IJREAT International Journal of Research in Engineering & Advanced Technology, Volume2Issue2, April - May,2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Biometrics and Steganography based Secure Online Voting System

V. Jothi Lakshmi[1], P.Vineka[2], V.Anbarasu[3]

[1, 2, 3]**Department of Information Technology, Jeppiaar Engineering College, Chennai, India**

Abstract

In India elections are conducted almost exclusively using Electronic Voting Machines (EVM's) developed over the past two decades by the government have been praised for their simple design, ease of use, and reliability. Illiterate people are cheated by some criminals through booth capturing wherein party loyalists would take over a polling station by force and stuff the ballot box. So we took effort to overcome these mischievous activities & maintain the right of vote. Thus in proposed methods there are different levels of security in the voting process which makes safer. The methods included are biometric techniques like thumb impression and face recognition for voter's authentication and cloud storage for database which would make voting process more effective.

1. INTRODUCTION

Today democracy has become an important part of people's lives, and to achieve democracy, it must meet several conditions. The heart of democracy is voting. Thus e-voting is used to casting and counting votes using electronic system which is physically supervised by representatives of governmental and remote. E-Voting is performed within the voter's sole influence, (e.g. voting from one's personal computer, mobile phone, television via the internet).

Electronic voting technology can speed the counting of ballots and can provide improved accessibility for disabled persons. Among biometric signs, fingerprint, face recognition shows the most promising future in real-world applications.

Each one has unique fingerprints, face which have been used for identification over time. There have been several studies on using electronic technologies to improve elections with biometric technique, cryptography, Steganography.

2. RELATED WORKS

Thumb impression is used for the voter's authentication. User security is provided by Steganography and Cryptography. Steganography main object is image and for cryptography it is keys. However hardware is required for taking thumb impression which is costly[1].

Face Recognition system is also used as an Authentication technique. The captured voter's image is sends toward the face recognition algorithm. But high light intensity is needed for good picture[2].

E-Vox, is both easy to use and system independent. The entire system requires only the voter register a name and password. It does not require voters to use a public key for encryption. However, the system cannot currently support a preferential balloting system without a nontrivial effort [3].

3. SYSTEM DESCRIPTION

Cloud contains database which can hold multiple information about the voters. During voting the voter must give fingerprint as the major input. The voting system may also provide some features like eye and face recognition. Then his finger print would be taken with the help of a finger print scanner this fingerprint would be send to the server for matching purpose. If it matches

then only the voter would be able to cast his vote successfully. The same procedure happens for eye and face recognition using webcam. The voter can select the name of the party to which he wants to cast his vote just by saying YES /NO/CANCEL /RESUME/OK. Similarly users can cast their vote to a candidate of the given party.

In order to process the finger print, image from the scanner will be sent to the server. Thus face and eye recognition image from webcam also will be sent to the server. For security purpose the image can be encrypted at the server side and at the end of the server image can be decrypted. when the image processing the image matching process is over the result would be send back to the client in the form of whether the voter is allowed to vote or not.

When the image is processed by the server the server would allow the voter to cast their vote, if their fingerprint and other identities matches with the image template in the cloud containing database otherwise user won't be allowed to do the same.

4. SYSTEM ARCHITECTURE

Phase1: The registration takes place in this phase. If the user already registered can directly login. New user can gives his full name, ward name, address, contact no, e-mail, etc and register it. After registration, user can sign up. After the login process has takes place it goes to the authentication phase.

Phase2: Authentication process like eye tracking, face recognition, thumb impression takes place in this phase. It uses stego image for face and eye tracking verification. The Steganography and cryptography technology are used for encrypting and decrypting the data. Every user is provided with stego image. Once the user face is recognized by using web cam then image is send to the server. If the stego image and face recognition is matched the voter is allow for vote. This is connected to the cloud network which can store the large database and easy to access.

