Online Voting System Powered by Biometrics

Priya S [1], Tadepalli Sarada Kiranmayee [2], Vishnu Bhagavath [3], Pavan Teja [4], Ravi Theja [5], M.S.Sai Prakash [6]
[1, 2] Asst. professor, Department of Computer science & Engineering, SRM Institute of Science & Technology, Chennai, Tamil Nadu, India.
[3, 4, 5, 6] UG Scholars, Department of Computer science & Engineering, SRM Institute of Science & Technology, Chennai, Tamil Nadu, India.

Abstract – The secure online voting system is the need of today's era. We propose a new secure authentication for online voting system by using biometric feature and steganography. Voter is asked to enter a password at the time of registration. Password is converted into secret message using timestamp and hashing. This secret message is stored in image using steganography. In this model, a person can also vote from outside of his/her allocated electorate or from his/her chosen location.

Index Terms – Authentication, Biometric Feature, Steganography, online voting.

1. INTRODUCTION

Nowadays, election process plays a very important role in democratic country. The election is a process for selection of a perfect candidate who will lead the nation. In a democracy, people Choose their leader by giving their vote. Recently in India, electronic voting system is used. In this system, voter availability at in the city is compulsory. This is major drawback of electronic voting system. An online voting system is the solution as voter can vote from anywhere.

2. RELATED WORK

In [1], online voting system with secure authentication is described based on Shamir's secret sharing technique. Two shares of password are created. One is given to user and one is kept with authority. At the time of voting, shares are combined to generate original secret. Here, if voter himself gives his share to some other person then that person can cast vote instead of legitimate voter.

Author proposed web-based internet voting system [2], in that author justifies the protection to vote. Mainly security is needed when vote travel from voting client to voting server. Author strong tools are the concept of number of encryption and decryption. A novel security for the online voting system by using multiple encryption schemes is proposed. This paper uses encryption and digital signature. Vote is encrypted and then voter signs the vote using digital signature. This is major problem with system as vote is linked with user signature. Also, for authentication only login and password is used which is transferable credentials.

Author explained [3] numerous passive and active attacks over the computer networks. Also, author presents stages of the attacks as well as strategy used to penetrate a network. Author has taken care form several threats in view of network administrator and additionally need of applying appropriate network security policy. In initial phase of attack detection is

crucial for the detection strategy. Several times attack is detected but the hacker is rests unidentified. Analyst takes several times to identify strategy of the attack.

3. EXISTING SYSTEMS

In current voting system, a voter is required to go to voting booth. After verification with some IDs, the voter is allowed to vote. The voter is then allowed to enter into Electronic Voting Machine(EVM) sections which allow a single vote. Once you pressed the button, you cannot vote again. However, this system must also be anonymous. The system must identify that voter can vote without revealing their actual identity and voter must be assured about it. Existing systems are as follows

- Ballot Box
- Electronic voting machine

3.1 Ballot Box:

A ballot box is a temporarily sealed container, usually a square box though sometimes a tamper resistant bag, with a narrow slot in the top sufficient to accept a ballot paper in an election but which prevents anyone from accessing the votes cast until the close of the voting period. This is paper-based voting system originated as a system where votes are cast and counted by hand, using paper ballots. Since the casted votes are counted by hand this method requires more time to announce the results.

Fig1: Ballot Box

3.2 Electronic Voting Machine:

An EVM consists of two units, control unit and balloting unit. The two units are joined by a five-meter cable. Balloting unit facilitates voting by voter via labelled buttons while control unit controls the ballot units, stores voting counts and displays the results on 7 segment LED displays. There is provision for 16 candidates in a single balloting unit and up to a maximum of 4 units can be connected in parallel. The conventional ballot paper/box method of polling is used if the number of candidates exceeds 64. The main drawback of EVMs is that it can record a maximum of 3840 votes and can cater to a maximum of 64 candidates.

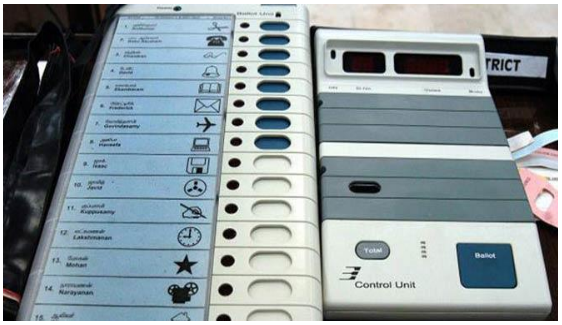

Fig 2: Electronic Voting Machine

Disadvantages of Existing System

- Fake registration.
- There is a chance to do revote.
- Less security.
- Need to go to polling booths.

