The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 3 || Pages || PP.71-75|| 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Secure Internet Voting System

[1] Arti Bhise, [2]Namrata Borate ,[3]Aarti Garje,[4]Yogita Karkal

[1]Department of Information Technology, JSCOE
[2]Department of Information Technology, JSCOE
[3]Department of Information Technology, JSCOE
[4] Department of Information Technology, JSCOE

ABSTRACT

The voting percentage of India is very less and is considerably declining day by day. The illiterate people can be fooled and their votes can be cast to different candidates. Also incidents like booth capturing are increasing and some undeserving candidates are getting elected. Thus the objective is to put a stop to all these malicious activities and to safeguard the right of voting of an individual through the idea proposed in this paper. The paper proposes an authentication algorithm which uses visual cryptography to provide security in internet voting system. Thus the plan is to make the voting process a secure and effective one. Visual cryptography scheme is one of the most secure techniques for privacy, that allows the encryption of secret image or data by transferring it into the secure share and the decryption is done without any computation devices.

Keywords – *Biometrics***,** *Internet Voting System (IVS), I-voting, Stegnography, Visual Cryptography (VC).*

Date of Submission: 25 February 2015 Date of Accepted: 20 March. 2015

I. INTRODUCTION

Elections are conducted in small scale organizations, corporate institutes and on a larger scale, in parliaments too, for appointing board members of that organizational body. These elections restrict the voters to be present at that voting location thus causing inconvenience. This causes an alarming need to bring remote voting systems to effect. Internet voting system using visual cryptography fulfills this need of being able to vote from anywhere without causing security concerns.

1.1 Internet Voting System

Internet voting system enables a voter to vote over the internet while providing accuracy and security. Internet voting system can be of two types-Poll-site and remote voting. Poll-site voting enables the voter to vote over the internet, at a voting poll. Remote voting enables the voter to vote from anywhere around the globe thus removing geographical restrictions [2].

1.2 Visual Cryptography

Visual cryptography is an encryption technique that encrypts data using secret key. The encrypted data can be decrypted using human visual system. Thus decryption can be done by someone without the knowledge of cryptography and does not require any decryption algorithm [3].

II. LITERATURE SURVEY

Our system is implemented for various corporate companies to convey their elections for different posts such as the presidential election, manager election etc. Even though the branches of the companies are situated in different parts of the country or the world, the elections can be conducted easily and effectively in a proper manner by using this Internet based voting system using visual cryptography because the voter can vote from the place where he is working by using this system. The literature survey done by us includes two existing systems that also implement the concept of electronic voting but use different techniques for providing additional security. They are as explained below:

2.1 Security Analysis of the Estonian Internet Voting System [5]

Many countries have tried with casting votes over the internet. According to the recent analysis Estonia uses internet voting for conducting political elections to a larger degree than other countries. Estonia introduced its online voting system in 2005 and it was named as I-voting. It was the first country that was offered internet voting nationally. This system has been used many times in local and national elections.

The concept of I-voting is as explained. An essential building block of the I-voting system is Estonia's national ID infrastructure. These national ID cards are smart cards with ability to perform cryptographic functions. With the help of card readers and client software it can authenticate to their websites via TLS client authentication and it will make legally binding signature on documents. These cards are mainly used for online banking and e-government services. In this I-voting system the voters use their ID cards to authenticate the server and cast their vote.

2.1.1 Advantages

- This system guards against attacks and ensures transparency of insufficient protection.
- Due to use of ID cards, system can easily authenticate that the voter is legal.
- Due to I-voting, the voting percentage of country can be increased to some extent as compared to previous elections

2.1.2 Disadvantages

- This system has serious procedural and architectural weaknesses which expose Estonia to the risk that can alter the outcome of election.
- The weakness of the system is in its basic design that this design implicitly trusts the integrity of voter's computers, server components, and the election staff.

2.2 Online Voting System Powered By Biometric Security Using Steganography[4]

Stegnography is data hidden within data. Stegnography is an encryption technique that can be used along with cryptography as an extra-secure method in which to protect data.

The system uses cryptography, Stegnography, biometrics as well as password security is provided to voters' accounts. The system uses images as cover objects for Stegnography and as keys for Cryptography. The key image is a Biometric measure, such as a fingerprint image. The proper use of cryptography greatly reduces the risk of this system as the hackers need to find both secret key and template. The basic idea is to merge the secret key with the cover image on the basis of the key image. The result of this process produces a stego image which looks quite similar to the cover image but not detectable by human eye. The system targets the authentication requirement of a voting system.

2.2.1 Advantages

- This system presents a method for integrating cryptography and Stegnography.
- The strength of the system resides in the new concept of key image.
- This system is also able to change the cover coefficients randomly.
- This system provides sufficient proof of authenticity of an individual in form of both biometric measures and secret key.

