

Secure Authentication and Tamper Detection in Remote Voting System

P. Sanyasi Naidu* and Reena Kharat*,**

ABSTRACT

In democratic country, all eligible citizens chose their government through voting. An online voting system is today's need. We have addresses issues in identification, authentication, confidentiality and integrity in the remote voting system. Password and biometric features based authentication is proposed in this paper. Confidentiality to the biometric database is provided by XOR based recursive visual cryptography and invertible XOR property. Confidentiality of the password is provided by using cryptography and steganography. Tampering of data is checked using hash code.

Keywords: Security; Authentication; Biometrics; Steganography; Online Voting; XOR-based Visual Cryptography;

1. INTRODUCTION

A secure remote voting system is need of today. Important security considerations in a remote voting system are trustworthy secure authentication with confidentiality to the registration database.

Following are security considerations given by NIST for remote voting system.

- Identification and Authentication - An unique identity provided by voter to get identified in the registration database uniquely. In authentication, the user provides credentials to the system which are verified to establish trust in user identity.
- Confidentiality - System must store registration data such that even someone get access to it cannot understand the data.
- Integrity – System must ensure the data used during authentication is same as the data given at the time of registration.

Authentication is provided using a password and biometric features. Confidentiality to the database is provided by XOR based recursive visual cryptography and steganography. Integrity is provided using hash code.

2. RELATED WORK

Our research focuses on issues in registration and authentication module of the online voting system. In [1] and [2], login ID and PIN/password have been used which are transferable credentials. One can transfer these credentials to another and another person can cast a vote instead of authorized voter.

Biometrics is biological characteristics which identify the person uniquely. Biometric credentials are non-transferable from one person to another. In [13], authors have used fingerprint is used for authentication. In [15], fingerprint and password are used during authentication. Fingerprint image is stored in the smart card of voter and registration database. The drawback of this system is the live fingerprint of the voter is not

* Department of Computer Science and Engineering, GITAM University, Vishakhapatnam, India, *Email: snpasala@yahoo.com*

** Department of Computer Engineering, Pimpri Chinchwad College of Engineering Pune, India, *Email: reenakharat@gmail.com*

taken during authentication. So, a fake smart card can be created with valid fingerprint and a fake voter can cast a vote instead of authorized voter.

In [3], cryptography and steganography are used together to provide confidentiality to embedded data. In [17], authors used LSB of the cover image to hide data. In [14], cryptography and steganography are used to provide secure authentication in an online voting system. The fingerprint is used as a secret key to store PIN. The live fingerprint of a voter is not taken during authentication. In [6], visual cryptography is used to create two shares of password image. The drawback of the system is if fake voter gets the share of password then he/she can cast a vote instead of valid voter. In [5], authors used live fingerprint for authentication. But this system does not provide confidentiality and integrity to the database. The microphone is low cost and commonly available device. So, in [12], the voice is used during authentication. But voice has false acceptance rate more than the fingerprint.

In [8], the fingerprint is used as a biometric measure. Confidentiality to the database is provided by visual cryptography. The problem here is if a voter has a crack on finger then he will not be authenticated as a legitimate voter. Therefore, multiple biometric factors are used in [9]. Here confidentiality is provided to the database. But, the scheme does not check if data in database and VIC has tampered or not. In [10], authors have given a scheme to provide confidentiality to password.

In 1994, Naor and Shamir have introduced visual cryptography [4]. Reconstructed image using visual cryptography has reduced image resolution and contrast [11]. In [7], XOR-based visual cryptography is used to reconstruct lossless image. In (2, 2) scheme, for a white pixel, same shares are selected and for black pixel, two inverse shares are selected. Recursive XVC introduced in [16] divides shares created in the first step recursively into sub-shares.

3. PROPOSED APPROACH FOR REGISTRATION AND AUTHENTICATION

Main purpose of authentication is only eligible voter should be allowed to vote. Each voter is allowed to cast only one vote at a time. For correct authentication, we need to use non-transferable credentials such as biometric features.