4. PROPOSED SYSTEM

Our objective is to present a high-level overview of fingerprint sensing and matching technology so as to provide high security to voting system. Using Cryptography and Steganography at the same time, we try to provide Biometric as well as Password security to voter accounts.

In our online voting system, there are four modules.

- Voter registration
- Authentication
- Vote casting and recording
- Vote Counting

4.1 Voter Registration:

In voter registration phases, voter will provide personal information and fingerprint which is biometric information. After registration, user is allowed to vote at the time of the election.

In registration module following steps are involved:

- First authenticated officer logs in into system and starts voter registration.
- Officer takes Registration details of voter like Name, Age, and DOB. Etc.
- Officer asks the voter to give fingerprint. Fingerprint scanner is used to scan finger print.
- Officer directs voter to enter PIN.

Our proposed work is a mixture of steganography and biometric security. By using various types of cover media like image, audio and video, we can hide secret data. In our work, image steganography is used to hide secret data. This image is used as a cover image.

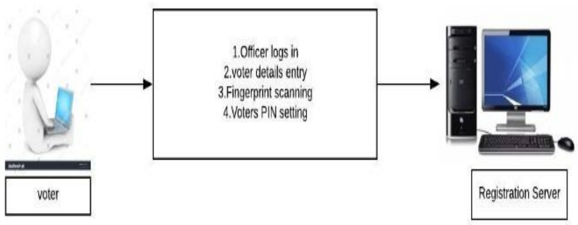

Fig 3: Voter registration module

In the background following steps are executed:

Every voter has been assigned a unique identification number (UIN). Voter's data given at the time of voting is stored against UIN. The process of generation of secret message is shown in Figure 4. Four-digit PIN is represented using 16 bits. Current time stamp value is represented using 32 bits. Both are concatenated. Then, we will apply SHA256 algorithm. This will give 256-bit hash code. Then, this hash code of 256-bits and time stamp value of 32 bits are concatenated to generate a secret message of size 288-bits.

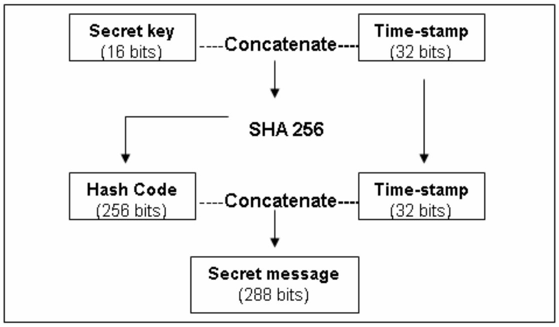

Fig 4 Generation of Secret Message

Cover image and key image shown in Figure 5 are used to generate stego image. User fingerprint is used as key image.

Fig 5 Cover image & key image

Secret message of size 288-bits is hidden in cover image with the help of key-image. This will give us stego image. The embedding algorithm given in [4] is used to embed secret message into cover image.

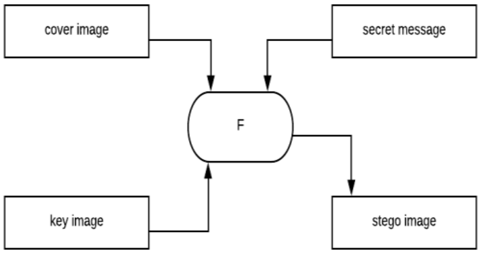

Fig 6: Stego Image Generation

4.2 Authentication module:

At the time of voting, voter has to pass through authentication phase. If he is authentic voter then he will be allowed to vote.

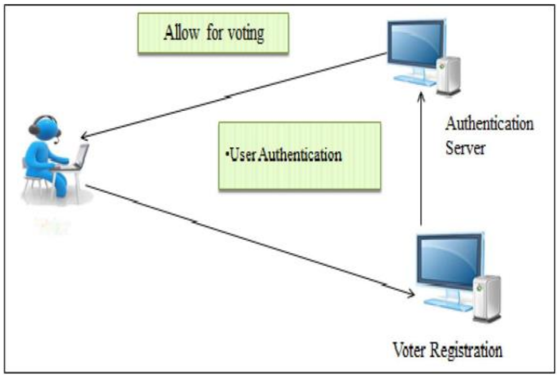

Fig 7: Authentication Module

At the time of voting, voter first login and his credential are checked by the system to verify if the voter is authentic or not. If authentication is successful, then allow the voter for voting. The decoding algorithm is used to decode 288-bits secret message. Fingerprint of voter is used in decoding algorithm. Extraction of secret message from stego image is shown in figure 8.

