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. 3, Issue 3, March 2015

Online Voting System Using Three Factor Authentication

Rashmi Nade, Monali Raut, Punam Agawane, Jayshree Shinde

Student, Dept. of I.T., BVCOEW, Savitribai Phule Pune University, Pune, India

ABSTRACT: The voting percentage of India is very less & is considerably declining day by day. The illiterate people can be fooled & their votes can be casted to different candidates other than the one whom they wished to give away their votes. Also incidents like the booth capturing are increasing day by day & some undeserving candidates are getting elected & ruling our Nation, thus leading to the loss of nations property & other thing. Thus we the students have tried to make a sincere effort to put a stop to all this malicious activities & safeguard the right of voting of each & every individual of India. The software will provide a user friendly GUI using which the voters can caste their votes to different parties & the corresponding candidates. Different levels of security would be provided in the software which would help in authentication of an individual.We are providing Biometric for identifying an individual, Online Voting Application by which a user can be able to vote using Internet, Finger Recognition Hardware Interface, Steganography. Thus we plan to make the voting process a secure & effective one.

KEYWORDS: Online Voting, Authentication, Biometric, Security, Steganoghraphy.

I. INTRODUCTION

The algorithm uses image based steganographic and cryptographic system. The Steganography partis needed as we want to involve biometric identity to provide added security. Mostly, Steganography uses images as cover media because after digitalization images contain the quantization noise which provides space to embed data. The general model of Steganography says if you want to send some secret message then choose a cover image, find its redundant bits and replace these bits with data bits of message. The message can be easily extracted by doing the same operations on the other end. Least significant bit insertion is a common approach to embed information in a cover file. This process overwrites the LSB of a pixel value with a message bit. If we choose a 24-bit image as cover, we can easily store 3 bits in each pixel. Human eye will not be able 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 viable that we can't embed anybodys personal information in this manner. So what we can do is that, we can encrypt the message before embedding, or we can perform steganography providing strong encryption at the same time. The method can easily work with still images as it yields random outputs, in order to make steganalysis more difficult it can cipher the message in a more secure manner.Using Cryptography and Steganography at the same time, we try to provide Biometric as well as Password security to voter accounts. The scheme uses images as cover objects for Steganography and as keys for Cryptography. The key image is a Biometric measure, such as a fingerprint image.

II. RELATED WORK

In [1] other requirements of such a system could be viewed as authentication, scalability, speed and accuracy. Among these, authentication can be viewed as the most critical issue. As online voting is risky, it is difficult to come up with a system which is perfect in all senses. Once we are sure that a voter is genuine, we can easily address other issues like anonymity and tamper resistance. If other security is done well, electronic voting could be a great improvement over paper systems. Flaws in any of these aspects of a voting system, however, can lead to indecisive or incorrect election results. In [3] they include Punch Card Systems, Global Election Management System (GEMS) and Direct Recording Electronic (DRE). As these systems are stand alone systems, they lack in ability of voting from anywhere. That is why the actual notion of online voting is missing in those systems.Rest of the paper is organized as follows. In the next section basic methodology is explained in subsections namely cover image creation, secret key expansion using hashing, embedding algorithm, authentication algorithm and voter account maintenance. Finally, we conclude in

10.15680/ijircce.2015.0303107

the last section.The algorithm uses image based steganographic and cryptographic system proposed in [2]. The Steganography partis needed as we want to involve biometric identity to provide added security. Mostly, Steganography uses images as cover media because after digitalization images contain the quantization noise which provides space to embed data. In [7] Steganography is the art of hiding information in ways that prevent the detection of hidden messages. It includes a vast array of secret communications methods that conceal the message's very existence. These methods include invisible inks, microdots, character arrangement, digital signatures, covert channels, and spread spectrum communications. Steganography and cryptography are cousins in the spycraft family: cryptography scrambles a message so it cannot be understood while steganography hides the message so it cannot be seen. In this article the authors discuss image ?les and how to hide information in them, and discuss results obtained from evaluating available steganographic software. They argue that steganography by itself does not ensure secrecy, but neither does simple encryption. If these methods are combined, however, stronger encryption methods result. If an encrypted message is intercepted, the interceptor knows the text is an encrypted message. But with steganography, the interceptor may not know that a hidden message even exists. For a brief look at how steganography evolved, there is included a sidebar titled ”Steganography: Some History.”