3.1. Registration Phase

Eligibility of an individual for voting is checked first before allowing him to go for registration. This is done by checking original identity card issued by the government, original address proof, etc. After verification, an eligible individual is allowed to register. We have used cryptographic hash algorithm SHA-512 to generate hash code.

Following are the steps in registration phase:

- 1) Each voter is issued with Voter's Identity Card (VIC). For each voter, unique voter identification number (VIN) is created.
- 2) Live fingerprint and photo of the face of a voter are taken.
- 3) XOR-based visual cryptography is used to create two shares of fingerprint-image i.e. share_{T₁} and share_{T₂}.
- 4) XOR-based visual cryptography is used to create two shares of photo-image i.e. share_{P₁} and share_{P₂}.
- 5) Share share_{T₁} and share_{P₁} are stored in VIC.
- 6) The hash code of share_{T₁} and share_{P₁} is created and stored voter's registration database DB₁ and DB₂ respectively.

- 7) Recursive XOR-based visual cryptography is used on share $share_T_2$ and $share_P_2$. It divides $share_T_2$ into $share_{11}$ and $share_{12}$ and $share_P_2$ into $share_{21}$ and $share_{22}$.
- 8) The hash codes of these four shares are created and stored in VIC.
- 9) Share $share_{11}$ is stored on DB_1 and share $share_{22}$ is stored in DB_4 .
- 10) Share $share_{12_22}$ is created as $share_{12_22} = share_{12} \text{ XOR } share_{22}$. It is stored in DB_2 .
- 11) Share $share_{11_21}$ is created as $share_{11_21} = share_{11} \text{ XOR } share_{21}$. It is stored in DB_3 .
- 12) The voter is further directed to enter the 4-digit password (PW) which is similar to our ATM PIN.
- 13) Timestamp (TS) of 32-bits is generated by the system.
- 14) Secret message is created using entered PW and TS as follows:

$$SM = (\text{Hash}(PW\|TS) \parallel TS).$$
- 15) Secret message is then encrypted using private key of Authentication Server as follows: $ESM = E(PU_{AS}, SM)$.
 Embed ESM in cover Image using LSB technique and PW as start position. It is stored in DB_5 .

3.2. Authentication Phase

On Election Day, a voter will be allowed for authentication if he has valid Voters Identification Card (VIC). Following are the steps for authentication phase.

- 1) The Smart card reader is used to read VIN, shares $share_T_1$, $share_P_1$ and four hash codes of database shares from Voters Identification Card (VIC).
- 2) Voter's registration database is searched with key VIN. Voter's personal information and $stego_image$ is extracted from the database.
- 3) Other shares $share_{11}$, $share_{12_22}$, $share_{11_21}$ and $share_{22}$ are read from DB_1 , DB_2 , DB_3 and DB_4 . The hash codes of these shares are generated and compared with hash code retrieved from VIC. If it matches then shares from database are unchanged. The hash code of shares $share_T_1$ and $share_P_1$ are generated. It is compared with hash code from DB_1 and DB_2 respectively. If it matches then VIC is unchanged.
- 4) Read voter's STATUS flag. FALSE STATUS flag indicates a vote has been cast. The TRUE STATUS flag indicates vote is not cast. If the flag is TRUE then continue with step 5.
- 5) The voter is directed to enter a password (PW).
- 6) Entered password (EPW) is used as starting position to decode $stego_image$ and the encrypted secret message (ESM) is retrieved.
- 7) ESM is decrypted using the public key of authentication server to retrieve the secret message.

$$SM = D(PU_{AS}, ESM).$$
- 8) First 512-bits of SM contain original hash code $OHC = \text{Hash}(PW\|TS)$ and last 32-bits contain an original timestamp.
- 9) New hash code (NHC) is generated by using Entered password (EPW) and original timestamp (TS) as

$$NHC = \text{Hash}(PW\|TS).$$
- 10) Generated new hash code (NHC) is compared with original hash code (OHC). If it is same then the password is correct otherwise not.