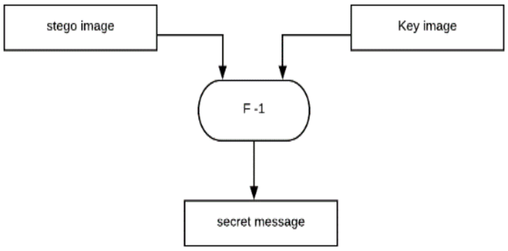

Fig 8: Extraction of secret message

Biometric security and steganography both are used at the same time to provide strong authentication. In this phase, voter is asked to enter four-digit PIN. It is then represented using 16-bits binary number. In the secret message of 288 bits, first 256 bits are hash code and last 32 bits are time stamp value. 16-bits binary number PIN entered by voter is concatenated with time stamp value. Now we will apply SHA 256 to generate hash code. The generated new hash code and retrieved hash code from stego image are compared. If both are equal, then the person is allowed to vote otherwise not. This authentication process is shown in figure 9.

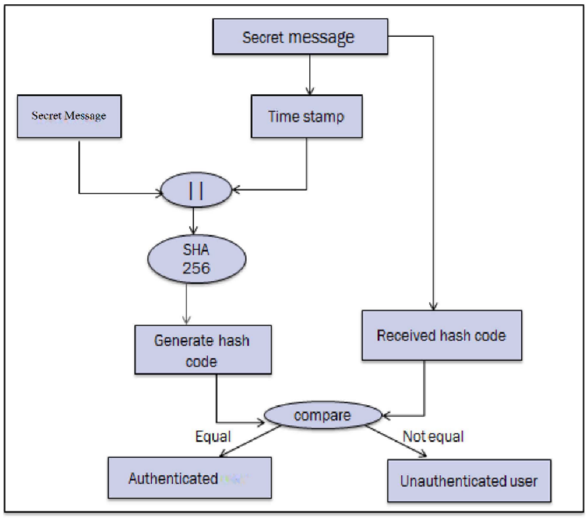

Fig 9: Authentication of Voter

4.3 Vote-recording and casting module:

Following steps are involved in vote recording and casting module

- After successful authentication, a ballot is displayed.
- Voter cast their vote by selecting one of the
- candidates.
- This vote is encrypted and stored in database located at voter recording and casting server.

4.4 Vote Counting:

After voting time is finished, no one is allowed to vote. Now votes are counted by the system and result is displayed. Votes stored in database can be counted Automatically and displayed by writing simple sql quires.

Advantages of Proposed System

- Highly secured and there is no chance to revote.
- Real time tracking of results.
- Ease of voting.
- Vote from anywhere.

5. CONCLUSION

In this paper we have presented a method for integrating cryptography and steganography to biometrics. The strength of our system resides in the new concept of key image. We are also able to change the cover coefficients randomly. This strategy does not give any chance to steganalytic tools of searching for a predictable set of modifications. Also, Considering the complexity of elections, we have provided sufficient proof of authenticity of an individual in form of both biometric measures and secret key. As future work, we will be trying to improve two considerable aspects of the algorithm, namely, speed and dependence on pseudo random function.

REFERENCES

[1] Ashwini Walake, Prof. Ms, Pallavi Chavan," Efficient Voting system with (2,2) Secret Sharing Based Authentication", (IJCSlT) International Journal of Computer Science and Information Technologies, Vol. 6 (1), 2015, 410-412

[2] Prof. S.M. Jambhulkar, Prof. Jagdish B. Chakole, Prof. Praful. R. Pardhi, ”A Secure Approach for Web Based Internet Voting System using Multiple Encryption”, 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.

[3] Ass. Prof. Ion Tutănescu, Prof. Emil Sofron, “Anatomy and Types of Attacks against Computer Networks”, Department of Electronics and Computers, University of Piteşti, ROMANIA 2012.

[4] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A, Barbhuiya, Sukumar Nandi, "Online Voting System Powered By Biometric Security Using Steganography" Second International Conference on Emerging Applications of Information Technology,2011.