Phase3: The final phase is the voting phase where the user can vote. The user can select the candidate and vote. After successfully processed, the user can logout from the corresponding site.

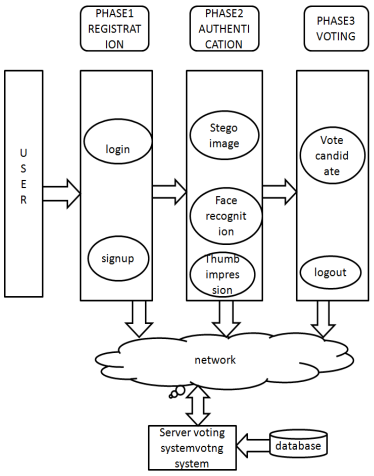

Figure 1.1Online voting system Architecture

5. PROPOSED ALGORITHMS

It has two types embedded and authentication algorithm.

5.1 Embedded Algorithm

It is also known as encoding algorithm which is used to create stego image. At the time of registration the system capture face of the user by the web camera and the finger impression in the form of the stego image and store the sample in the server database.

After this system will generate the PIN and secrete key for the user. With this it captures the photo system which gives the cover image. Stego image can be generated by the cover image.

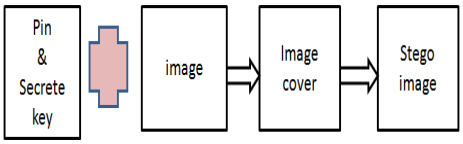

Figure 1.2 Stego image creation (encoding)

Embedded Algorithm

Begin
SI[ ]=CI[ ]
for every bit of Secret Message SecretMsg[i] **do**
ifSecretMsg[i]=1 **then**
if CI[Random[i]] and KI[Random[i]]both either even or odd **then**
if odd **then**
SI[Random[i]]=CI[Random[i]]-1
else
SI[Random[i]]=CI[Random[i]]+1
else
SI[Random[i]]=CI[Random[i]]
else
if CI[Random[i]] and KI[Random[i]]both either even or odd **then**
SI[Random[i]]=CI[Random[i]]
else
SI[Random[i]]=CI[Random[i]]+1
END

Stego image is the number which is given for every user for security purpose and avoiding duplication of vote the number is send to the user mail account. This image then passes to the server for authentication algorithm.

5.2 Authentication algorithm

It is the Decoding process initially PIN is generated from the Stego image. We can compare the Key image and the Secrete image of the individual from the voter Database. If the Stego image is valid then the system will generate the user id and password for the login. After the successful login system will capture the face of the user by the webcam and thumb impression by the scanner for the recognition. In this algorithm, we are compare the two image first is newly capture image and the second is same photo of the person which are stored at the time of registration in the database. .If the image can be match then the user will get the candidate list and ward no. According to their choice the user can vote their selected candidate. Then logout from the corresponding site and they can't re-enter.

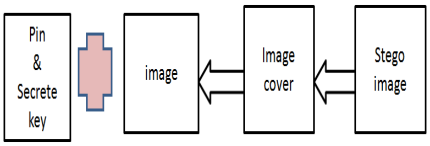

Figure 3.3 stego authentication algorithms

Authentication Algorithm

Begin
SecretMsg[ ],Date[32],SecretKeyDate,j
for i=0 to 287 **do**
if SI[Random[i]] & KI[Random[i]] both either even or odd **then**
SecretMsg[i]=0
else
SecretMsg[i]=1
for i=256 to 287 **do**
Date[j++]=SecretMsg[i]
SecretKeyDate=Concatenate(SecretKey,Date)
if

compare(SecretMsg[],SHA256(SecretKeyDate))**th en**
Return:Authentic Person
else
Return:Not an Authentic Person
END

6. RESULTS AND DISCUSSION

By analysing the online voting system with statistical data, we found that only three out of seven peoples are voted successfully in online. Failures are occur due to some lack of knowledge in using system, technical problems. This figure 1.4 shows the relation between numbers of voters versus number of voting.