- 11) If voter enters the wrong password then give him three chances. If he still fails to enter correct password then reject him as an unauthentic voter.
- 12) If voter enters correct password then do biometric authentication using next steps.
- 13) Share $share_{12}$ is created as $share_{12} = share_{12,22} \text{ XOR } share_{22}$.
- 14) Share $share_{T_2}$ is created as $share_{T_2} = share_{11} \text{ XOR } share_{12}$.
- 15) The original fingerprint image is reconstructed as $share_{T_1} \text{ XOR } share_{T_2}$.
- 16) Share $share_{21}$ is created as $share_{21} = share_{11,21} \text{ XOR } share_{11}$.
- 17) Share $share_{P_2}$ is created as $share_{P_2} = share_{21} \text{ XOR } share_{22}$.
- 18) The original face image is reconstructed as $share_{P_1} \text{ XOR } share_{P_2}$.
- 19) Now live fingerprint of a voter is taken and compared with the reconstructed fingerprint. If it matches then go to next step number 21. Otherwise, go to next step.
- 20) Live photograph of voter's face is taken and compared with reconstructed face image. If it matches then go to step 21. Otherwise voter is given three chances. After third chance, if none of the biometric features is matched then reject the voter as not authentic voter.
- 21) Allow voter to vote and set STATUS flag as FALSE.

4. RESULTS AND DISCUSSION

During registration phase, shares of the fingerprint are created as shown in figure-1. Shares of face image are created as shown in figure-2.

Shares $share_{P_1}$ and $share_{T_1}$ are stored in the smart card. Recursive XOR-based visual cryptography is used for shares $share_{P_2}$ and $share_{T_2}$. Invertible property of XOR is used for the construction of shares for storing in different databases as shown in figure-3.

Shares from the database are XORed to generate share for construction of In authentication phase, fingerprint image and face image as shown in figure-4.

