IJCSC Volume 5 • Number 1 March-Sep 2014 pp.29-32 ISSN-0973-7391

Study on Security of Online Voting System Using Biometrics and Steganography

Neha Gandhi
M.Tech Scholar, Deptt. Of Computer Sc. & Appl, K.U., Kurukshetra
nehagandhi128@gmail.com

Abstract: It is very important to provide security to voting system and mostly which is online one. In this paper we provide security to online voting system with secure user authentication by providing biometric as well as password security to voter accounts. Basic idea behind this is to combine secret key with cover image on the basis of key image. As a result such new image is produced by system called stego image which is quite same as cover image. The key image is a biometric measure, such as a fingerprint image. Extraction of stego image is take place at server side to perform the voter authentication. The system minimizes the risk factor as hacker needs to find not only the template but also secret key and it is not possible. It makes election procedure to be secure against a variety of fraudulent behaviors. To improve speed SHA 256 used for hashing is replaced with MD5.
Keywords: Biometric, Online Voting, Stego image, Steganography. .

Introduction

Integrity of the election process will help in determining the integrity of democracy itself. So the whole system of election must be secure and robust against a variety of fraudulent behaviors. System should be transparent and comprehensible so that voters and candidates can accept the results of an election [11]. But, now- a-days it has become common for some forces to indulge in rigging which may eventually lead to a result contrary to the actual verdict given by the people. Furthermore, the traditional way of voting will take a long process and time. So, the novel online voting will become the best solution for the matters; besides provide easier way of voting. When we compared it with existing voting system the Electronic voting has several advantages [11] like: Electronic voting system is capable of saving considerable printing stationery and transport of large volumes of electoral material. It is very easy to transport, store, and maintain. It completely rules out the chance of votes which are not valid. In a voting system, whether electronic or using traditional paper ballots, the system should meet the certain important criteria such eligibility and authentication, uniqueness, accuracy, integrity, verifiability, reliability, secrecy, flexibility, convenience, transparency, and cost effectiveness. Among these, authentication can be viewed as the most critical issue.

Online voting system

It is a web based that facilities the running of elections and surveys online. Objective behind the development of this system is to simplify the process of organizing elections and make it easy for voters to vote remotely from their home computers while taking into consideration better security, anonymity and providing auditioning capabilities. Basically ,Users are individuals who interact with the system through web browsers. Biometrics is basically science that tries to fetch human biological features with an automated machine either to authentication or identification. Biometric systems try to exchange Knowledge with feature of an individual, e.g. finger print.

A. Necessity

Electronic voting machines use in India , punch card systems, Global Election Management System used in other countries have lack of indecisive or incorrect election results. So, we have present Online Voting System with Biometric and Steganography, to avoid rigging and to increase the accuracy and the speed of the process so that, everyone can cast his vote irrespective of his location.

B. Advantages

1) Cost saving
2) Reduced administration
3) Create and deploy ballot very quickly and with integrity of the vote counting.
4) No need for renounces
5) Greater performance

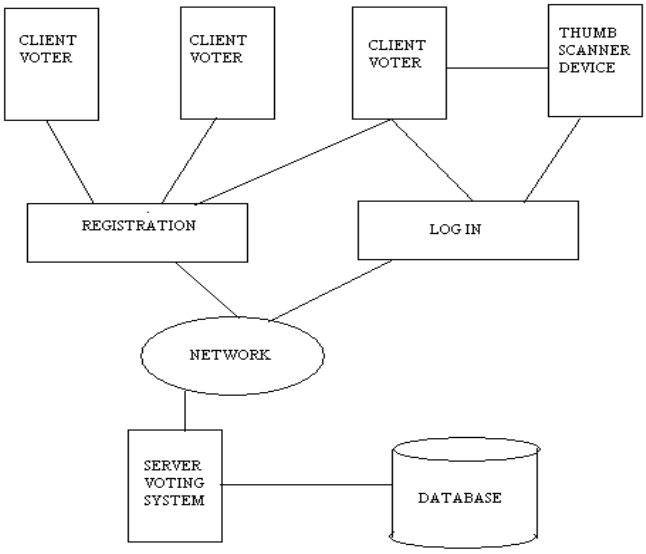

Figure 1: System Architecture

Voting Procedure

Once any individual go through the authenticity criteria, he/she will be logged into his/her voting account. You can easily restrict a voter from logging into his/her voting account more than once during elections. Once any particular voter is authenticated by the system, a secure channel will be established using https and then he/she will be able to cast the vote. The vote will remain secret, i.e., this will not be reflected anywhere in the database that which user has voted for whom. At last, the account will be closed and that disabling user to log back in by any means again. This completes the voting process. The methodology behind the voting process is explained in the fig 2.

