ISSN: 2321-7782 (Online)
Volume 1, Issue 7, December 2013
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

Online Voting System Powered by Biometric Security using Cryptography and Stegnography

Mayuri U. Chavan[1]
B.E.Comp
Department of Computer Engineering
Jaihind College of Engineering, Kuran
Pune - India

Priyanka V. Chavan[2]
B.E.Comp
Department of Computer Engineering
Jaihind College of Engineering, Kuran
Pune - India

Supriya S. Bankar[3]
B.E.Comp
Department of Computer Engineering
Jaihind College of Engineering, Kuran
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. Thus we plan to make the voting process a secure & effective.***

Keywords: Online Voting, Cryptography, Stegnography, Biometric.

I. INTRODUCTION

Electronic voting system, that have security context or known as e-trusted voting system. In this study, the prototype builds based on secured and trusted framework for electronic voting. The System allows the voters to participate by using username and password. Voter can enter the system and votes on the existing text during election date and the voter can see the result after the end of election date. e-voting is the process of using computerised systems in statutory elections, both to cast and count votes (e-counting). e-voting and e-counting open up elections to risks of fraud on a much greater scale than paper and pencil-based systems. Current technology means that e-voting cannot deliver transparent, verifiable and anonymous elections.

The application would basically provide online support for voting, thus simplifying the voting process. The domain area of this project basically is Biometrics Finger Print Recognition. It deals with one part of the human body unique to each and every individual on earth. Every individual on earth has a different set of fingerprints, even identical twins carry different sets of prints. This project exploits this uniqueness of the human race to store, match and compare one fingerprint to another and to determine whether the two fingerprints in question match or not. It uses the Finger Print Recognition to mainly assist the physically impaired people of India. The interactive audio would guide the voter through the entire voting process and in turn recognizes his response caste his or her vote for a particular party.

II. CRYPTOGRAPHY

Most people are concerned with keeping communications private. Encryption means the transformation of data into some unreadable form. The purpose of it is to ensure privacy by keeping the information hidden from anyone for whom it is not intended. Decryption is the reverse of encryption; it is the transformation of encrypted data back into some readable form. Encryption and decryption require the use of some secret information, usually referred to as a key. The data to be encrypted is called as plain text. The result of encryption process is encrypted data is called as cipher text. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, for other mechanisms, the keys used for encryption and decryption might be different.

A. Types of Cryptographic algorithms

There are various types of Cryptographic algorithms. They are categorized based on the number of keys that are employed for encryption and decryption the three types of algorithms are listed as follows:

a) *Secret Key Cryptography (SKC)*: Single key is used for both encryption and decryption. The most common algorithms in use include Data Encryption Standard (DES), Advanced Encryption Standard(AES).

b) *Public Key Cryptography (PKC):* One key is used for encryption and another for decryption. . RSA (Rivest, Shamir, Adleman) algorithm is an example.

c) *Hash Function:* Uses a mathematical transformation to irreversibly "encrypt" information. MD (Message Digest).

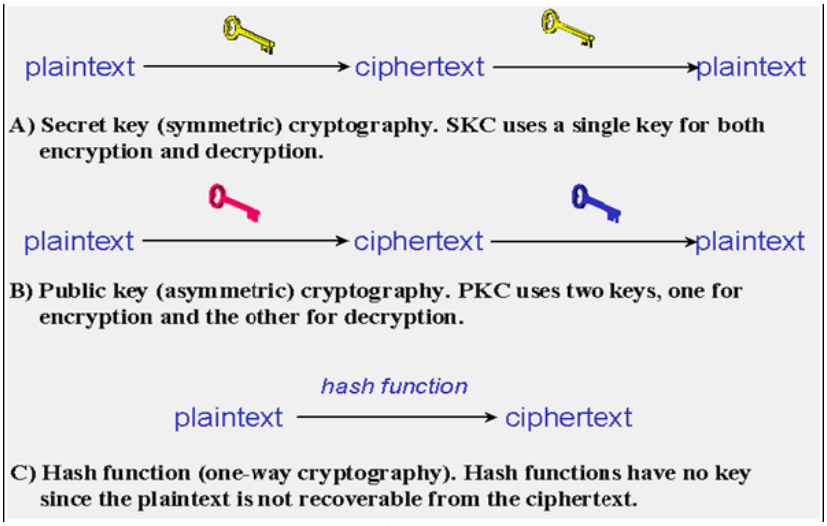

Fig. 2.1: Types of Cryptographic algorithms

III. STEGNOGRAPHY

Stegnography is the art and science of concealed communication. The basic idea is to embed important data in a standard cover object as image to form the stego-image. The stego-image is stored and transmitted to the receiver in the same way as the cover object. To unintended observers, the stego-image exhibits the content of the cover object. However, from the designated receiver's viewpoint, the stego-image carries important data under the camouflage of the cover object that can be revealed using the corresponding extraction algorithm. Unlike encryption techniques in which the important data are protected by the unread ability of the cipher text, the main idea of stenography is to conceal the very existence of the important data.