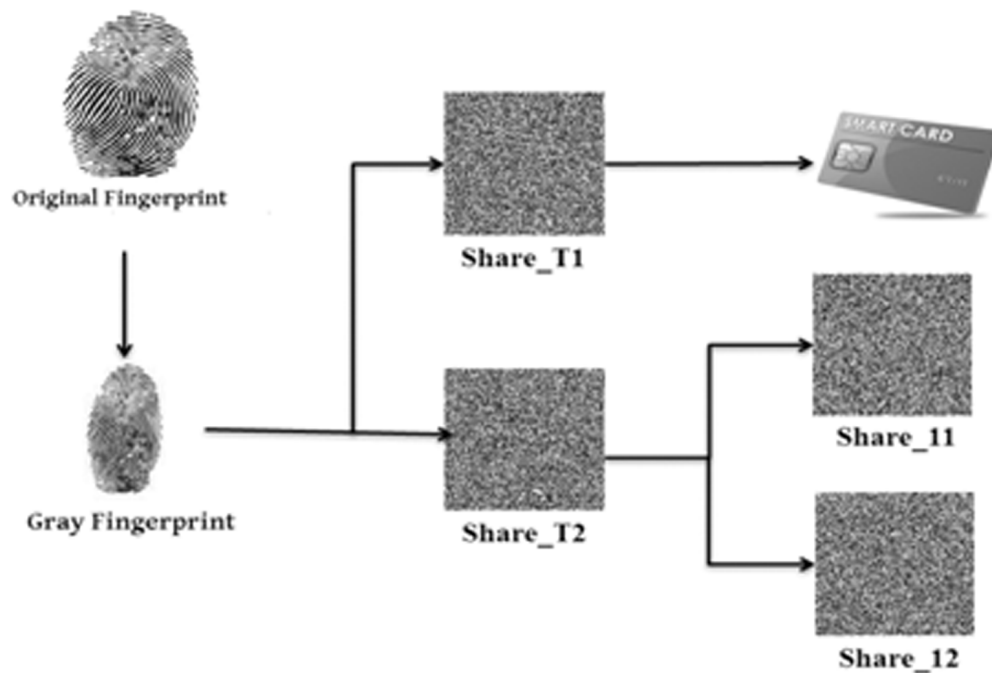


Figure 1: Shares of Fingerprint Image

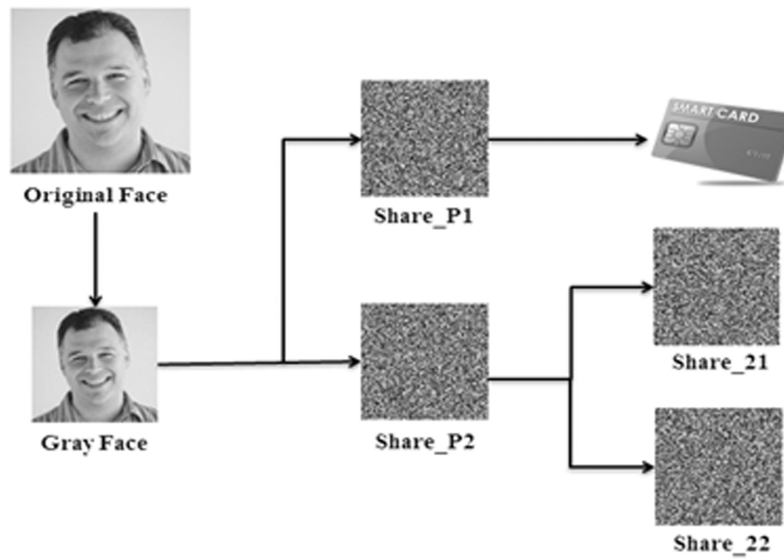


Figure 2: Shares of Face Image

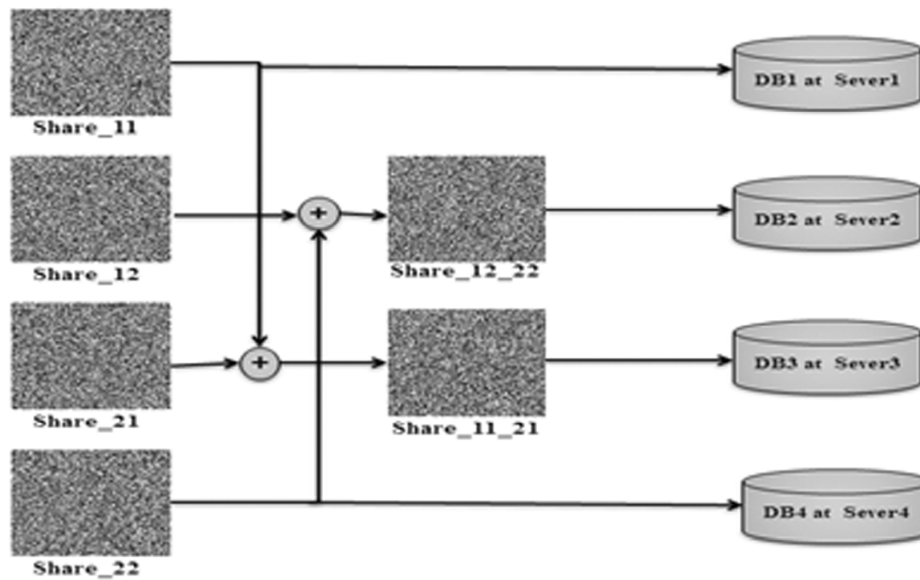