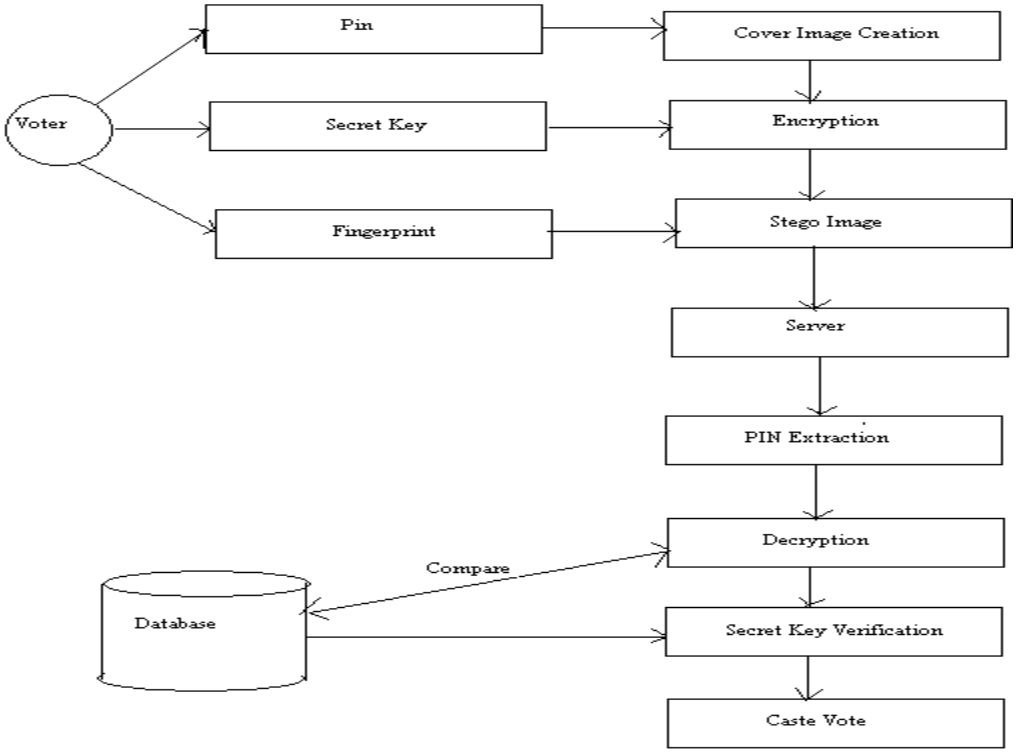

Figure 2: Online Voting System Flowchart

Biometrics

It is the automated recognition of individuals based on their behavioral and biological characteristics. Biometric recognition means by measuring behavioral and biological characteristics of an individual in a recognition inquiry and comparing these data with the biometric reference data which had been stored during a learning procedure, in this way the identity of a specific user is determined. Because it is difficult to misplaced, forged, or shared biometric identifiers, they all are considered more reliable for recognition of person than traditional token or knowledge based methods. The main objectives of biometric recognition are user convenience, security and higher efficiency. Fingerprints are unique for each finger of a person including identical twins. Face Recognition is the process of identification of a person by their facial image. These techniques makes it possible to use the fingerprint and facial images of a person to authenticate him into a secure system, So the Electronic voting system has to be improved based on the current technologies viz., biometric system. A pre requisite for authentication is enrollment, in which the biometric features are saved.

Concept of Steganography

Voting can be done through internet with the concept of Steganography and biometrics. Voter PIN and the secret key are send to the server securely by using Steganography. Steganography is the concept of hiding private or sensitive data within something that seems to be nothing out of the normal. If a person sees the digital object, he or she will have no idea that there is any hidden information, and therefore the person will not try to decrypt the information. The basic model of Steganography says if you want to send some private information then choose a cover image, find its redundant bits and replace these bits with data bits of the information. The information can be easily extracted by doing some operations on the other end.

Least significant bit insertion is a common way to embed information in a cover image. This method overwrites the LSB of a pixel value with a message bit. If we choose a 24-bit cover image, it will become easy to store 3 bits in each pixel. Person will not be able to find the difference in any case. Unfortunately, this method of LSB modification changes some properties of the cover image, so hacker can detect the distortions in the resulting stego image. This is quite viable that we can't embed anybody's personal information in this manner. So, what we can do is that, we can encrypt the information before embedding, or we can do Steganography providing strong encryption at the same time.

Fingerprint images are chosen as keys for encrypting the secret key. Fingerprint recognition is used for user authentication because it is the most deployed biometric technique, both in civil and criminal applications, because of its high maturity and cost-effective capture and processing.

Some information about the voter should be collected to support such a system. Firstly, each and every individual in the country should be provided with a Personal Identification Number. This is needed for maintenance of voter accounts in the database. Secondly, we need Thumb Impressions (fingerprint images) of all the individuals. Thirdly, when we create an account every person will be provided with a system generated Secret key which he/she should not reveal to anybody. That will be needed to cast the vote.

Related Work

Subba Rao et al., [1] in 2011 proposed a Steganography technique that is based on randomizing the sequence of cipher bits. Advantage of this technique is there is no one-to-one mapping between a given cipher text and an image.

