemented in the various computerized work. This reduces normal paperwork and increases time.

E-voting is a computerized voting system implemented in both the on-line process an offline process. Each voter registers his details with a unique ID and stored in the database. Normally, all computers connected with LAN or internet. Whenever the voting process implements, voter details are retrieved and verified. This process implemented in several stages. Major stages are voter details collection, voter details matching with high security, voting tabulation with central administration.

Voter identification is the crucial factor in E-voting system. This process is implemented in two stages. One is data security and another one is human identity. Data security is implemented by a variety of encryption/ decryption algorithms and human identity is implemented in human biological features.

Data security focuses voter details with a unique ID. These details are encrypted and stored securely. Simply it is converted into digital format because the voter details matching process is a simple one when accessing digital data. The counting process is automated and secured in this system. Varieties of encryption and decryption algorithms are implemented in this process.

Human identity is also an important factor in E-voting system because some security violations detected in this system such as human malpractices. Biometric security features are implemented in this system such as fingerprint recognition, iris recognition, retina based recognition. This paper focuses data security in human identities, such as retina based e-voting system and analyses accuracy and efficiency in this system.

2. RELATED WORK

Security is the major factor of the e-voting process. The main focus of this E-Voting system is security and privacy and it can be time-consuming and very hard for election committee administrators. Finally, it is difficult to handle voters.

User privacy achieves greater security in e-voting. It brings the clarity of this voting system. This system satisfies the factors such as Requirement: each voter has only one voting account and allowed at one time, Privacy: voter's votes are private and secure one and no alternative process. It is useful for voting calculations. The voter simply puts their votes and no other actions implemented. Any public sectors can verify this voting process in an effective manner. Researchers improve the security in this system by implementing security algorithms and achieve greater results. Researchers improve a normal voting system to reduce paper works and automate computerized implementation. But accuracy and scalability are the important factors in e-voting system. Security attacks are also the major issues in this voting system.

Security is implemented in hardware, software, and data. Hardware security is physical system properties such as computers connected to LAN, and operating system performance. Software security is the e-voting system application security, this leads to prevent unauthorized access to this system. Data security is the user data privacy that data is stored in an encrypted form and no one access without permission. All these three security systems achieve greater results in the e-voting system. Security policies are also implemented in the e-voting system. That is, each voter has a unique id implementation and some essential details are included in this system. Then each voter has only one vote and no other way to put a vote in alternative methods. These policies bring greater security and most of the security violations are reduced in this system.

A Cat map named block Cat map is also considered for permutation development based on multiple-dimensional chaotic maps to create the large key space. The encrypted algorithm is basically based on the permutation substitution. Different chaotic maps are used to control each key. There are different types of analysis, i.e. cipher sensibility analysis, weak-key analysis, statistical analysis, entropy analysis, differential analysis, cipher random analysis to test the security of the new image encryption scheme. This image encryption technique basically provides the solution for higher security and higher speed as well as lower precision for one-dimensional chaotic function.

The Double encryption approach has basically three chaotic random sequences are generated with the help of the Chen system. First of all scrambling of widening image which having two plaintext images take place. After that, it is separated into two new provisional images. After this with the help of third sequence, i.e. modulated by a random phase key generated on the logistic map, one interim image is converted to the private phase key. With the help of this private key, second interim image basically converted to the ciphertext with white noise distribution. In the amplitude-phase retrieval process which is based on this private phase key[19,20], another interim image is converted into the ciphertext with the white noise distribution.

But security policies are changing in different voting systems. It depends on central administration election process in all countries. Some major policies are common in all voting systems. This paper analysis, a policy that brings security in retina based e-voting system.

Access control provides greater security in the system and implemented in certain resources. This limits the user, who has authorized a user or unauthorized user and checks the policy violations. Unique identification is implemented in access control. But it is not secure if the credential is missing or transferred.

Various securities related studies based on the image pre-processing methods for improving the image quality, authentication and identification [21, 22]

3. RETINA SECURITY METHOD IN E-VOTING

Retina security technology implements human eye retina and implements blood vessel patterns in the eye. The main process of this security system is implemented in the structure of the retina and blood vessels are individual one from others. This unique future is the human identifier in the voting system. New technologies such as IR technology [16,17,18] absorbed blood vessels in the retina. Blood vessel scanning technology is faster than other technologies. Retina security technology is used in high-security environments such as Military environments. In the 1980's more number of Retina technologies [3,10] was introduced such 35 new technologies were implemented.