The advantages of using a method that conceals the important data are that it also prevents an observer from selectively blocking the transmission of such data. Moreover, in contrast to a watermarking system in which the embedded data tend to be related to the cover object, the information carried in the stego-image tends to be independent of the cover object-one crucial principle in designing a stegnography algorithm is maintaining the imperceptibility of the important data. Stegnography is the art of hiding information in ways that prevent the detection of hidden messages. Stegnography, derived from Greek, literally

means "covered writing." 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. Stegnography and cryptography are cousins in the spycraft family. Cryptography scrambles a message so it cannot be understood. Stegnography hides the message so it cannot be seen. A message in cipher text, for instance, might arouse suspicion on the part of the recipient while an "invisible" message created with stegnographic methods will not. The data to be encrypted is called as plain text. The encrypted data obtained as a result of encryption process is called as cipher text. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different. Servers are often dedicated, meaning that they perform no other tasks besides their server tasks. On multiprocessing operating systems however, a single computer can execute several programs at once. A server in this case could refer to the program that is managing resources rather than the entire computer.

IV. Statement of Scope

A. *Major Inputs*

Our central server would contain the database for each every voter. Whenever the voter comes to give away his/her vote, 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 caste his vote successfully. In case of Finger Print Based voting the system would prompt the voter for the party names firstly. 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 he can caste his/her vote to a Candidate of the given party.

B. *Processing Functionality*

The fingerprint of the voter is send to the server for processing. The image taken from the scanner would be encrypted in a specific format then it would be send to the server for further processing. At the server end this image would be decrypted the original template of the image would be obtained, all the processing on the image would be done at the server like extracting the main points in the image from which it would be differentiated from the other, storing the key features of the image like color of the image, its shape, brightness etc. 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.

C. *Outputs*

When the image is processed by the server the server would allow the voter to caste his vote if his fingerprint matches with the image template in the database otherwise he won't be allowed to do the same.

V. System Features

A. *System Architecture*

Every individual in country is first register for voting. So, our first step is registration. At time of registration each person gives his full name, ward name, address and contact no, email-id etc. and register. After doing this system provide PIN and SK to person. He gives his thumb impression. After that the login process takes place. If voter is already register then directly login process take place. At login process he enters his PIN SK which is assign to him at time of registration. Voter can cast their vote from anywhere where internet access is there. After login stego image encode the SK PIN which is in encrypted form. This image is send to server. At server side decoding is take place verification of PIN SK is done. If PIN SK is valid then server sends the thumb template to the client. At client side it receive thumb template, compare this thumb template with voter thumb template. If both are match then system gives permission to voter for voting. Finally result is generated on website.

