ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 1, Issue 9, November 2013

OnVote – Secured online voting

Priyanka Chordia[1],Pooja Chavan[2], Bhagyashri Patil[3], Rutuja Patil[4], Mrs. Priyanka More[5]

Student, Dept. of Computer Engineering, VIIT, Pune, India[1,2,3,4]

Asst Professor, Dept. of Computer Engineering, VIIT, Pune, India[5]

ABSTRACT: Integrity of the election process directly determines the integrity of democracy itself. So the election system must be secure and robust against a variety of unauthorized behaviors. It should be transparent and comprehendible. But in history, there are examples of elections being manipulated in order to influence their outcome. In a voting system, whether electronic or using traditional paper ballots, the system should meet the following criteria: Obscurity, Tamper-resistant, Human factors.

In this paper we are proposing an Online voting system using Cryptography and Steganography at the same time for providing high security for the voters. Here, we are trying to provide Biometric as well as password security to voter account. The system uses images for various purposes such as cover objects for Steganography and as keys for Cryptography. The fundamental idea is to generate a cover image which has the secret key merged into it. The image generated out of this process is a stego image which is the key image. The key image is a biometric means, such as an image of fingerprint. By using cryptography and steganography together it greatly reduces the risk of being hacked by the hackers as both secret key and the template are to be identified. Since the generated image looks similar to the cover image it becomes difficult to identify if any secret key is present in it. The system is built to provide authentication to the voting system.

Keywords: Steganography, Cryptography, Biometric, stego image, online voting

I. Introduction

Elections are said to be the process for selecting the governing body and the governing person for a country. The integrity of the election process determines the integrity of the democracy itself. For that the election system has to be secure and robust against a variety of deceitful behaviors, and should be transparent and comprehensible that candidates and voters can accept the result of the elections. But, we can see through the history that elections were manipulated in order to influence their outcome. And hence the need for a secure voting system emerged. There are certain criteria's which any voting system, it may be paper voting or electronic voting, should meet :-

A. Obscurity : Obscurity of ballot should be preserved, both to guarantee the voters the voters safety when voting against a malevolent candidate and to guarantee that voter have no proof that proves which candidates receive their votes.

B. Tamper-resistant : The voting system must also be tamper-proof to thwart a wide range of attacks, including ballot stuffing by voters and incorrect tallying by insiders.

C. Human factors : A voting system must be comprehensible and usable by the entire voting population, regardless of age, infirmity or disability.

The election must be –

1. Sufficiently robust to withstand a variety of fraudulent behaviors.
2. Scalability.
3. Speed, accuracy and authentication.

Out of these authentications can be viewed as the most critical issue. Online voting system is used to keep a track of the votes and facilitate the user by making it possible for an individual to vote online. This system is being developed to simplify the process of organizing elections and making it possible for the voters to vote remotely from their home computers provided that they have a finger print detector and the software installed on it or from the voting centers approved by the government while taking into consideration security, anonymity and providing auditioning capabilities. The users are individuals who interact with the system through the web browsers.

II. NECESSITY

The current methods used for voting in India and many other countries is by using Electronic Voting Machine to implement electronic voting in place of ballot papers and boxes which were used in earlier conventional voting system. It may be vulnerable to deceitful activities like misuse of voters information, booth capturing and so on.

The objective behind developing the system is to present a new online voting system employing biometrics in order to avoid tackling and to enhance the accuracy and speed of the process so that one can cast the vote irrespective of one's location.

III. RELATED WORK

1. Subba Rao et al., [1] has proposed a technique that is based on steganography for randomizing the sequence of cipher bits. The main benefit of this technique is there is no one-to-one mapping between a given cipher text and an image.
2. Namita Tiwari and Dr.Madhu Shandilya [2] evaluated the LSB based Methods of Image Steganography on GIF File Format. In their paper they focused on hiding the message in the least significant bits of the colors of the pixels of a GIF image.
3. Hanan Mahmoud Hanan et al., [3] proposed a remarkable Technique for Steganography in Fingerprint Images. The paper has the description of 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.
4. Sanjay Saini and Dr. Joydip Dhar [4] proposed an intrude proof secure online voting model. In their paper an online voting framework was formulated which ensures that the voter is able to vote in a public environment without his vote being spyed on by a neighbor.

IV. PROPOSED METHODOLOGY

Using this system voting can be done online with the help of steganography and biometrics. The user has to register first with the help of the administrator who takes the personal information of the user and generates a Personal Identification Number i.e. the PID. The PID and the secret key are transmitted to the server securely using steganography. Steganography is the idea of hiding vulnerable data in the form of image or inside an image which appears to be a normal image. The general model of steganography says if one wants to send some secret message then choose a cover image, find its redundant bit and replace it with the message bit. The message can be easily extracted by doing the same operations on the other side.

The stego image looks similar to the original image and hence make it difficult to identify between the original and the stego image making it secure against any attack. [5]Least significant bit approach is a common approach to embed information in a cover file. This process overwrites the LSB of a pixel value with a message bit. Human eye is unable to find the difference in any case. Unfortunately, this process of LSB modification changes the statistical properties of the cover image, so eavesdroppers can detect the distortions in the resulting stego image. This is quite feasible that we can't embed anybody's personal information in this manner. So, we are going to encrypt the message before embedding, or we will perform steganography providing strong encryption at the same time.