A. Electronic Voting Machines

Electronic voting machines are the devices that reduce paper-based voting system. It is an embedded kit contains the voting unit and the control unit. Voters put their vote in the voting unit and it has predefined voting facilities. The control unit is accessed by the administrator. The voting unit has different buttons and each button refers to a candidate with symbols.

B. Internet Voting

Internet voting is implemented in the rural areas such as computer-implemented an Internet-enabled areas and implemented the election process. To elect officers with Board members, Business enterprises and organizations makes use of Internet voting and for the other proxy elections. Privately Internet voting systems have been used in many modern nations.

C. Hash Functions

Hashes are implemented in a voting system that is used in user data and convert data in a different format by using mathematical functions. This process is used to identify malicious modifications to the software or when software is corrupted or when incorrect versions are about being installed.

D. Digital Signatures

Digital signatures are implemented in the e-voting system and use hash functions to convert data into signatures. Signatures are helping to identify data when transferring electronically in this system. Digital signatures [11,12,13] are not analogous to physical hand wrote signatures as they provide the unique identity of whom signed a message in elections, impressions are used to sign the contents of the voting process to ensure that this system is not changed.

4. THE PROCESS OF SECURE E-VOTING

The proposed work implements Retina based image encryption and implements a matching process in E-voting system. This process generates high security in E-voting. The following diagram illustrates the retina based e-voting system process.

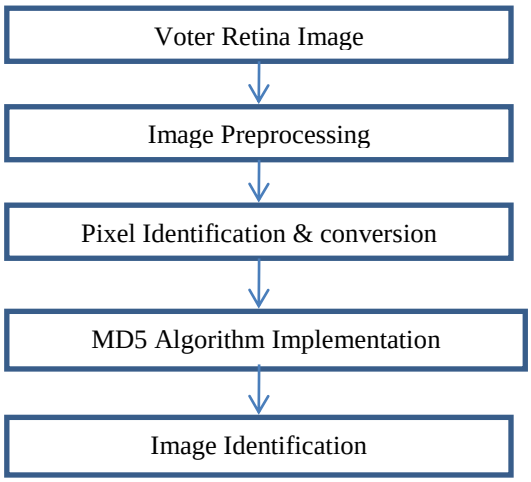

Fig. 1: Retina identification model

In Retina based scanning process, the retina vascular tree structure is uniquely one. Using this feature, the biometric identification process is a more secure one. The proposed work identifies these tree structures based on retina image and it is taken from RGB retinal image and achieved by using green

channel information, which the 10% smallest magnitude curvelet coefficients were set to zero. This step is followed by an inverse curvelet transform which results in an enhanced image from which an estimate of the vascular tree is obtained using the segmentation procedure.

However, in the proposed approach the image is initially divided into NxN sub-regions and the method explained previously is applied to each image sub-region. In this way, a Fractal Dimension value is computed for each image sub-region. Besides the Fractal Dimension computation for each image sub-region, five other similar values are computed for five images obtained from the original image as will be described shortly.

These five image measures the regularity, roughness and direction details of the original image and the values of the Fractal Dimension of each sub-region of the original image together with the corresponding Fractal Dimensions of these five images, henceforth designated by fractal descriptors, are highly specific to each vascular tree, thus making them useful for recognition tasks. The number of these six-dimensional descriptors per image depends on the image partitioning degree. When choosing a smaller image sub-regions more sub-regions are obtained and consequently more descriptors for each image are obtained as well. The choice of the right sub-region size to use is an important issue which is analyzed in the Results section, where we investigate the effect of this parameter on the performance of the method.

Since some image sub-regions do not have any positive pixel value (no detected vessels in the sub-region), their corresponding Fractal Dimension descriptor will be a null vector, not contributing to the patient images recognition. It was found that better image retrieval performance results were obtained by performing an initial clustering with only two child nodes (k=2). One of the children node clusters not only all the null descriptor vectors but also the ones with very small Fractal Dimension values (which are corresponding to image sub-regions with little retinal vascular tree information). The null descriptor vectors cluster is not considered in the following clustering iterations nor in the search step.

5. Algorithm Implementation

Message Digest 5 algorithm is an easiest cryptographic algorithm for large file encryption process. This algorithm implements the hash function [10,14,15].The hash value is normally 128-bit size. The digital signature creation process is implemented with this algorithm.

Four rounds are implemented in this algorithm and each round carries the permutation process of used data with has a function. The result of each round repeated in the next round with a hash function. MD5 is considered one of the most efficient algorithms currently available.