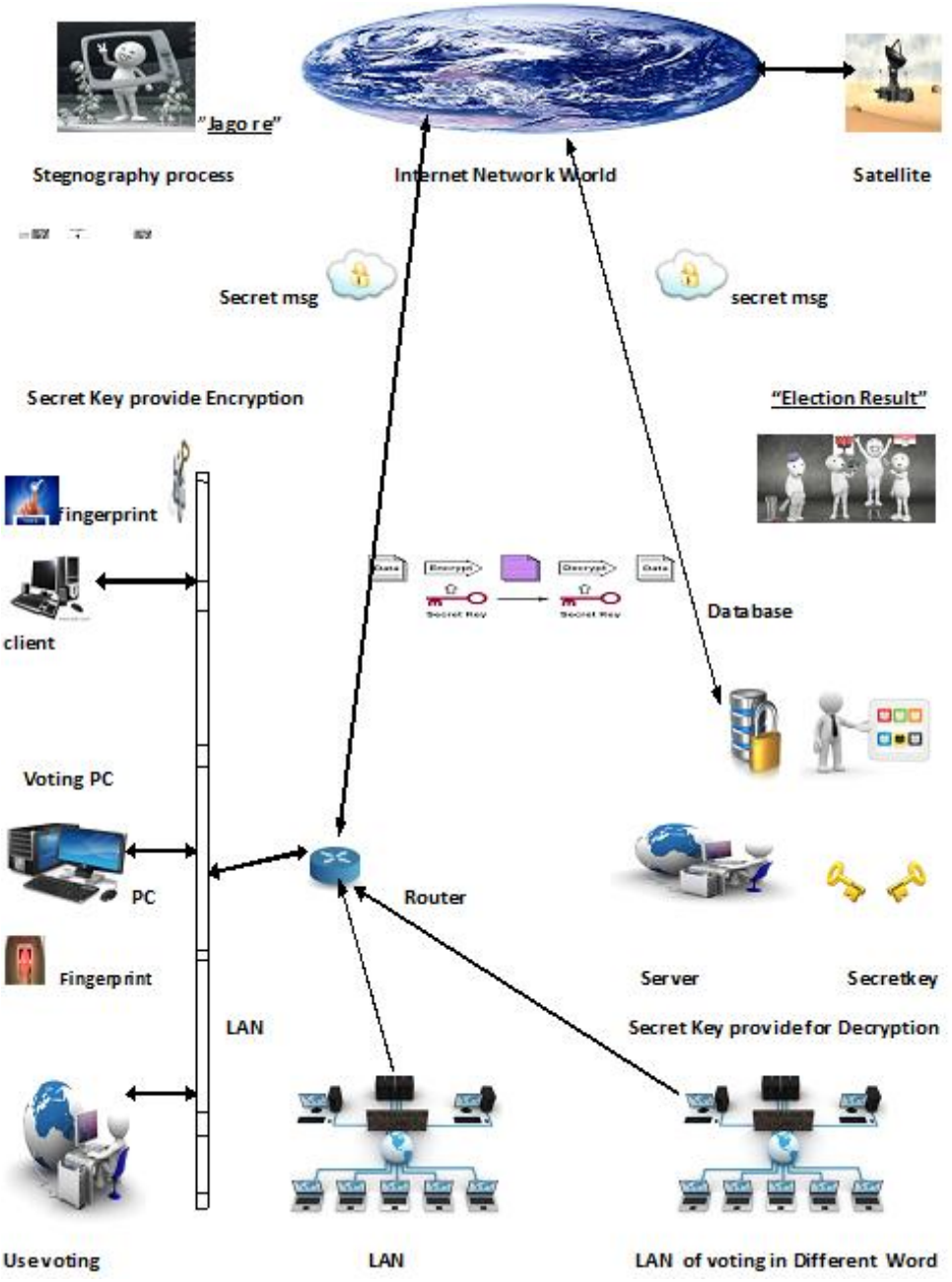

Fig. 5.1: e-voting Architecture

B. Cryptography

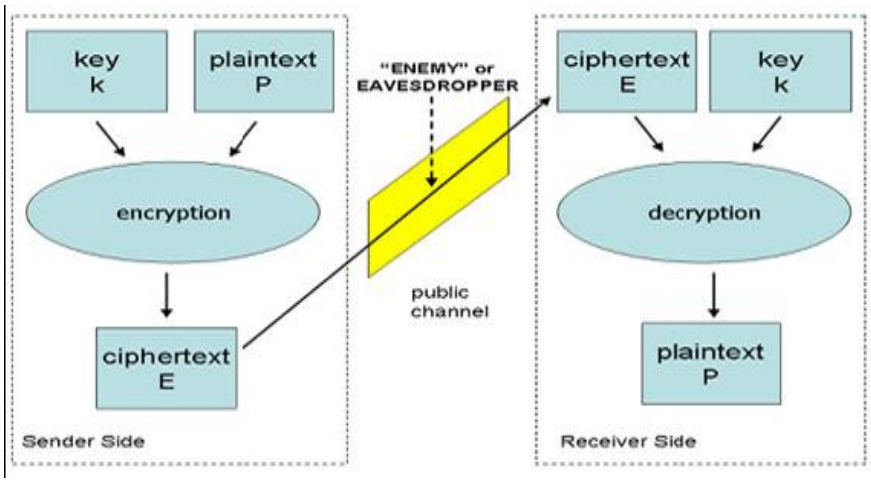

Fig. 5.2: Cryptography

The science of securing data communication is cryptography. By cryptography confidential information can be stored and transmitted across insecure networks in manner such that unauthorized person cannot read the information except the authorized recipient. Cryptographic objectives encompass using mathematical techniques to all aspect of Information security from confidentiality, entity authentication and origin authentication and data integrity. Usually the sender A sends secret message to the intended receiver B, over a communication line which may be tapped by an adversary. Cryptography encompasses many problems including authentication, encryption, key distribution, and decryption. The traditional solution to these problems achieved through Private key Encryption (PKE).