The image to be chosen is the fingerprint image 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. First of all , 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, during the account creation every individual will be provided with a system generated Secret key which he/she should not disclose to anybody. This will be needed to cast the vote. The voter account creation process is shown in fig 1.1:

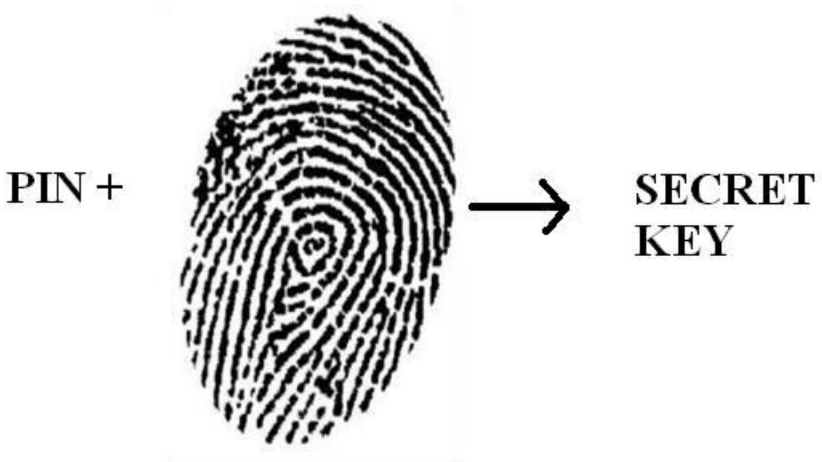

Fig 1.1 Secret Key Generation

Assuming that all voters' information in a country is collected securely , biometric reader available for voting, the system is online during the election period only, the methodology is as follows.

To cast a vote, a voter logs into the system by entering the personal identification number and secret key. Along with this voter has to give the thumb impression on the fingerprint sensor. The system will generate the cover image and embed the secret key into it according to the predefined procedure to generate the stego image as shown in fig 1.2:

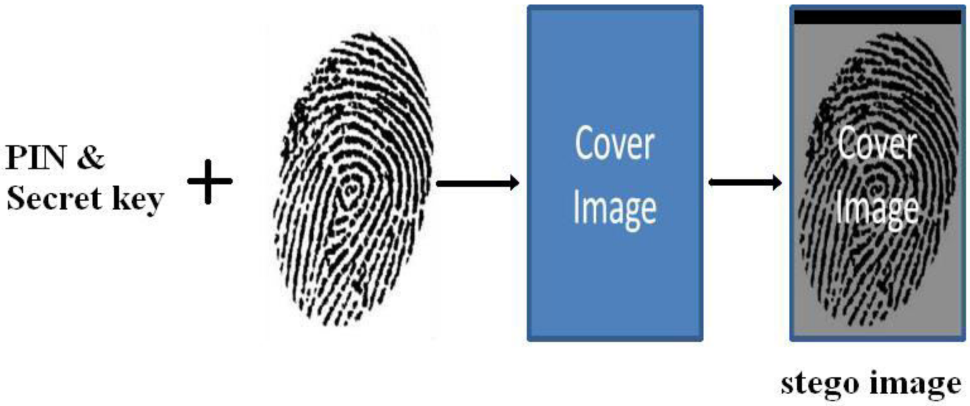

Fig 1.2: Stego Image Creation

Now this generated stego image will be sent securely to the server for voter authentication. Fingerprint fraud may be restricted by using advanced fingerprint readers which employ Ultrasonic and Capacitance.

At the server side, Optical Character Recognition technique will be used to read the personal identification number represented on the image. After reading it, the server will find out the details of that individual from the database. These details will be his/her fingerprint image and secret key. Using these details, the image can be decoded to find out the embedded message which should be the secret key of that individual. Once authentication is complete, the voter will be allowed to vote. The voter can select the desired candidate and finalize the vote. After casting the vote, the account will be closed and in the database the voted bit will be set to one for that voter. On the basis of the same procedure followed by every voter, the votes will be calculated altogether and the person with the maximum votes will be obtained.

V. ADVANTAGES

1. Cost Saving.
2. Reduced Administration.
3. Create and deploy ballot quickly and with ease, integrity of the voting count.
4. No need for renounces.
5. Greater Performance.

VI. CONCLUSION

The focus of this paper is to enforce a method of integrating biometrics and steganography to present highly secure online voting system. The security of the system will be maintained highly by generating cover image for each voter. The user will be able to cast the desired vote being anywhere in the country provided that the procedure meets the system requirements.

REFERENCES

1. Subba Rao, Brahmananda Rao, Rukma Rekha, "Secure image steganography based on randomized sequence of bits", eighth international conference on information technology , pp.332-335,2011.

2. Constantinos patsakis, Evangelos Fountas, "Extended fibonacci LSB data hiding technique ti more integer bases"3*rd* international conference on advanced computer theory ,pp.V4-18,2010.

3. Hanan Mahmoud Hanan Saad Al-Hudaibah Sarah Ahmad Al-Naeem Suha, **"**Novel Technique for Steganography in Fingerprints Images: Design and Implementation" Sixth International Conference on Information Assurance and Security , pp.97-102, 2010.

4. Sanjay Saini and Dr. Joydip Dhar, "An eavesdropping proof secure online voting model" International Conference on Computer Science and Software Engineering ,pp.704-708, 2008 .

5. B. Swaminathan and J. Cross Datson Dinesh , "Highly Secure Online Voting System with Multi Security using Biometric and Steganography" , pp.103-107, 2012.