Table 1: Comparative analysis

Type	Sub-regions	Fr. Descriptor Value	Conversion Ratio
Image 1	3	45	72%
Image 2	5	70	81%
Image 3	4	52	78%
Image 4	5	68	80%
Image 5	6	81	90%

Processing Steps

1. Get a Retina image for a user
2. Convert it in RGB image in image preprocessing
3. Image sub-regions are generated with pixel values
4. Repeat the above process in multiple relevant pictures from the same user
5. Applying fractional dimension in sub-regions
6. Based on fractional values, get one image
7. Apply MD5 algorithm in the image with key

Moreover, some fractional values appear in almost all images, while others are very rare, not contributing to correct image retrieval. Due to this, lists of all possible descriptor vectors were organized and their occurrences in image list were counted.

6. Result and Discussion

The model is implemented on a PC with a Pentium Dual-Core processor running Microsoft Windows XP. All the algorithms are implemented in Java. The topic repository uses the PHP when directory and the data is stored in MYSQL open Server. Initially, the image sub-region size was evaluated in terms of enabling the construction of sufficiently large datasets with which a reduced amount of images could be selected as belonging to the same user of the query image. In this system, almost two or three retina image samples are implemented for every user.

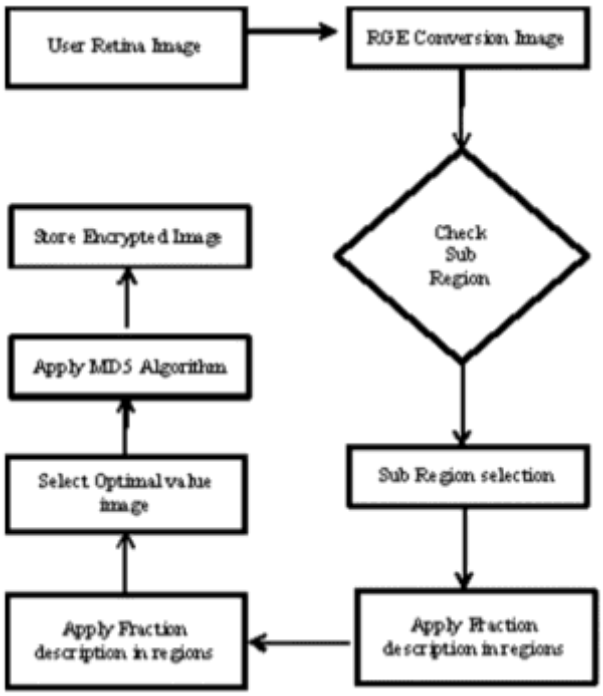

Fig. 2: Process flow model

The MD5 algorithm is implemented in a hash function and accessing a large amount of data. Different hashing algorithms produce a different hash value, but cannot re-create the original data from the hash.

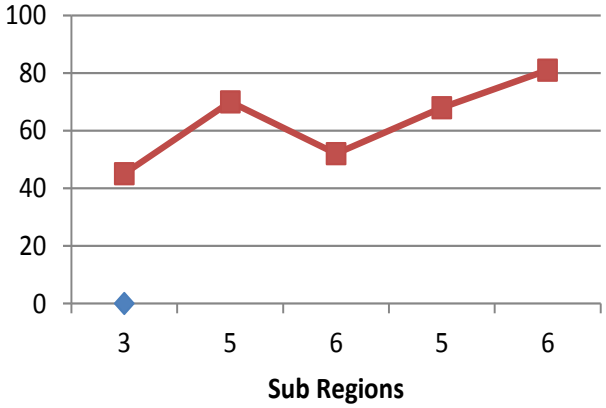

Fig. 3: Graphical Analysis

The conventional image encryption method combines phase shifting process in digital hologram implementations. Retina images are encrypted in quadrature phase shifting encryption and then compressed in the reduced size image. This process implements easy reconstruction of images.

7. Conclusion

The E-Voting System is a digital electronic system that user data are collected in a digital manner and processed securely. Security is the important factor in this system. This paper focuses a survey for security methodologies in E-voting systems and mainly focuses on retina security mechanisms and implemented MD5 security algorithms. Retina security is the most important identification checking mechanism insecurity. Various retina images are identified and generated sub-regions to get optimal fractional descriptor values. Using these values an image is selected and converted to an encrypted image using the MD5 algorithm. This method has greater flexibility as compared with other security methodologies.

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] Jain, R. Bolle, S. Pankanti Eds, "BIOMETRIC - Personal Identification in Networked Society", Kluwer Academic Publishers, Boston/ Dordrecht/ London, 1999.

