International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

Securing Authentication Database of Online Voting System using PIN Based Lossless Image Secret Sharing Scheme

Reena Kharat, P. Sanyasi Naidu

Abstract*: Voting is vital part of democratic country as it allows citizen to choose their own government. Government plays important role in progress of each country. Result of election is good if most of the people votes. In today's digital world, it is necessary to have secure online voting system at place which will save voter's time and motivate citizen to vote. Secure authentication is the main issue in online voting system. The authentication module should allow authentic voter to cast their vote. Even though secure authentication is provided, someone having access to authentication database may use it to get authentic entry into the system. Research in this paper shows new and secure authentication module which provides confidentiality to authentication database so that no one can use the authentication database to pass through the system. We have achieved this using PIN based image secret sharing.

Index Terms: Online voting, Authentication, Secret Sharing Scheme.

I. INTRODUCTION

Now a days everything we want/ need, we get it online. We can do purchase/sell online, transfer money from one account to another. We don't need to travel for these things. Similarly, in this fast life people don't want to travel or wait in queue to cast their vote. In [20], author has shown how number of voters is reducing from 2011 to 2014 in many countries. So, there is need to provide online voting system to increase number of voters. People will be motivated to vote if the system is secure.

We have considered following security requirement given in [4, 5 and 12] for developing secure online voting system.

- Identification – It is a process by which voter is uniquely identified in the registration database.
- Authentication – It is a process by which trust is established in user identity.
- Confidentiality - It is a process by which confidentiality is provided to registration database such that even someone gets the data; it will not be useful for authentication.

Our system provides authentication using a PIN and biometric features. We provide confidentiality to the database using our secure and lossless multi-image secret sharing scheme.

I. RELATED WORK

The main issue in online voting system is how to secure database of authentication. If database is not secure, then anyone get access to data can vote as legitimate voter. Login and password based authentication given in [6] and [7], is not secure as these credentials are transferable from one to another. Non-transferable Biometrics credential is used in [17]. In [19], fingerprint used during authentication is stored in database as it is which can be stolen. Steganography and cryptography are used in [18] to provide secure authentication. In [18 and 19] biometric features are used but it is not matched with live biometric feature of a voter during authentication. In [11], live fingerprint is used during authentication phase. But confidentiality is not provided to the database. Every voter having access to computer may not have fingerprint scanner, so authentication based on fingerprint will restrict number of online voters. We need secure system which can be used for all online voters who has access to internet.

Visual cryptography was first proposed by Naor and Shamir [10] for sharing an image secretly between two parties using OR operation. OR operation reconstructs the original image with loss. So authors in [13] have used XOR operation to reconstruct lossless image. In [14], confidentiality is provided by visual cryptography for fingerprint image. In [1], (n, n)- Multi-secret sharing schemes is proposed. Here, n secret images are encrypted into n number of shares. For recovery of secret images, all n shares are required. Authors in [3] have proposed multi-secret image sharing based on XOR operation. This method leaks partial secret even if less than (n+1) shares are available.

Fingerprint and face image are used in [15] during authentication. Applying XOR operation recursively to construct complex shares was introduced in [21]. Authors in [2] have proposed Boolean-based multi-secret image sharing scheme for sharing n images secretly. One can obtain partial secret from less than (n − 1) shares. The strong MSIS scheme is proposed in [22]. This scheme does not leak any partial secret from (n−1) or fewer shares.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
Reena Kharat*, CSE Department, GITAM Institute of Technology, GITAM University, Visakhapatnam.Computer Department, Pimpri Chinchwad College of Engineering, Pune, India.
P.Sanyasi Naidu, CSE Department, GITAM Institute Of Technology, GITAM University, Visakhapatnam

But the XOR operations in this scheme take more time. The shortcomings of [2, 3 and 22] for (n, n)-MSIS scheme are overcome using additive modulo arithmetic in [8]. Reverse bit function is used in [8] to increase the randomness of shares we used. But using this method, one can get a secret image using two shares only. To avoid leaking of secret, we need MSIS which generates shares such that each share depends upon all secret images. Authors in [9] have used additive modulo and random matrix to generate randomness in generated shares. After reconstruction of shares using this method PSNR value is 43.16dB. So, in this scheme there is loss of image. In [16], authors have proposed visual cryptography scheme using private key. This scheme reconstructs images with average PSNR value less than 40dB. In all recovery methods, generation of secret image depends upon generated shares. If shares are stolen, then secret image can be recovered easily. We need a scheme which doesn't only depend upon shares generated but also takes some PIN value. User has to give this PIN at the time of share generation. One has to give this PIN as input while reconstructing secret image. Even if all shares are available and PIN is not correct, secret image will not be reconstructed.