C. Stegnography

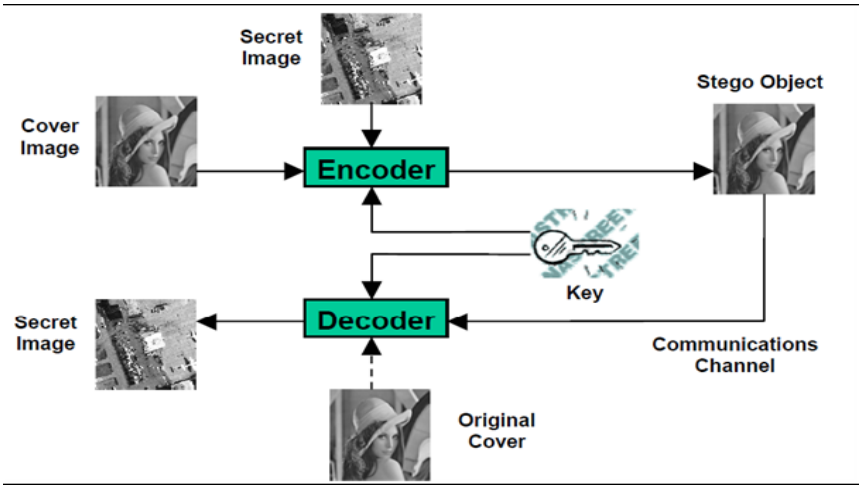

Fig. 5.3: Stegnography

Stegnography is the science of concealed digital information within electronic files like image, sound, an article, a shopping list such that no-one determines that the hidden communication is taking place. The technique secure data by obscuring and embedding the content in another media called carrier in which the information is saved for transmission. The technique of data security by simple encryption is not sufficient anymore as technology of Super Information Highway evolves.

VI. ADVANTAGES

a) An electronic voting system can be involved in any one of a number of steps in the setup, distributing, voting, collecting, and counting of ballots, and thus may or may not introduce advantages into any of these steps.

b) An electronic voting system can be involved in any one of a number of steps in the setup, distributing, voting, collecting, and counting of ballots, and thus may or may not introduce advantages into any of these steps.

c) Potential disadvantages exist as well including the potential for flaws or weakness in any electronic component.

d) Server operates Automatically, No need to handle to person.

VII. APPLICATIONS

a) Engineering research in E-voting Technology.
b) After the user voting SMS from server to user voting successfully done.
c) Constitutional Court.

VIII. CONCLUSION

A. *Concluding Remarks*

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 random cover image generation for each voter. Thus, the citizens can be sure that they alone can choose their leaders, thus exercising their right in the democracy.

B. *Future Work*

Create the e-voting system usable for handicap people by using the eye retina or voice, etc.

References

1. "Cryptography and Network Security: Principles and Practice" by William Stallings Book Name: Cryptography and Network Security, Edition: Fourth Edition. Last updated: Thursday, June 3, 2010.
2. "Cryptography and Network Security" by Atul Kahate Tata McGraw-Hill Education, Published Year: 07-Sep-2008
3. An Efficient Online Voting System http://www.ijmer.com/papers/Vol2
4. Online Voting System Powered By Biometric Security Using Stegnography 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 Stegnography.pdf
5. Secure Online Voting System Proposed By Biometrics and Stegnography
6. A Biometric-Secure e-Voting System for Election Processes http://www.sundaychennai.com
7. E-Voting System http://www.vvk.ee/public/dok/Yldkirjeldus eng.pdf
8. A Survey on Voting System Techniques http://www.ijarcsse.com/docs/papers/Volume 3/1 January2013/V3I1-0221.pdf
9. Analyzing Internet Voting Security http://www.cs.berkeley.edu/daw/papers/cacmserve.pdf
10. Proposal of a new online voting system http://easyvote-app.sourceforge.net

AUTHOR(S) PROFILE

Miss. Mayuri U. Chavan, currently pursuing her B.E degree in Computer Engineering from Jaihind College of Engineering, Kuran (Pune University, Pune). Also received the Diploma in Information Technology from Shivneri Polytechnic,Khanapur(MSBTE) in 2011.

Miss. Priyanka V. Chavan, currently pursuing her B.E degree in Computer Engineering from Jaihind College of Engineering, Kuran (Pune University, Pune). Also received the Diploma in Information Technology from Shivneri Polytechnic,Khanapur(MSBTE) in 2011.

Miss. Supriya S. Bankar, currently pursuing her B.E degree in Computer Engineering from Jaihind College of Engineering, Kuran (Pune University, Pune). Also received the Diploma in Information Technology from Pimpri chinchwad polytechnic,akurdi(MSBTE) in 2011.

