IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

E-Voting System using Visual Cryptography & Homomorphic Encryption

Ruchita Tekade[1], Prof. Reena Kharat[2], Varsha Magade[3], Marjina Shaikh[4], Pallavi Mendhe[5]

Department of Computer Engineering, Pimpri Chinchwad College Of Engineering, Pune, India[1,2,3,4,5]

Abstract: Election is a process of establishing a democracy in the country. This process should be ensured to maintain the integrity and confidentiality of the vote casted and the authentication before citizens of particular country casts their votes [1]. It is very important to provide security to voting system. In this paper we provide security to voting system with secure user authentication[7] by providing biometric fingerprint to voter. In this system user has to enroll his/her finger print for voter ID card[1]. Finger print scanner will create image for that finger print. Share construction algorithm will be used to construct two shares of finger print image. One share[6] will be stored in database and another share will be stored in voter's ID card[1] (VIC). Here database & voter's ID card don't contain actual image of fingerprint. Unless and until both shares are available, original fingerprint image[6] cannot be reconstructed. Fresh and reconstructed fingerprint image are compared. If they match then voter is authentic as he/she claimed. As voter is authentic so he/she will cast the vote. After casting homomorphic encryption[2] is applied and results get counted. It makes election procedure to be secure against a variety of fraudulent behaviors.

Keywords: Authentication, Homomorphic encryption, Secret Sharing scheme, Visual Cryptography.

I. INTRODUCTION

E-Voting solutions generally aim at increasing participation, improving the outcomes elections by addressing challenges associated with traditional voting practices. The notion of e-voting in this paper refers to the use of technology to support one or more of the major phases of the electoral process - from registration stage in the pre-voting phase to voting/balloting and verification to counting or tallying after voting [2], [3].Also, the rapid growth of authentication systems has changed the view of people toward the way these systems deal with. Providing security to voting system is an important issue in real life. This model helps in achieving the authenticity, non-traceability of vote cast and security with confidentiality also being enforced. This is handled in the e-voting system by combining biometric with visual cryptography[4]. Biometrics deals with computerized methods of certifying the identity of a person based on physiological or behavioral characteristics. In this paper, different approaches are discussed for authentication and vote casting while fulfilling privacy requirements of voting and their results are compared.

II. LITERATURE SURVEY

1. Voter's Registration and Authentication

Each voter has to enroll to exercise voting rights. Everyone in the world has unique fingerprint. Fingerprint scanners will be used to scan fingerprint of each voter. Secret sharing algorithm[6] is used in voter enrollment and authentication module. It consists of 2 parts: share construction and secret reconstruction. Share construction algorithm will be used to construct two shares of finger print image[6]. One share will be stored in database and another share will be stored in voter's ID card (VIC). Here database & voter's ID card don't contain actual image of fingerprint. Unless and until both shares are available, original fingerprint image cannot be reconstructed. Each voter will have voter's ID card (VIC) which contains voters private information and one share of his/her fingerprint[6]. In Authentication, voter has to provide VIC which contains share of finger print image. Card reader will read share from VIC. The shares from VIC and database are given to secret reconstruction algorithm[6] and fingerprint image is reconstructed. Fresh fingerprint image is taken at time of authentication from the voter through fingerprint scanner. Fresh and reconstructed fingerprint image are compared. If they match then voter will be authenticated for voting as he claimed. Otherwise voter will not be allowed to vote.

A. Visual cryptography

Moni Naor and Adi Shamir [4] Visual cryptography, Visual cryptography is introduced first in 1994 by Naor and Shamir .Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system[4], without the aid of computers.

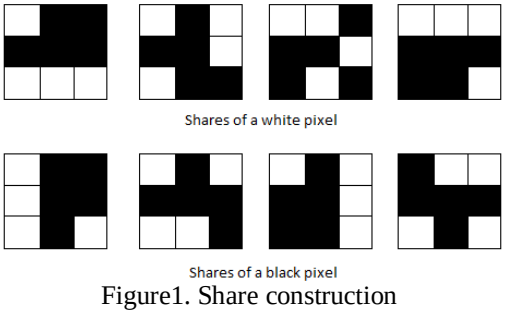

Figure1. Share construction

Visual cryptography scheme[4] eliminates complex computation problem in decryption process, and the secret

DOI 10.17148/IJARCCE.2016.5168

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement. Naor and Shamir[4] this encoding scheme to share a binary image into two shares Share1 and Share2.