Figure 3: Shares to Databases

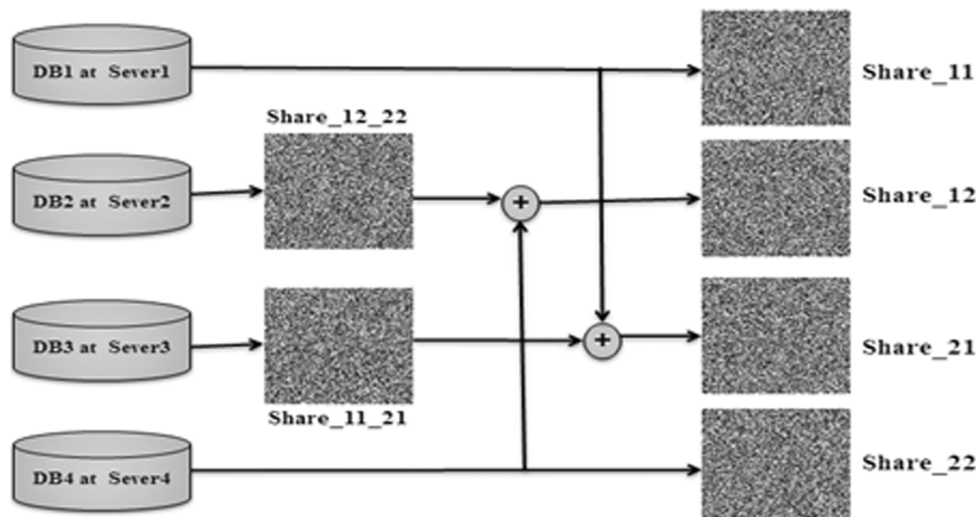


Figure 4: Shares from Databases

The fingerprint image is reconstructed as shown in figure-5. The face image is reconstructed as shown in figure-6.