2.2.2 Disadvantages

- Countries with large population have to invest large amount of money, time as well as man power for voting set up.
- This system is much complicated to implement and maintain.

III. INTERNET VOTING SYSTEM USING VISUAL CRYPTOGRAPHY

There are number of visual cryptography schemes as follows.

3.1 Two out of two visual cryptography scheme

In this type of Visual cryptography scheme, the secret image is divided into two shares. This is the simplest kind of visual cryptography. The major application of this scheme is found with IVS that uses 2 out of 2 Visual secret sharing schemes for authentication purpose. To reveal the original image, two shares are required to be stacked together.

Pixel colour	Original pixel	Share 1	Share 2	Share1 + Share 2
Black	■	■□	□■	■■
Black	■	□■	■□	■■
White	□	■□	■□	■□
White	□	□■	□■	□■

Fig 1. Pixel representation for 2 out of 2 visual cryptography scheme

3.2 n out of k visual cryptography scheme

This type of visual cryptography scheme divides a secret image into k number of shares. Then the secret image can be revealed from any n number of shares among k. For example, in 3 out of 6 VC scheme, any 3 shares out of 6 shares are sufficient to reveal the secret data. The major problem this scheme is that the user needs to maintain many shares which may result into loss of shares. Also more number of shares means more memory consumption.

3.3 k out of k visual cryptography scheme

In This type of visual cryptography scheme secret is divided into k number of shares and for reconstruction of the secret image, all k shares are required. For example, in 6 out of 6 VC scheme, Secret is revealed only after stacking all the 6 shares, where k= 6. This scheme is not so popular because managing k number of shares is difficult task and it also increases time complexity [1].

IV. METHODOLOGY

The system comprises of three modules namely admin module, client module and server module. The working of the system is as shown in the Fig 2.

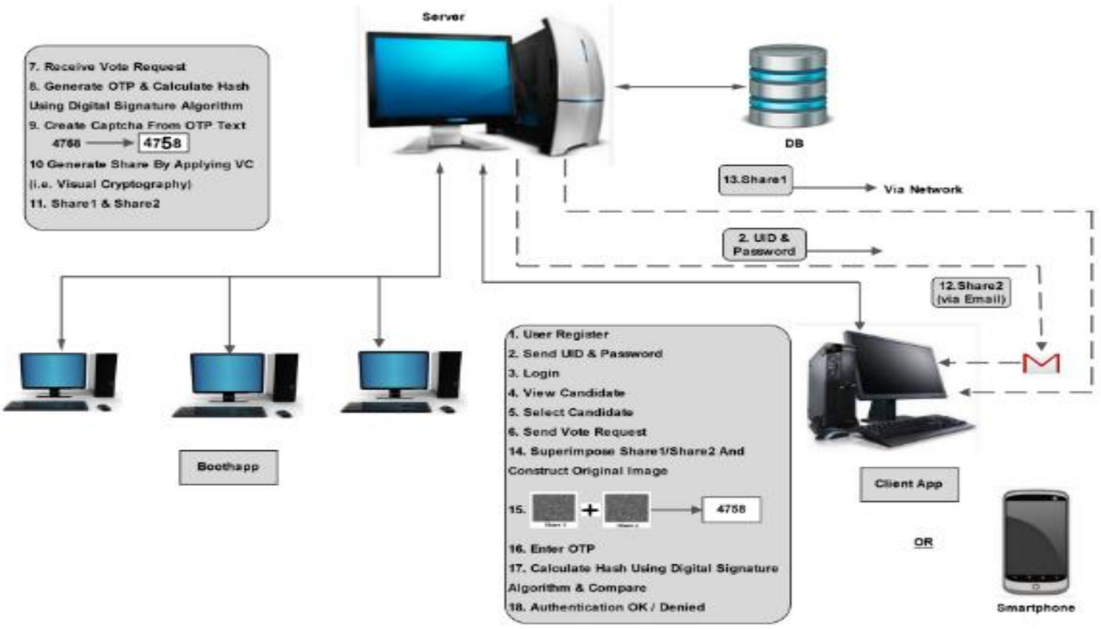
Server
7. Receive Vote Request
8. Generate OTP & Calculate Hash Using Digital Signature Algorithm
9. Create Captcha From OTP Text
4758
4758
10 Generate Share By Applying VC (i.e. Visual Cryptography)
11. Share1 & Share2
DB
13.Share1
Via Network
2. UID & Password
12.Share2 (via Email)
Boothapp
1. User Register
2. Send UID & Password
3. Login
4. View Candidate
5. Select Candidate
6. Send Vote Request
14. Superimpose Share1/Share2 And Construct Original Image
15.
+
4758
16. Enter OTP
17. Calculate Hash Using Digital Signature Algorithm & Compare
18. Authentication OK / Denied
Client App
OR
Smartphone

Fig 2. System Overview

The admin module consists of functions like add/manage user, add/manage candidate, add/manage parties and view votes. The admin can add, update, and delete information related to the users, candidates and parties through this module.