III. SCOPE

Using Cryptography and Steganography at the same time, we try to provide Biometric as well as Password security to voter accounts. The scheme uses images as cover objects for Steganography and as keys for Cryptography. The key image is a Biometric measure, such as a fingerprint image. Proper use of Cryptography greatly reduces the risks in these systems as the hackers have to find both secret key and the template. The basic idea is to merge the secret key with the cover image on the basis of 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.

The scope of the project can be further broaded to:

1) Online Voting System for VidhanSabha
2) User Authentication using Finger Print Biometrics
3) Steganography using LSB to hide user Voting ID
4) Database Management

IV. SYSTEM DESIGN

Discription of the System Architecture and System Flow is :

- Every person in the country is first register for voting. So, our first step is the registration.
- At the time of registration each person give thumb impression for the security purpose by using Digital Persona Hardware.
- After doing this system provide to person a personal identification number(PIN) and secrete key is generated.
- By using Personal identification number and secrete key with thumb gives cover image.
- After that stego image is generated by using cover Image.
- The registered user login to the system for voting by entering PIN and secrete key with thumb impression.
- After login at the server side stego image will be decoded by using authentication algorithm.
- Decoding the stego image details of the voter are find from the database at the server side.
- If details are matched with the database stored then voter will be authenticated for voting and caste the vote.
- Finally result is generated.