II. PROPOSED APPROACH

Online voting system should allow only legitimate voter to vote. Each voter is allowed to cast only one vote at a time. For fulfilling these conditions, we need correct authentication system. Authentication module should use non-transferable credentials such as biometric features. So it is very essential to secure biometric images which are used for authentication. We have designed three different algorithms which make use of PIN, XOR and additive modulo operation to store images securely.

A. Registration Phase

New voter registration takes place at registration desk of government office. It is totally controlled by government. Registration officer verifies identification of voter issued by government and enters following details for each voter in the system – First Name, Middle Name, Last Name, Address, City, State, Country, Mobile Number, Login Name, Password1, Password2, PIN, Path of Fingerprint Image, Path of Face Photo Image. Following steps are followed to provide confidentiality to biometric database and PIN. Fingerprint Image, Face Photo Image and PIN are not stored as it is in the database. Shares are created using the following three different methods. Algorithm-1 gives proposed method-1.

Algorithm-1: Proposed Method-1 for Share Generation
Input: {FP: Fingerprint Image, FI: Face Image, PIN}
Output: Four share images {T1, T2, T3, T4}

1. Construct two intermediate shares randomly
   a. S1 = Random()
   b. S3 = Random()
2. Construct two intermediate shares using XOR operation
   a. S2 = S1 ⊕ FP
   b. S4 = S3 ⊕ FI
   c. S5 = S1 ⊕ S3
   d. S6 = S2 ⊕ S4
   e. S7 = S1 ⊕ S6
   f. S8 = S4 ⊕ S5
3. Construct PIN image from PIN.
   PIN_Image = Image(PIN)
4. Construct temporary shares to add effect of PIN using XOR operation
   a. S9 = S5 ⊕ PIN_Image
   b. S10 = S6 ⊕ PIN_Image
   c. S11 = S7 ⊕ PIN_Image
   d. S12 = S8 ⊕ PIN_Image
5. Construct final share images using additive modulo operation
   a. T1 = S9
   b. T2 = (T1 + S10)
   c. T3 = (T2 + S11)
   d. T4 = (T3 + S12)
6. Store shares T1 and T3 in database
7. Store shares T2 and T4 in Voter's Identification Card (VIC).
8. Issue VIC to voter.

Proposed method-2 is given by Algorithm-2.

Algorithm-2: Proposed Method-2 for Share Generation
Input: {FP: Fingerprint Image, FI: Face Image, PIN}
Output: Four share images {T1, T2, T3, T4}

1. Construct two intermediate shares randomly
   a. S1 = Random()
   b. S3 = Random()
2. Construct two intermediate shares using XOR operation
   a. S2 = S1 ⊕ FP
   b. S4 = S3 ⊕ FI
   c. S5 = S1 ⊕ S3
   d. S6 = S2 ⊕ S4
   e. S7 = S1 ⊕ S6
   f. S8 = S4 ⊕ S5
3. Construct PIN image from PIN.
   PIN_Image = Image(PIN)
4. Construct final share images using additive modulo operation
   a. T1 = (S5 + PIN_Image)
   b. T2 = (T1 + S6 + PIN_Image)
   c. T3 = (T2 + S7 + PIN_Image)
   d. T4 = (T3 + S8 + PIN_Image)
5. Store shares T1 and T3 in database
6. Store shares T2 and T4 in Voter's Identification Card (VIC).
7. Issue VIC to voter.

Proposed method-3 is given by Algorithm-3.