The client module consists of the android application installed on the user's smart phone. The application requires the user to register himself after which he needs to sign up using the same username and password as used while registering. Then the user is to select the candidate he wishes to vote. Once the user clicks on the 'Vote' button he is supposed to upload the share 1 sent to him via his e-mail id while the share 2 is automatically uploaded by the server. Authenticated users will be shown a captcha which the users have to enter correctly. Upon entering the captcha correctly the user's vote will be registered successfully.

The server module is concerned with generation of shares, generation of captcha and authentication of users.

This process of encryption/decryption is illustrated in the fig 3.

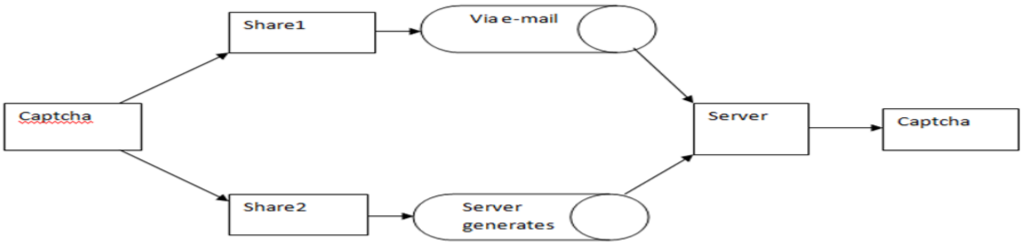

Fig 3. Encryption/Decryption process

4.1 Algorithms used

4.1.1 RGB separation

1) Consider the pixel having R, G, and B components (in Hexadecimal format) as:-
9966ff where,
99: is R component
66: is G component
Ff: is B component
We have to perform different Boolean operations on these components
2) To obtain B component (AND with ff)
9966ff
AND ff
Ans=0000ff
Here ff is the B component
3) To obtain G component (right shift by 8-bits AND with ff)
9966
AND 00ff
Ans=66
Here 66 is G component
4) To obtain R component (right shift by 16 bits AND with ff)
99 AND ff
Ans=99
Here 99 is R component

4.1.2 Gray Scale (to simplify operations on pixels)

Take the average of all three components which will give grayscale value

GS=R+G+B/3

Thus GS=R=G=B

4.1.3 Threshold (to separate background and foreground image)

```
If (GS>TH) then
GS= 255 [pixel is white]
Else
GS=0   [pixel is black]
```

Where TH is threshold value which is=128 and GS= Gray Scale value.

V. CONCLUSION

The designed system is used in election processes in clubs, corporate organizations, government elections etc. The system uses two way authentication as the authentication process is performed on the server side as well as the client side thus providing greater security. The electronic voting system has several advantages like allowing remote voting which removes geographical restrictions to the voter. The encryption technique that is used in our system is visual cryptography which makes use of encrypted shares and decryption is done by human visual system which reduces difficulties in decryption.

IV. ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without mentioning the people who make it possible. We are grateful to a number of individuals whose professional guidance along with encouragement have made it very pleasant endeavor to undertake this project. We have a great pleasure in presenting the paper "Secure Internet Voting System" under the guidance of Prof. A. K. Gupta and for giving us an opportunity to work on this topic. Her encouraging words went a long way in providing the patience and perseverance, which were needed to complete this project successfully. Also her true criticism towards technical issues provided us to concentrate on transparency of our project. We would like to express our gratitude to Dr. M.G. Jadhav, Principal of Jayawantrao Sawant College of Engineering and Prof. S. V. Todkari, Head of Department of Information Technology for their support and guidance.Finally we express our sincere thanks to our parents and all those who helped us directly or in directly in many ways in completion of this paper.

REFERENCES

[1] Rajendra A B and Sheshadri H S, Visual Cryptography in Internet Voting system, *IEEE,* 2013

[2] Anusha MN Srinivas B K., Remote Voting System for Corporate Companies using Visual Cryptography*, International Journal of Advanced Research in Computer Science and Software Engineering Research, Volume 2,* Issue 6, June 2012

[3] Puja Devi Rana, Anita Singhrova, Suman Deswal Design and Implementation of K-Split Segmentation Approach for Visual Cryptography, *International Journal of Scientific and Research Publications*, *Volume 2*, Issue 8, August 2012

[4] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi, Online Voting System Powered By Biometric Security Using Steganography, *IEEE*, 2011

[5] J. Alex, Halderman Harri Hursti, Jason Kitcat, Margaret MacAlpine, Travis Finkenauer1 Drew Springall,
Security Analysis of the Estonian Internet Voting System, May 2014