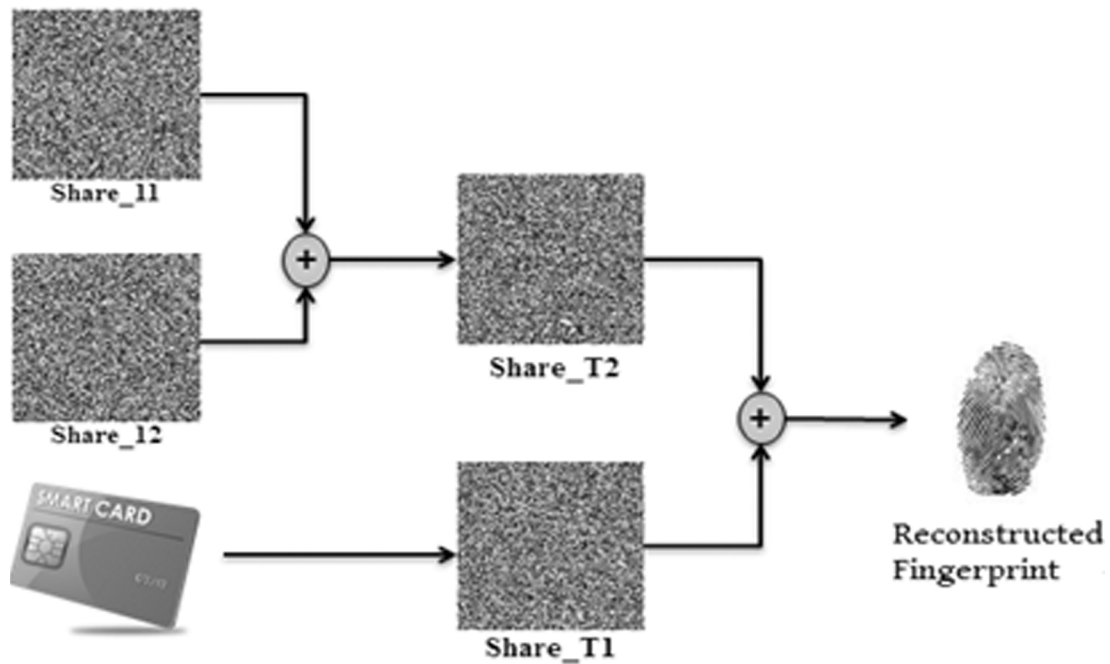


Figure 5: Reconstruction of Fingerprint Image

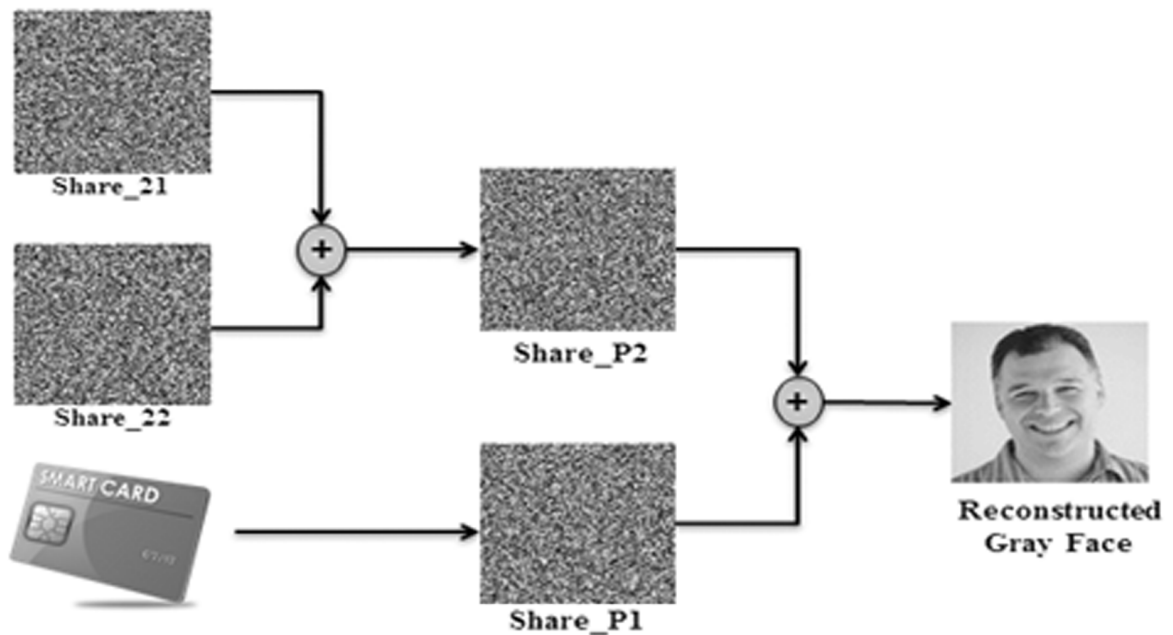


Figure 6: Reconstruction of Face Image

We have compared reconstructed image with original image. There is no change in any single pixel as XOR operation is invertible. So, we get MSE as zero and PSNR as infinity for both images. The result is shown in figure-7.

During authentication phase, images are reconstructed by using shares from VIC and four shares from four different databases located on four different servers. If fake VIC is produced during authentication, then it will contain fake shares. Original fingerprint and face image will not be reconstructed as fake shares





	Original Gray Image	Reconstructed Image	MSE	PSNR
Fingerprint			0	∞
Face			0	∞

Figure 7: MSE and PSNR

from the database are XORed with database shares. So, the fake voter will be caught easily with this process.

5. CONCLUSION

Non-transferable credentials like biometric features are used in authentication along with password authentication. Only authentic voter can pass our authentication. Both VIC and databases contain shares of images instead of original images. Thus, confidentiality of voter's registration database is maintained. Use of hash code helps to know whether database and VIC have tampered or not. The System maintains STATUS flag for each voter which guarantees one vote per voter.