Algorithm-3: Proposed Method-3 for Share Generation
Input: {FP: Fingerprint Image, FI: Face Image, PIN}
Output: Four share images {T1, T2, T3, T4}

1. Construct two intermediate shares randomly
   a. S1 = Random()
   b. S3 = Random()
2. Construct two intermediate shares using XOR operation
   a. $S2 = S1 \oplus FP$
   b. $S4 = S3 \oplus FI$
   c. $S5 = S1 \oplus S3$
   d. $S6 = S2 \oplus S4$
   e. $S7 = S1 \oplus S6$
   f. $S8 = S4 \oplus S5$
3. Construct PIN image from PIN.
   PIN_Image = Image(PIN)
4. Construct final share images using additive modulo operation
   a. T1 = (S5 + PIN_Image)
   b. T2 = (S6 + PIN_Image)
   c. T3 = (S5 + S7 + PIN_Image)
   d. T4 = (S6 + S8 + PIN_Image)
5. Store shares T1 and T3 in database
6. Store shares T2 and T4 in Voter's Identification Card (VIC).
7. Issue VIC to voter.

Figure 1 Shows The Working Of Share Generation During Registration Phase Using Algorithm -3.

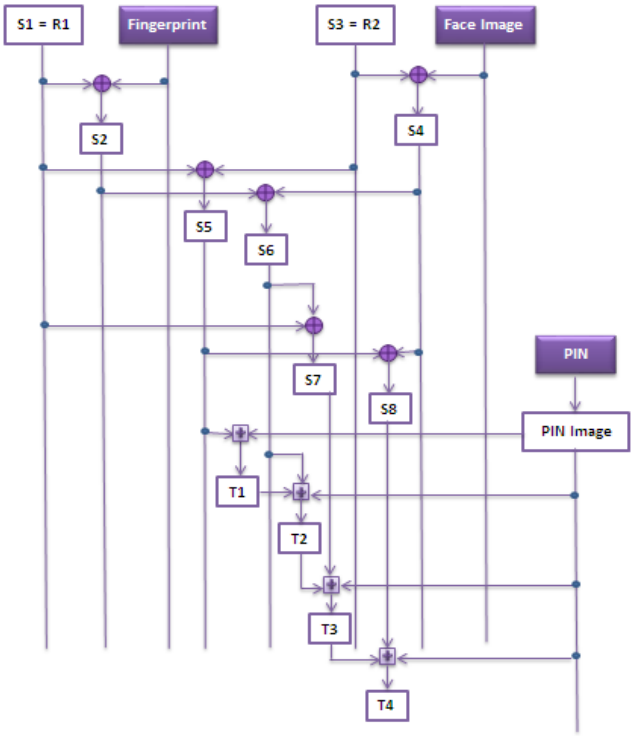


Figure 1. Shows The Working Of Image Reconstruction During Authentication Phase

B. Authentication Phase

Voter is allowed to vote if it passes through authentication phase. Voter submits shares T2 and T4 from VIC. Voter enters PIN during authentication. Shares T1 and T3 are taken from the database. Images are reconstructed using the following three different methods. These reconstructed images are matched with live images. If both matches, then voter is allowed to vote.

Proposed Method-1 for Secret image reconstruction using shares generated by algorithm-1 is given in Algorithm-4.

Algorithm-4: Proposed Method-1 for Image Reconstruction
Input: Four share images {T1, T2, T3, T4} and PIN
Output: {FP: Fingerprint Image, FI: Face Image}

1. Construct PIN image from PIN.
   PIN_Image = Image(PIN)
2. Construct temporary shares using additive inverse modulo operation
   a. S9 = T1
   b. S10 = T2 – T1
   c. S11 = T3 – T2
   d. S12 = T4 – T3
3. Construct intermediate shares using XOR operation & PIN_Image to remove effect of PIN from shares
   a. $S5 = S9 \oplus PIN\_Image$
   b. $S6 = S10 \oplus PIN\_Image$
   c. $S7 = S11 \oplus PIN\_Image$
   d. $S8 = S12 \oplus PIN\_Image$
4. Construct intermediate shares using XOR operation
   a. $S1 = S6 \oplus S7$
   b. $S2 = S4 \oplus S6$
   c. $S3 = S1 \oplus S5$
   d. $S4 = S5 \oplus S8$
5. Construct final secret image using XOR operation
   a. $FP = S1 \oplus S2$
   b. $FI = S3 \oplus S4$

Proposed Method-2 for Secret image reconstruction by using input shares generated by algorithm-2 is given in Algorithm-5.