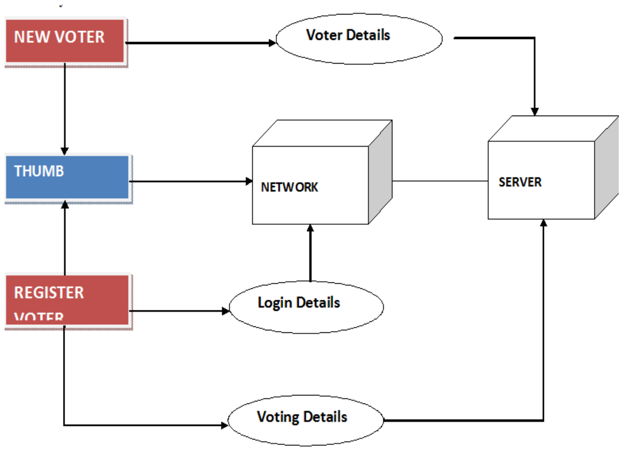


Fig. 1 System Architecture

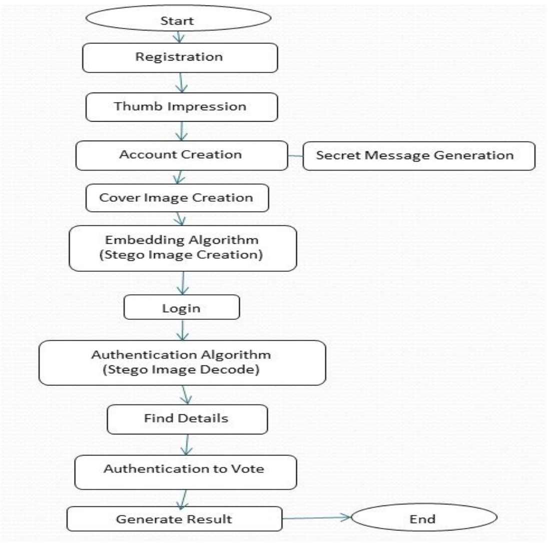


Fig. 2 System Flow

V. PROPOSED METHODOLOGY

A. Steps to acquire and Process :

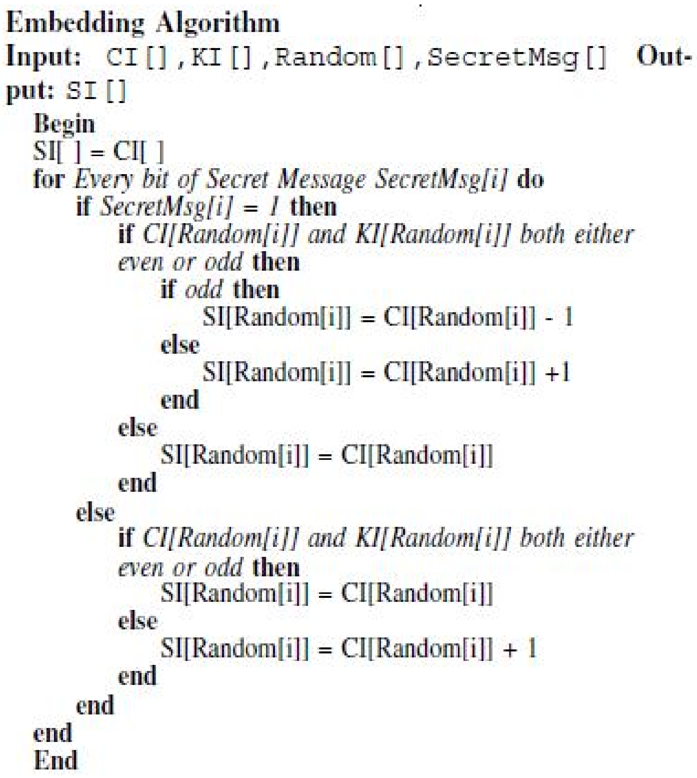
The embedding algorithm makes use of a stegocryptographic model. The model easily unifies cryptographic and steganographic models. It basically results as a steganographic one with the addition of a new element as the key image. It finally delivers cryptographic functionality while preserving its steganographic nature. The output of this embedding process is a stego image S and the inputs are expanded secret key concatenated with time-stamp, i.e. secret message, a cover image and the key image. In this embedding process we are going to modify the 256*256 pixels cover image given by the array CI[] of 3 □ 216 size. As we need to embed 288 bits of secret message into cover image by encryption, we need to determine the bytes of cover image which we are going to modify. These are determined by random function with secret key as seed. Here, we have array Random[] of size 288 with values ranging from 1 to 3 □ 216. Initially stego image array SI[] is same as that of cover image array CI[]. We have a key image array KI[] of 3 □ 216 bytes. So, in order to yield stego image S we are going to modify the array SI[] by the following embedding algorithm.

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. 3, Issue 3, March 2015



```
Embedding Algorithm
Input: CI[],KI[],Random[],SecretMsg[] Output: SI[]
  Begin
  SI[ ] = CI[ ]
  for Every bit of Secret Message SecretMsg[i] do
      if SecretMsg[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
              end
          else
              SI[Random[i]] = CI[Random[i]]
          end
      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
      end
  end
  End
```