B. Implementation of Authenticated and Secure Online Voting System

Srivatsan Sridharan [5] introduces Authenticated and Secure Online Voting System. All eligible voters having a Universal Identification Number of their country (For Example the Smart Card in USA) is allowed to cast their respective vote.

Three phases -: voter registration, online vote capturing and the instant online counting[5] and result declaration. A Secret Voting Password provided to voter during registration acts as an authentication mechanism which enables the voters to securely cast their vote along with their captured biometric identification[5]. Card is the primary requirement of this system in avoiding the multiple votes to be cast by any individual.

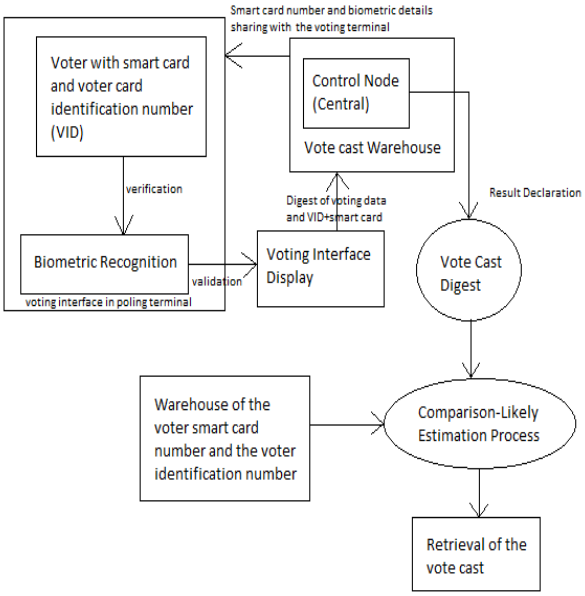

Figure 2. Architecture of Online Voting Model.

C. Web based secure e-voting system with fingerprint authentication

The elections that are made by using traditional methods[3] are no longer preferred because of the long period of preparation, fake voting, faulty voting, mistakes made in counting the votes, long period of counting and high cost of voting process.

In order to avoid these disadvantages affecting directly the economy and policy of the country, it is obligatory to carry the available voting system to an electronic system[3]. In this study, an electronic voting system, E-voting[3] for a general election is developed and fingerprint authentication based e-voting system is applied. As a result, security of the voting system is greatly improved by using biometric authentication system[3].

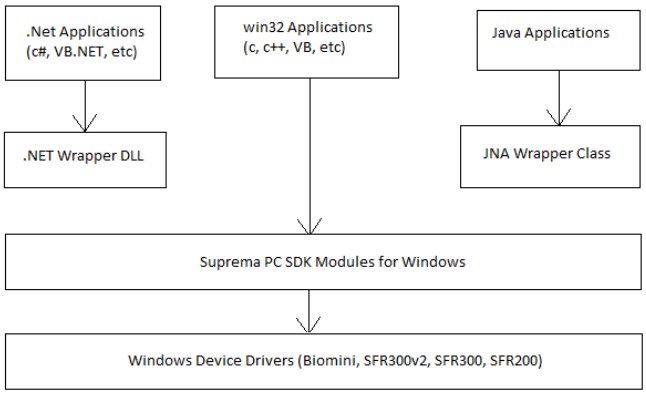

Figure 3. General structure of fingerprint device programming.

2. Votes casting and result

If voter authenticated then voter will allowed to vote as he/she claimed, or if not authentic then not allowed to vote. Initially all bits are set to 0. As voter selects one candidate bit get set to 1. With the help of homomorphic encryption system[9] overcome problem of falsifying results. The experimental results show high accuracy and high security of implemented system.

A. *A Fully Homomorphic Encryption Scheme With Better Key Size*

Fully homomorphic encryption[10] is faced with two problems now. One is candidate fully homomorphic encryption schemes are few. Another is that the efficiency of fully homomorphic encryption is a big question. In this paper, a fully homomorphic encryption scheme based on LWE [10] is proposed, which has better key size. So we can use this technique in our voting system to improve integrity of votes given by authenticated voters. The learning with errors (LWE)[10] problem was introduced by Regev as a generalization of the well-known "learning parity with noise" problem, to larger moduli. The goal of this paper is to construct a FHE[10] scheme with better key size. The smaller key come from the different style of the basic encryption scheme and we can choose secret key from binary set.