Algorithm-5: Proposed Method-2 for Image Reconstruction
Input: Four share images {T1, T2, T3, T4} and PIN
Output: {FP: Fingerprint Image, FI: Face Image}

1. Construct PIN image from PIN.
   PIN_Image = Image(PIN)
2. Construct temporary shares using additive inverse modulo operation
   a. S5 = T1 - PIN_Image
   b. S6 = T2 – T1 - PIN_Image
   c. S7 = T3 – T2 - PIN_Image
   d. S8 = T4 –

T3 - PIN_Image

3. Construct intermediate shares using XOR operation
   a. S1 = S6 ⊕ S7
   b. S2 = S4 ⊕ S6
   c. S3 = S1 ⊕ S5
   d. S4 = S5 ⊕ S8
4. Construct final secret image using XOR operation
   a. FP = S1 ⊕ S2
   b. FI = S3 ⊕ S4

Proposed Method-3 for Secret image reconstruction by using input shares generated by algorithm-3 is given in Algorithm-6.

Algorithm-6: Proposed Method-3 for Image Reconstruction

Input: Four share images {T1, T2, T3, T4} and PIN
Output: {FP: Fingerprint Image, FI: Face Image}

1. Construct PIN image from PIN.
   PIN_Image = Image(PIN)
2. Construct temporary shares using additive inverse modulo operation
   a. S5 = T1 - PIN_Image
   b. S6 = T2 - PIN_Image
   c. S7 = T3 - PIN_Image - S5
   d. S8 = T4 - PIN_Image - S6
3. Construct intermediate shares using XOR operation
   a. S1 = S6 ⊕ S7
   b. S2 = S4 ⊕ S6
   c. S3 = S1 ⊕ S5
   d. S4 = S5 ⊕ S8
4. Construct final secret image using XOR operation
   a. FP = S1 ⊕ S2
   b. FI = S3 ⊕ S4

Figure 2 Shows The Working Of Secret Image Reconstruction During Authentication Phase Using Algorithm -6

III. RESULTS AND DISCUSSION

Share generation algorithm takes fingerprint, face photo and PIN as the input during registration phase and generates four shares as output. This is shown in Fig. 3 for algorithm-3. This is one-time process. Share T1 & share T3 are stored in database. Share T2 & share T4 are stored in Voter's Identification Card (VIC).