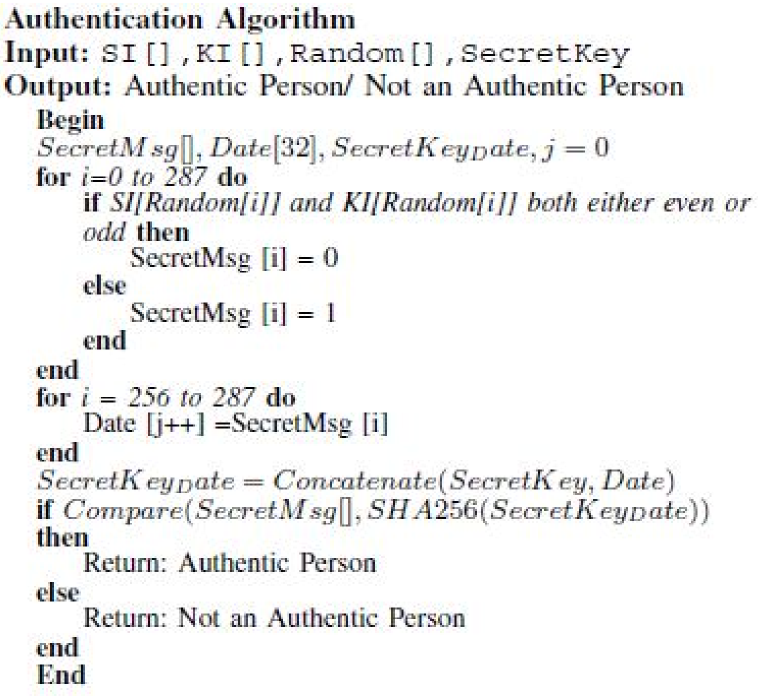
Both cover image and key image byte values are odd we are making stego image byte value one less than cover image byte value, else one more than that. If secret message bit is zero and both cover image and key image byte values are even or odd we are keeping stego image byte value same as cover image byte value, else one more than that. We should notice that during extraction we have to apply the same random function with the same seed. For example,
1) Cover image array of size 10: CI [] = {2, 32, 15, 16, 80,07, 92, 99, 51, 60}
2) Key image array of size 10: KI [] = {5, 12, 11, 07, 98,21, 28, 86, 24, 31}
3) Random array of size 5: RA [] = {2, 5, 7, 9, 10}
4) Scret Message of size 5 bits: SM [] = {1, 0, 1, 0, 1}
5) Initially, stego image, SI [] = CI []: SI [] = {2, 32, 15,16, 80, 07, 92, 99, 51, 60}
After modify SI using embedding algorithm, the result is showed in Table 1: From the above algorithm, final stego image is: SI [] = {2, 31, 14, 16, 80, 07, 92, 99, 51, 61}

TABLE I
YEILDING STEGO IMAGE

SM[i]	CI[Random[i]]	KI[Random[i]]	SI[Random[i]]
1	CI[2]=15	KI[2]=11	SI[2]=14
0	CI[5]=07	KI[5]=21	SI[5]=07
1	CI[7]=99	KI[7]=86	SI[7]=99
0	CI[9]=60	KI[9]=31	SI[9]=61
1	CI[1]=32	KI[1]=12	SI[1]=33

B. Interpret inputs for the project :

Now, from the matching entry in the voter database, we read the key Image and Secret key of that individual. The key to successful comparison is the time-stamp value. The timestamp (e.g. Date) delivers the security from replay attacks, so that the same stego image can not be used again in future. Using this secret key as seed we are generating the array Random[] of size 288. From the stego image we are forming the array SI[].



```
Authentication Algorithm
Input: SI[],KI[],Random[],SecretKey
Output: Authentic Person/ Not an Authentic Person
  Begin
  $SecretMsg[], Date[32], SecretKey_{Date}, j = 0$
  for i=0 to 287 do
      if SI[Random[i]] and KI[Random[i]] both either even or
      odd then
          SecretMsg [i] = 0
      else
          SecretMsg [i] = 1
      end
  end
  for i = 256 to 287 do
      Date [j++] =SecretMsg [i]
  end
  $SecretKey_{Date} = Concatenate(SecretKey, Date)$
  if $Compare(SecretMsg[], SHA256(SecretKey_{Date}))$
  then
      Return: Authentic Person
  else
      Return: Not an Authentic Person
  end
  End
```

In the above algorithm, we are checking bytes of stego image and key image, if both are odd or even we are taking the secret message as one otherwise zero. Using the Date value contained in the secret message and SecretKey we can verify the authenticity. Previous example is continued,
1) From the above embedding algorithm we have:
SI [] = {2, 31, 14, 16, 80, 07, 92, 99, 51, 61}
2) From Database we have:
KI [] = {5, 12, 11, 07, 98, 21, 28, 86, 24, 31}
Extraction of secret message is shown in Table II:

TABLE II
OBTAINING THE SECRET MESSAGE

KI[Random[i]]	SI[Random[i]]	SM[i]
KI[2]=11	SI[2]=14	1
KI[5]=21	SI[5]=07	0
KI[7]=86	SI[7]=99	1
KI[9]=31	SI[9]=61	0
KI[1]=12	SI[1]=33	1

VI. SIMULATION RESULTS

By analysing the Online Voting System is proposed with integrated Cryptography and Steganography. Failures are occur due to some lack of knowledge in using system, technical problems. This figure 3 shows the relation between numbers of voters versus number of voting.

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. 3, Issue 3, March 2015

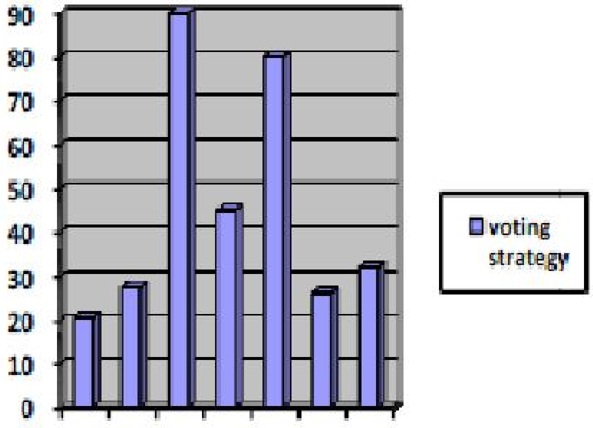


Fig. 3 Graphical Representation

In this System, 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 obtained. The information is secure. Other than the voter nobody can know the voting details. Process can be done quickly. It avoids 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. Result should be in correct manner and it is a real time vote system.

VII. CONCLUSION AND FUTURE WORK

In this document brief introduction to the project idea is given under the problem definition & scope heading. The main the interfaces, software functions and behavior of the project has been depicted in the Software Requirement Specification. The project plan deals with the project estimates, risk management & other management functions. The design details, including the software functionality, class, deployment and component diagrams along with the user interfaces have been documented in the High Level Design Document.Thus, the preliminary work required before project implementation has successfully been done and documented. This document would definitely help us to enhance the overall understanding of the project and help in the actual implementation of it.

REFERENCES

1. William Stallings, ”Cryptography and Network Security, Principles and Practices”, Third Edition, pp. 67-68 and 317-375, Prentice Hall, 2003.
2. Bloisi, D. and Iocchi, L., ”Image based Steganography and Cryptography”, In Proc. of 2nd Int. Conf. on Computer Vision Theory and Applications (VISAPP), pp. 127-134, 2007.
3. Dr.K.Kuppusamy1 Associate Professor Department of Computer Science Engineering Alagappa University Karaikudi 630 003 & K.Kavitha 2 M.Phil Scholar Department of Computer Science & Engineering Alagappa University Karaikudi 630 003 ,”Secure Electronic Registration & Voting System Based On Biometrics”, National Conference on Future Computing Volume 1, March 2012.
4. Staone, M.S. and Khandare, M.V., *“Image based Steganography using LSB insertion technique”*, IEEE WMMN, pp.146-151, January 2008.
5. A. K. Jain, A. Ross, and S. Prabhakar, "Fingerprint Matching Using Minutiae and Texture Features", *Proc International Conference on Image Processing (ICIP)*, pp. 282-285, Greece, October 7-10, 2001.
6. Prabha Susy Mammen and S. Ramamoorthy , ”A Novel Data Hiding Technique based Bio-Secure Online Voting System” , International Conference on Computing and Control Engineering (ICCCE 2012), 12 & 13 April, 2012.
7. Johnson, N. F. and Jajodia, S., ”Exploring steganography: Seeing the unseen”, IEEE Computer Magazine, pp. 26-34, February 1998.