Constantinos Patsakis and Evangelos Fountas [2] in 2010 proposed Fibonacci LSB Data Hiding Technique to more integer bases. In this work, a new embedding method, which generalizes the idea of Fibonacci decomposition, enabling more data to be embedded in an image with good statistical properties was presented.

Namita Tiwari and Dr.Madhu Shandilya [3] in 2010 evaluated the LSB based Methods of Image Steganography on GIF File Format. This paper focused on hiding the message in the least significant bits of the colors of the pixels of a GIF image.

Hanan Mahmoud Hanan et al., [4] in 2010 proposed a Novel Technique for Steganography in Fingerprints Images. This paper describes the design and implementations of a project concerning the hiding of messages in images specifically fingerprint images. The policy of this project is to keep the confidential messages hidden inside the drawing of the fingerprints.

Sanjay Saini and Dr. Joydip Dhar [5] in 2008 proposed an eavesdropping proof secure online voting model. In this paper an online voting framework was formulated which ensures that the voter is able to vote in a public environment without his vote being eavesdropped on by a neighbor.

E.S. Shameem Sulthana and Dr.S.Kanmani [6] in 2011 presented the Evidence based Access Control over Web Services scheme using Multi Security. This paper explains about voting through internet, with facial detection integrated with finger print authentication and automated load balancing, fused with data hiding security.

Alok Kumar Vishwakarma and Atul Kumar [7] in 2011 proposed a Novel Approach for Secure Mobile-Voting using Biometrics in Conjunction with Elliptic Curve Crypto-Stegano Scheme. This paper describes a secure mobile-voting system using cryptography and Steganography.
Nabin Ghoshal and J. K. Mandal [8] in 2011 proposed a Steganographic Scheme for Colour Image Authentication. This paper deals with a novel steganographic technique which demonstrates the colour image authentication technique in frequency domain based on the Discrete Fourier Transform (DFT). Experimental results confirmed that this algorithm performs better than discrete cosine transformation (DCT), Quaternion Fourier Transformation (QFT) and Spatio Chromatic DFT (SCDFT) based schemes.
Masoud Afrakhteh and Subariah Ibrahim [9] in 2010 presented an Enhanced Least Significant Bit Scheme robust against Chi-Squared attack. Among the steganographic techniques and particularly in conventional least significant bit (LSB) insertion method, there is a challenging issue and that is how to embed desired secret bits in a cover medium in a way not to be seen by human vision. This paper proposes a method that utilizes more surrounding pixels unlike BPCS, PVD and MBNS methods which use 3 or 4 immediate neighbors of each pixel and finally, it is finally, it is proved that the method is robust against Chi-squared attack.
Guo-Shiang Lin et al., [10] in 2010 proposed a framework for Enhancing Image Steganography with Picture Quality Optimization and Anti-Steganalysis based on Simulated Annealing Algorithm. In this paper, a closed-loop computing framework was proposed which iteratively searches proper modifications of pixels/coefficients to enhance a base steganographic scheme with optimized picture quality and higher anti-steganalysis capability.

Conclusion

In this paper we use a technique to provide security to an online voting system by combining concept of Steganography with Cryptography. Steganography and Cryptography is used together to provide security to voter account. So for this images and keys get used in combination first time. Here main object for Steganography is image and for cryptography it is keys. New idea is basically to replace SHA 256 with MD5 hashing to improve speed. Security level is enhanced by random cover image generation for each voter .The voter authentication process of system is improved by combining both biometric and password security. As a future work, multi-biometrics measure can also be used to implement online voting system.

References

[1] Subba Rao, Brahmananda Rao, Rukma Rekha, ”Secure image steganography based on randomized sequence of bits”, eighth international conference on information technology 2011.
[2] Constantinos patsakis, Evangelos Fountas,”Extended fibonacci LSB data hiding technique ti more integer bases”3r*d* international conference on advanced computer theory 2010.
[3] 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.
[4] 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.
[5] Sanjay Saini and Dr. Joydip Dhar, “An eavesdropping proof secure online voting model” International Conference on Computer Science and Software Engineering 2008.
[6] 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.
[7] 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.
[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 Chi-Squared Attack” Fourth Asia International Conference on Mathematical/Analytical Modeling and Computer Simulation 2010.
[10] Guo-Shiang Lin, Yi-Ting Chang, and Wen-Nung Lie “A Framework of Enhancing Image Steganography with Picture Quality Optimization and Anti-Steganalysis Based on Simulated Annealing Algorithm” IEEE Transactions on Multimedia, August 2010.
[11] Tadayoshi Kohno,Adam Stubblefield,Aviel D.Rubin, and Dan S.Wallach. *“Analysis of an Electronic Voting System”,* Proc. IEEE Symposium on Security and Privacy (May, 2004), found at http://avirubin.com/vote/analysis/index.html.