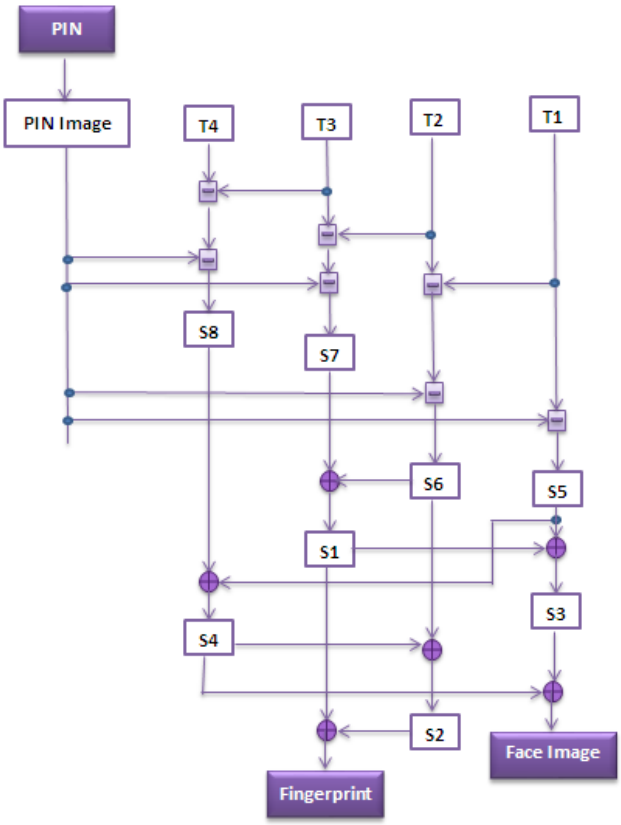


Figure 2. Image Reconstruction during Authentication Phase using Algorithm-6

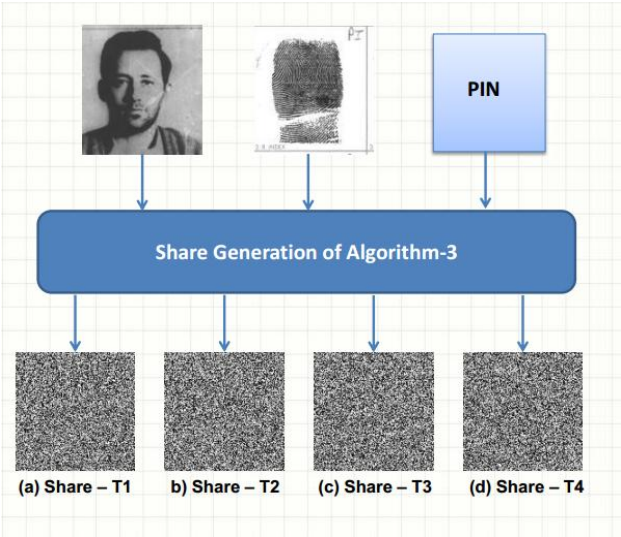


Figure 3. Share Generation Step During Registration Phase Using Algorithm-3

During authentication, voter provides two shares from VIC and PIN. Remaining two shares are taken from database and image reconstruction algorithm is applied. If voter enters the PIN same as the PIN entered during registration, then we get original images back with PSNR as infinity. This is shown in Fig. 4.

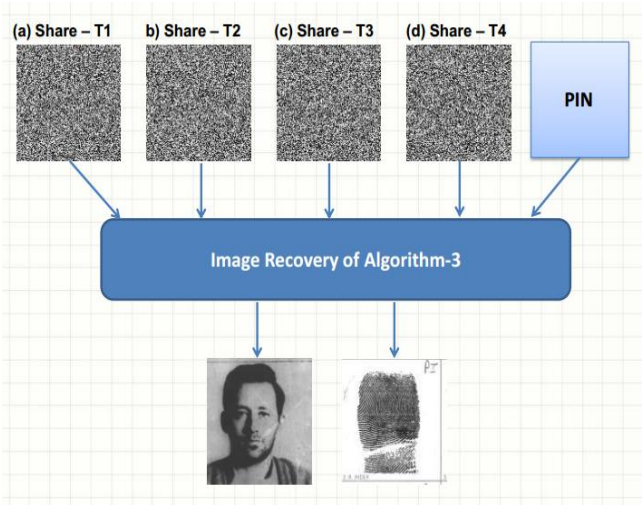


Figure 4. Secret Image Reconstruction Step During Authentication Phase With Correct PIN Using Algorithm-6

If voter enters the PIN with 50% difference with the PIN entered during registration, then we do not get original images back and PSNR is below 10dB. This is shown in Fig. 5.

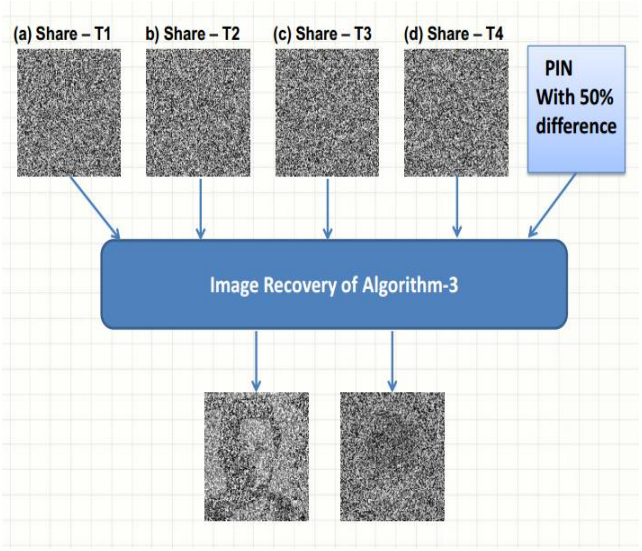


Figure 5. Secret Image Reconstruction Step During Authentication Phase With 50% Pin Difference Using Algorithm-6