[2] V. C. Ossai, et. Al., "Enhancing E-voting systems by Leveraging Biometric Key Generation (Bkg)" in American Journal of Engineering Research (AJER), Vol. 2, Issue-10, pp. 180-190, 2013.

[3] .Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman Attacking the Washington, D.C. Internet Voting System In Proc. 16th Conference on Financial Cryptography & Data Security, Feb. 2012 [3].Jossy P. George Saleem S TevaramaniAnd KB RajaPerformance Comparison Of Face Recognition Using Transform Domain Techniques World Of Computer Science And Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 2, No. 3, 82-89, 2012

[4] D. Ashok Kumar, T. UmmalSariba Begum A Novel design of Electronic Voting System Using Fingerprint International Journal Of Innovative Technology & Creative Engineering (Issn: 2045-8711) Vol.1 No.1 January 2011

[5] HongkaiXiong, Yang Xu, Yuan F. Zheng Wen Chen, Fellow, With Tensor Voting Projected Structure In Video Compression Ieee Transactions On Circuits And Systems For Video Technology, Vol. 21, No. 8, August 2011

[6] KashifHussainMemon, Dileep Kumar, and Syed Muhammad Usman, Next Generation A Secure E-Voting System Based On Biometric Fingerprint Method 2011 International Conference On Information And Intelligent ComputingIPCSIT Vol.18 (2011)

[7] ShivendraKatiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi Online Voting System Powered By Biometric Security Using SteganographyInternational Conference On Emerging Applications Of Information Technology 2011

[8] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Security Analysis of the Diebold AccuVote-TS Voting Machine. Proc. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), Boston, MA, Aug 2007

[9] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. Analysis of an Electronic Voting System. Proc. IEEE Symposium on Security and Privacy, Oakland, CA, pages 27–40, May 2004.

[10] Elliot Proebstel, Sean Riddle, Francis Hsu, Justin Cummins, Freddie Oakley, Tom Stanionis, and Matt Bishop. An Analysis of the Hart Intercivic DAU eSlate. Proc. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), 2007.

[11] . David A. Wagner, et al. California Secretary of State's Top-to-Bottom Review (TTBR) of Electronic Voting Systems. July 2007.

[12] Eliza Newlin Carney. Voting Without a Net in South Carolina. National Journal, June 21, 2010. http://www.nationaljournal.com/njonline/rg_20100621_7815.php.

[13] Andrew W. Appel. How I Bought Used Voting Machines on the Internet. Feb 7, 2007. http://www.cs.princeton.edu/~appel/avc/.

[14] Andrew Appel, Maia Ginsburg, Hari Hursti, Brian W. Kernighan, Christopher D. Richards, Gang Tan, and Penny Venetis. The New Jersey Voting-Machine Lawsuit and the AVC Advantage DRE Voting Machine. Proc. Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE), 2009.

[15] Adam Aviv, Pavol Cerný, Sandy Clark, Eric Cronin, Gaurav Shah, Micah Sherr, and Matt Blaze. Security Evaluation of ES&S Voting Machines and Election Management System. Proc. USENIX/ACCURATE Electronic Voting Technology Workshop (EVT), 2008.

[16] Ch.-H. Lin, T.-H.Chenb, Ch.-S.Wub(2013), A batch image encryption scheme based on chaining random grids, Scientia Iranica D 20 (3), 670681.

[17] GuoshengGu, Jie Ling(2014), A fast image encryption method by using chaotic 3D cat maps, Optik 125 47004705. Manish Kumar, D.C. Mishra, R.K. Sharma(2014), A first approach on an RGB image encryption, Optics and Lasers in Engineering 52 2734.

[18] Yicong Zhou, Long Bao, C.L. Philip Chen(2014), A new 1D chaotic system for image encryption, Signal Processing 97 172182.

[19] Ahmed A. Abd El-Latif, Li Li, Ning Wang, Qi Han, XiamuNiu(2013), A new approach to chaotic image encryption based on the quantum chaotic system, exploiting color spaces, Signal Processing 93 29863000. Miao Zhang, Xiaojun Tong(2014), A new chaotic map based image encryption schemes for several image formats, The Journal of Systems and Software 98 140154.

[20] RaduBoriga, Ana Cristina Niculescu, IustinPriescu(2014), A new hyperchaotic map and its application in an image encryption scheme, Signal Processing: Image Communication 29 887901.

[21] 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.

[22] 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.