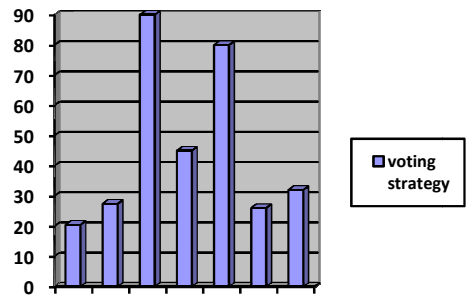

Figure 1.4 Graphical representation

Server operates automatically, manual operation is not needed which reduce administration.It reduce the manual work and it takes only less time and high performance is also obtained. The information is secure. Other than the voter nobody can know the voting details. The process can be done quickly. It avoids the duplicate vote. So it gives right to vote to everyone. People can select the right leader. Voting can be done from anywhere through web. It surely increase the voting percentage

7. CONCLUSION AND FUTURE WORK

In this system we have enforced a method for integrating Cryptography and Steganography to present a highly secure Online Voting System. The security level of our system is greatly improved by the new idea of stego image generation with algorithm.

It can include features like fingerprint, face and eye recognition for more security. It also uses the cloud which contain database in order to store voter's information. So, the data can be easily accessible. Thus, the citizens can be sure that they alone can choose their leaders, thus exercising their right in the democracy.

It can be used in future engineering research. After voting Confirmation SMS can send to the voter from server to indicate voting is successfully done. Create the e-voting system usable for handicapped people by using the eye retina or voice, etc for authentication.

REFERENCES

[1] Face Base Online Voting System Using Stegnography (Volume 3, Issue 10, and October 2013).

[2] Secure Online Voting System Proposed By Biometrics and Steganography Issue 5,May 2013.

[3] New System of E-Voting Using fingerprint (volume 2,Issue 10,October 2012)

[4] Online Voting System Powered By Biometric Security Using Stenography 2011 second International Conference on Emerging Applications of Information Technology http://www.softinfology.com/ieee/catlog/security/ PSJAV 16 Online Voting System Powered By Biometric Security Using Steganography.pdf.

[5] Secure Online Voting System Proposed By Biometric and Steganography.

[6] A Biometric-Secure e-Voting System for Election Processes http://www.sunday chennai.com

[7] E-Voting System http://www.vvk.ee/public/ dok/ Yldkirjelduseng.pdf.

[8] A Survey on Voting System Techniques http://www.ijarcsse.com/docs/papers/Volume 3/1 January 2013/V3II-0221.pdf.

[9] Analyzing Internet Voting Security http://www.cs.berkeley.edu/daw/paper/camserve.pdf.

10] Proposed Of a new online voting system http://easyvote-app.sourceforge.net.

AUTHORS

First author –**V. Jothi Lakshmi**, is currently doing her Third year **B. tech Information Technology**at**Jeppiaar Engineering College** in Chennai**,** Tamil Nadu .She has presented a paper based on cloud computing in national level technical symposium and has attended many workshops.
Email ID - jvothjo30@gmail.com

Second author**–P.Vineka,**is currently doing her Third year **B. tech Information Technology** at**Jeppiaar Engineering College** in Chennai, Tamil Nadu .She has presented a paper based on big data in national level technical symposium and has attended many workshops related to ethical hacking android.
Email ID–vineka1994@gmail.com

Third author – **V Anbarasu B.E., M.Tech., (Ph.D)** is working as an **Associate Professor** in the **Department of Information Technology** at **Jeppiaar Engineering College** in Chennai, Tamilnadu. His areas of interest are Operating Systems, Human Computer Interface and Programming Paradigm. He has 10 years of teaching experience. He has presented 12 papers in International and National Conferences and also published 5 papers in International and National journals. He has attended several workshops and FDPs.
Email ID - anbarasukv@gmail.com