Total 120 images of fingerprint [23] and 120 images of face [24] are taken for testing of algorithm - 1, 2, and 3. For each algorithm twelve different PINs are given as input with difference with original PIN of 0, 1%, 10%, 20%, 30%, 40%, 50%, 60%, 70%, 80%, 90% and 99%. Reconstructed secret images are compared with original secret images. If PIN entered during authentication is same as PIN given at the time of registration, then we get original biometric images as it is. In this case PSNR value is infinity. For other PINs, PSNR value is calculated. Average of PSNR of 120 images is taken for each PIN and graph is plotted as shown in Fig. 6, Fig. 7 and Fig. 8 for algorithm - 1, 2, and 3 respectively. If user entered PIN matches with original PIN used for share generation then exact secret image is reconstructed with PSNR value as infinity.

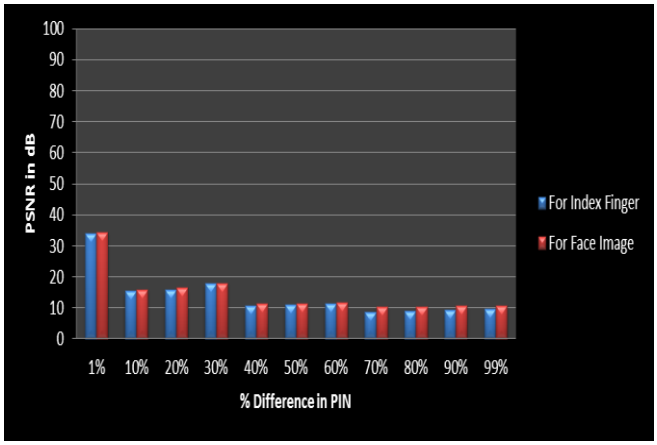


Figure 6. PSNR Verses % Difference In PIN For Algorithm-1

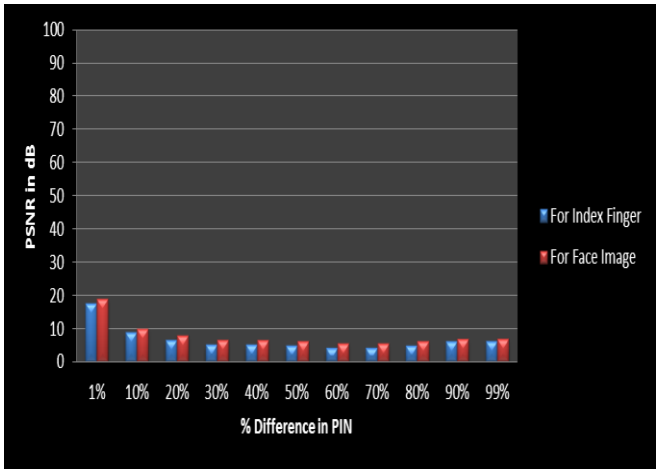


Figure 7. PSNR Verses % Difference In PIN For Algorithm-2

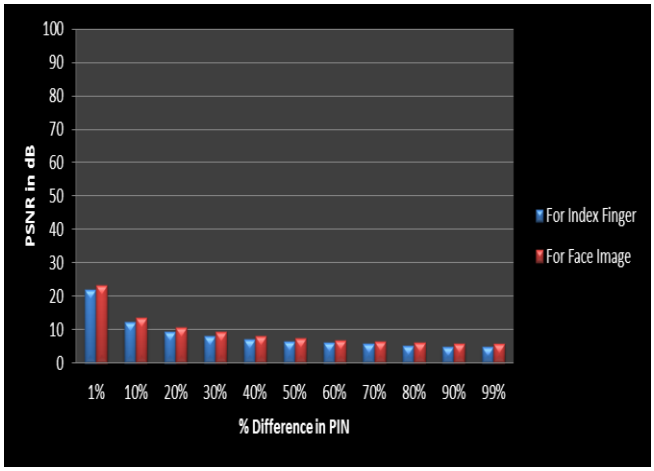
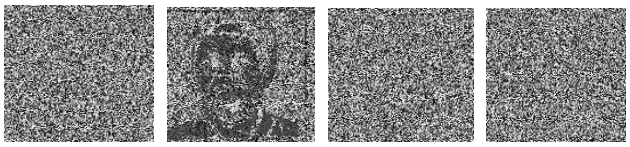