B. *A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption*

In this paper, a hybrid homomorphic encryption[9] is introduced. That combines public-key encryption (PKE)[9] and somewhat homomorphic encryption (SHE)[9] to reduce the storage requirements of most somewhat or fully homomorphic encryption (FHE) applications. In this model, messages are encrypted with a PKE[9] and computations on encrypted data are carried out using SHE or FHE after homomorphic decryption[9]. The concept of computation on encrypted data without decryption was first introduced by Rivest, Adleman and Dertouzos in 1978. To enhance the performance of the hybrid scheme, we must evaluate a modular exponentiation by a secret exponent efficiently.

C. *Secure Image processing using LWE Based Homomorphic Encryption*

The paper proposes the practical implementation of Image processing operations on encrypted images[7] which are

stored in the cloud or transmitted over unsecured channel, using LWE based Homomorphic encryption[7] scheme. LWE scheme is proved to be amazingly versatile and secured and well suitable for Homomorphic encryption. LWE[7] based Homomorphic encryption is implemented to explore the operations on encrypted binary/gray scale image.

III. COMPARITIVE STUDY

Electronic Voting is an often seen as tool for making the electoral process more efficient and for increasing trust in its management. Secure authentication[7] and registration are ensuring that the principle of universal and equal suffrage, summarized as "one Voter : One Vote ".

The integrity of votes is handled by the homomorphic encryption technique which is easier to implement in practical world than any other technique. The authentication of the voter is the main phase in voting system that is done by visual cryptography method. Visual cryptography[4] is the technique in which shares of the original image are created so that no one can access ones personal information. Thus we can say that visual cryptography and homomorphic encryption methods[2] are efficient methods to secure current voting system.

IV. SUMMARY AND CONCLUSION

In the field of electronic voting has been growing as countries globally are exploring methods to increase election's accuracy, and transparency. The possibility of two users having the same identification features[1] in the biometric system is virtually zero. Two-factor authentication could drastically reduce the incidence of identity theft, and other fraud, as the password would no longer be enough to give a secure access to their information. The problem of falsification will be overcome because authorization will succeed only when user will provide its ID card[1] with fresh fingerprint. Security and privacy is enhanced by preserving biometric shares at different places like smart card and database instead of whole data at same place. With the help of homomorphic encryption system[9] overcome problem of falsifying results. The experimental results show high accuracy and high security of implemented system. Secure authentication[7] and registration are ensuring that principles of universal and equal suffrage, summarized as "one voter: one vote".

REFERENCES

[1] A. Ojo, A. Adeshina, and C. Ayo, "Electronic VotingID: Lessons and Guide for Developing Countries", in 6th European Conference on e Government (ECEG 2006), Philipps Universitat Marburg, germany 27-28 April 2006, 2005, no. Bannister, pp. 303-311.

[2] K. Sampigethaya and R. Poovendran, "A framework and taxonomy for comparison of electronic voting schemes", Comput. Secur., vol. 25, no. 2, pp. 137-153, Mar. 2006.

[3] *Adem Alpaslan ALTUN and Metin BĐLGĐN,"Web based secure e-voting system with fingerprint authentication", Scientific Research and Essays Vol. 6(12), pp. 2494-2500, 18 June, 2011.*

[4] Moni Naor and Adi Shamir, "Visual cryptography", In Proceedings of the advances in cryptology Eurocrypt 1-12,1995.

[5] Srivatsan Sridharan, "Implementation of Authenticated and Secure Online Voting System", 4th ICCCNT 2013 July 4 - 6, 2013

[6] Rajeswari Mukeshi, V.J.Subashini "Fingerprint Based Authentication System Using Threshold Visual Cryptographic Technique", IEEE-International Conference On Advances In Engineering, Science and Management (ICAESM -2012) March 30, 31, 2012

[7] Ratna Kumari Challa, G. Vijayakumari, Sunny B, "*Secure Image processing using LWE Based Homomorphic Encryption*", 978-1-4799-608S-9/1S/$31.00©2015 IEEE.

[9] Jung Hee Cheon and Jinsu Kim, "*A Hybrid Scheme of Public-Key Encryption and Somewhat Homomorphic Encryption*", IEEE Transactions On Information Forensics And Security, Vol., 10, No. 5, May 2015.

[10] CHEN Zhigang, WANG Jian, ZHANG ZengNian, SONG Xinxia, "A Fully Homomorphic Encryption Scheme with Better Key Size", China Communications· September 2014.