REFERENCES

- [1] Hayam K. Al-Anie, Mohammad A. Alia, Adnan A. Hnaif: E-Voting Protocol Based on Public Key Cryptography. International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011, pp.87-98.
- [2] Hussein Khalid Abd-alrazzq, Mohammad S. Ibrahim, Omar Abdulrahman Dawood: Secure Internet Voting System based on Public Key Kerberos. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 3, March 2012, pp. 428-435.
- [3] Hayfaa Abdulzahra, Robiah Ahmad, Norliza Mohd Noor: Combining Cryptography and Steganography for Data Hiding in Images. Applied Computational Science, ISBN: 978-960-474- 368-1, pp. 128-135, 2014.
- [4] Moni Naor and Adi Shamir: Visual cryptography. in Proceedings of Advances in Cryptology EUROCRYPT 94, LNCS Vol. 950, pages 1- 12. Springer - Verlag, 1994.
- [5] Mohammed Khasawneh, Mohammad Malkawi, Omar Al-Jarrah, Thaier S. Hayajneh and Munzer S. Ebaid: A Biometric-Secure e-Voting System for Election Processes. Proceeding of the 5th International Symposium on Mechatronics and its Applications (ISMA08), Amman, Jordan, May 27-29, 2008.
- [6] Nathanael Paul, David Evans, Avi Rubin, Dan Wallach: Authentication for Remote Voting. Workshop on Human-Computer Interaction and Security Systems, April 6, 2003, Ft. Lauderdale, FL.
- [7] P. Tuyls, H. D. L. Hollmann, and J. H. V. Lint, L. Tolhuizen: A polarisation based Visual Crypto System and its Secret Sharing Schemes. Available at the IACR Cryptology ePrint Archive, <http://eprint.iacr.org/2002/194/>.
- [8] P.Sanyasi Naidu, Reena Kharat, Ruchita Tekade, Pallavi Mendhe, Varsha Magade: E-Voting System Using Visual Cryptography & Secure Multi-party Computation.2nd ICCUBEA 2016, IEEE.

- [9] P.Sanyasi Naidu, Reena Kharat: Multi-factor Authentication using Recursive XOR-based Visual Cryptography in Online Voting System. *Security in Computing and Communications: 4th International Symposium, SSCC 2016*, Springer, pp. 52-62.
- [10] P.Sanyasi Naidu, Reena Kharat: Secure Authentication in Online Voting System Using Multiple Image Secret Sharing. *Security in Computing and Communications: 4th International Symposium, SSCC 2016*, Springer, pp. 336-343.
- [11] Pim Tuyls, Tom Kevenaar, Geert-Jan Schrijen, Toine Staring, Marten van Dijk: Visual Crypto Displays Enabling Secure Communications. *Security in Pervasive Computing*, Volume 2802 of the series *Lecture Notes in Computer Science* pp. 271-284.
- [12] Sanjay Saini, Joydip Dhar: An eavesdropping proof secure online voting model. *2008 International Conference on Computer Science and Software Engineering*, IEEE, 2008.
- [13] Shalini Vermani, Neetu Sardana: Innovative Way of Internet Voting: Secure On-line Vote (SOLV). *IJCSI International Journal of Computer Science Issues*, Vol. 9, Issue 6, No 3, November 2012, pp. 73-78.
- [14] Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi: Online Voting System Powered By Biometric Security Using Steganography. *2011 Second International Conference on Emerging Applications of Information Technology*, IEEE, 2011.
- [15] Srivatsan Sridharan: Implementation of Authenticated and Secure Online Voting System. *4th ICCCNT 2013*, IEEE, July 4-6, 2013.
- [16] Thomas Monoth, Anto P. Babu: Recursive Visual Cryptography Using Random Basis Column Pixel Expansion. *ICIT 2007*, IEEE, pp. 41-43.
- [17] Wayne P.: *Disappearing Cryptography*. Boston: AP Professional Books, 1996.