Figure 8. PSNR Verses % difference in PIN for Algorithm-3

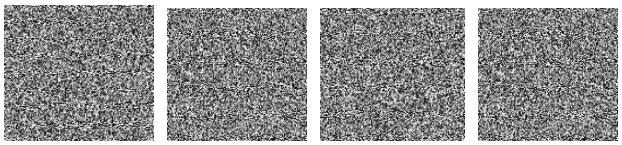
When difference between PIN is 1%, Fig. 6 shows that algorithm-1 gives PSNR value around 35dB. Fig. 7 shows that algorithm-2 gives PSNR value around 18dB when difference between PINs is 1%. Fig. 8 shows that algorithm-3 gives PSNR value around 22dB when difference between PINs is 1%. So, PSNR values given by algorithm-2 and algorithm-3 are in acceptable range.

Fig. 9 shows final shares generated through algorithm-2 and Fig. 10 shows final shares generated through algorithm-3. Fig. 9(b) is of share T2 which is leaking part of secret. So, we can conclude that shares generated through algorithm-3 does not leak secret and comparatively more secure.



(a) Share–T1 (b) Share–T2 (c) Share–T3 (d) Share–T4

Figure 9. Final Shares generated through algorithm-2



(a) Share–T1 (b) Share–T2 (c) Share–T3 (d) Share–T4

Figure 10. Final Shares Generated Through Algorithm-3

So algorithm-3 will give better security among the three proposed algorithms.

Table 1 Shows Comparative Analysis Of Proposed Scheme With Existing Schemes.

Method Name	Chen and Wu [2]	Chen and Wu [3]	Yang [22]	Maroti & Neeta [8]	Proposed Method
Lossy/ Lossless?	Loss-less	Loss-less	Loss-less	Lossless	Lossless
Share Reveals Secret	Partial	Partial	Partial	NO	NO
Recovery Strategy	XOR	XOR	XOR	Arithmetic Modulo	XOR & Arithmetic Modulo
PIN used? (Yes/ No)	NO	NO	NO	NO	YES
Reveals secret if all shares are given	YES	YES	YES	YES	NO

Table 1: Comparative Analysis

IV. CONCLUSION

The proposed PIN base multiple image secret sharing scheme is very useful. PIN is not saved at server side. Even when all shares are available, secret image will not be reconstructed without correct PIN. Results shows that even there is a one-bit difference in PIN, the PSNR value is below acceptable range. So this scheme will guarantee confidentiality of biometric image database of voter in online voting system.

REFERENCES

1. Blundo, Carlo, et al. “Multi-secret sharing schemes”, Advances in Cryptology CRYPTO94, Springer Berlin Heidel-berg, 1994.
2. Chen, Chien-Chang, and Wei-Jie Wu, “A secure Boolean-based multi-secret image sharing scheme,” Journal of Systems and Software, PP. 107-114, 2014.
3. Chen, Tzung-Her, and Chang-Sian Wu, “Efficient multi-secret image sharing based on Boolean operations,” Signal Processing, 91, PP. 90-97, 2011.
4. Ghassan Z.Q. and Rani Taha: Electronic Voting Systems: Requirement, design and Implementation. Computers Standards and Interface, Elsevier, Vol. 29, (2007): pp.376-386.
5. Gritzalis, Dimitris A.: Principles and requirements for a secure e-voting system. Computers & Security, Elsevier, Vol. 21, No. 6, (2002): pp.539-556
6. 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.
7. 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.
8. Maroti Deshmukh, Neeta Nain, Mushtaq Ahmed, “An (n, n)-Multi Secret Image Sharing Scheme using Boolean XOR and Modular Arithmetic,” IEEE 30th International Conference on Advanced Information Networking and Applications**,** pp. 690-697, 2016.
9. Mohit Rajput and Maroti Deshmukh, "Secure (n, n + 1)-Multi Secret Image Sharing Scheme using Additive Modulo," Twelfth International Multi-Conference on Information Processing-2016 (IMCIP-2016), Elsevier, pp. 677-683, 2016.
10. Moni Naor and Adi Shamir, “Visual cryptography,” Proceedings of Advances in Cryptology EUROCRYPT 94, LNCS, Vol. 950, pages 1-12. Springer - Verlag, 1994.
11. 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.
12. Nelson Hastings, Rene Peralta, Stefan Popoveniuc, Andrew Regenscheid, “Security Considerations for Remote Electronic UOCAVA Voting,” National Institute of Standards and Technology (NIST), Feb. 2011.
13. P. Tuyls, H. D. L. Hollmann, and J. H. v. Lint, L. Tolhuizen, “A polarisation based Visual Crypto System and its Secret Sharing Schemes,” IACR Cryptology ePrint Archive, 2002. http://eprint.iacr.org/2002/194/.
14. P.Sanyasi Naidu, Reena Kharat, Ruchita Tekade, Pallavi Mendhe, Varsha Magade, “E-Voting System Using Visual Cryptography & Secure Multi-party Computation,” 2016 International Conference on Computing Communication Control and automation, ICCUBEA 2016, IEEE, pp. 1-4, 2016.
15. 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, 2016.
16. Rola I. Al-Khalid, Randa A. Al-Dallah, Aseel M. Al-Anani, Raghad M. Barham, Salam I. Hajir, “A Secure Visual Cryptography Scheme Using Private Key with Invariant Share Sizes,” Journal of Software Engineering and Applications, 10, 1-10, 2017.
17. 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.
18. 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.
19. Srivatsan Sridharan, “Implementation of Authenticated and Secure Online Voting System,” 4th ICCCNT 2013, IEEE, July 4 - 6, 2013.

20. Thibaut Jaulin, "Geographies of external voting: the Tunisian elections abroad since the 2011 Uprising," Comparative Migration Studies, Springer, Vol. 4, pp.1-19, 2016.
21. Thomas Monoth, Anto P. Babu, "Recursive Visual Cryptography Using Random Basis Column Pixel Expansion," ICIT 2007, IEEE, pp. 41-43.
22. Yang, Ching-Nung, Cheng-Hua Chen, and Song-Ruei Cai, "Enhanced Boolean-based multi secret image sharing scheme," Journal of Systems and Software, 2015.
23. NIST 8-bit Gray Images of Mated Fingerprints, NIST Special Database 9. Available: https://www.nist.gov/srd/nist-special-database-9
24. NIST Mugshot Identification Database (MID), NIST Special Database 18. Available: https://www.nist.gov/srd/nist-special-database-18

AUTHORS PROFILE

Reena kharat is working as Assistant Professor in Compute Engineering department of Pimpri Chinchwad College of Engineering, Pune. Reena has completed her Masters of Technology in Computer Science & Engineering from Indian Institute of Technology, Bombay. Currently, she is pursuing her Ph.D. in Computer Science & Engineering department of GITAM Institute of Technology, from GITAM University, Visakhapatnam. She has total 15 years of teaching experience. She has guided seven post graduate student projects and 18 undergraduate student projects. She also worked in financial industry as software engineer for two years. Her area of interest is Information Security, data mining and data analytics. She has published 22 research papers.

P. Sanyasi Naidu is working as Associate Professor in Computer Science & Engineering department of GITAM Institute of Technology, from GITAM University, Visakhapatnam. He has completed his Ph.D. in Computer Science & Engineering from Andhra University. He has completed Masters of Technology in Computer Science & System Engineering from Andhra University. He has total 22 years of teaching experience. He has guided 18 post graduate student projects and 35 undergraduate student projects. Currently he is guiding 8 research scholar for Ph.D. His area of interest is information & Network Security. He has published 29 research papers. He is life member of ISTE.