

# Preventing Phishing Attack on Voting System Using Visual Cryptography

Ahood Alotaibi<sup>1</sup>, Lama Alhubaidi<sup>1</sup>, Alghala Alyami<sup>1</sup>, Leena Marghalani<sup>1</sup>,  
Bashayer Alharbi<sup>1</sup>, Naya Nagy<sup>2</sup>

<sup>1</sup>College of Cybersecurity and Digital Forensics, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

<sup>2</sup>College of Computer Science and Information Technology, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

Email: 2190000825@iau.edu.sa, 2190005581@iau.edu.sa, 2190002117@iau.edu.sa,

2190004310@iau.edu.sa, 2190003144@iau.edu.sa, nmnagy@iau.edu.sa

**How to cite this paper:** Alotaibi, A., Alhubaidi, L., Alyami, A., Marghalani, L., Alharbi, B. and Nagy, N. (2022) Preventing Phishing Attack on Voting System Using Visual Cryptography. *Journal of Computer and Communications*, **10**, 149-161.  
<https://doi.org/10.4236/jcc.2022.1010010>

**Received:** May 24, 2022

**Accepted:** October 28, 2022

**Published:** October 31, 2022

Copyright © 2022 by author(s) and  
Scientific Research Publishing Inc.

This work is licensed under the Creative  
Commons Attribution International  
License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## Abstract

Phishing is one of the most common social engineering attacks that users over the internet fall for. An example is voting systems, and because such systems should be accurate and error free, phishing prevention techniques are crucial. Visual Cryptography (VC) is utilized for efficient voting system authentication to cast votes. VC is one of the most secure approaches for privacy protection as it ensures the confidentiality of the voting system. This paper discusses proposed phishing prevention methods and compares different proposed methods.

## Keywords

Remote Voting System (RVS), Voting System (VS), Shares, Ballots, Authentication, Visual Cryptography, Phishing, Captcha

## 1. Introduction

Elections are held around the world, citizens in democratic countries have the power to elect a representative for their party to settle things in a democratic way. However, voters must cast their ballots at a polling location. Area elections are held for the government. To vote, the voter must be present at the polling station. This may weaken voter support, so, web-based voting makes this process easier. Electronic voting systems offer various features that make them different from traditional voting methods, as they also enhanced voting system features over traditional voting methods including mobility, privacy, simplicity, accuracy, and adaptability. On the other hand, voting systems might be exposed to a new threat like phishing which affects the system security. When fraudsters gain

your personal information, they can use it to commit various types of identity fraud, jeopardizing voters' reputation. Having a secure and reliable voting system, cryptographic and steganographic techniques should be applied. One of the suggested solutions is VC. Systems are used to safeguard information from hackers. It's a mechanism for encrypting visual data that can be decrypted by the human visual system without the use of computers.

## 2. Background

Network security is critical in ensuring that enterprises are adequately protected from outside threats and adversaries. System administrators monitor network security, which involves the authorization of access to data on the network. However, different types of threats can be found in networks as described in [1]. For instance, password attacks, IP spoofing, and most notably phishing it is a malicious attempt to obtain personal information such as usernames, passwords, and credit card numbers by impersonating a trustworthy entity. They are seen as a significant risk since they can disrupt a corporate system and result in massive losses. Phishing is one of the most cyber attacks to gain popularity. It is an aim towards identity theft to obtain confidential and private information about individuals or companies in exchange for money or other advantages. In the meanwhile, **Figure 1** below demonstrates the various types of voting systems.

## 3. Proposed Methods

### 3.1. MSE and PSNR Method

The paper [2], discusses about authentication of voters in a Remote Voting System (RVS), a new VC scheme is suggested. The current technique, unlike classical VC, is based on the creation of a new matrix utilizing the bitwise XOR operation. Because it uses structural similarity measures like Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) for verification, this authentication system is ideal for RVS. The experimental results show that the suggested approach is computationally efficient and achieves a decent balance of security, storage, and performance.

Name	Definition	Disadvantages
Paper ballot system	Traditional voting procedure in which the vote is cast using paper and a stamp. Each voter has their own ballot, that is not shared.	Time consuming, low counting speed, and booth capture.
Electronic voting system	Electronic ballot voting system that allows voters to broadcast their secret vote ballots to election officials through the Internet	People with limited computer skills are unable to vote properly, high cost, vulnerable to security, and consume an amount of energy at voting stations.
Online voting system	The most recent electronic voting technology is the online voting system, in which the voted ballot is communicated over the public Internet via a web browser.	vulnerable to security













**Figure 1.** Types of voting systems.

*Proposed Steps:*

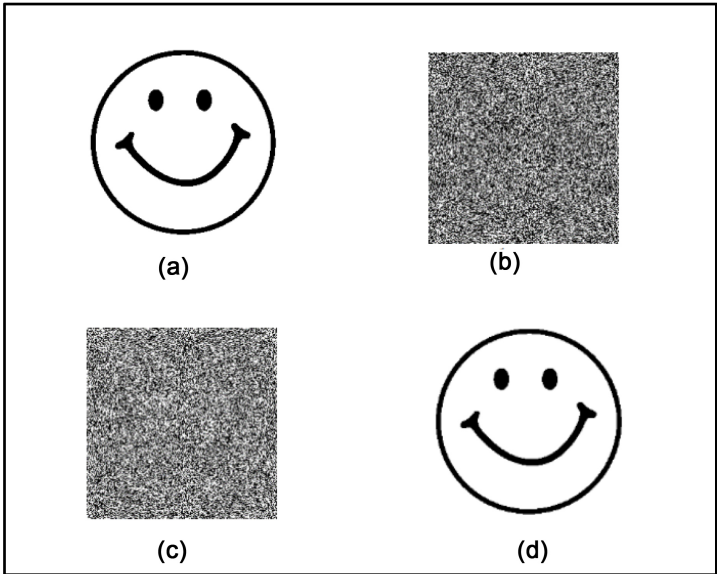
**1) Matrices Creation:** The suggested scheme is not intended to be expandable. As a result, one row of the C0 is randomly chosen to encode a white pixel, and one row of the C1 is randomly chosen to encode a black pixel. Then, for each row, one element will be assigned to one share and the other to another. Furthermore, the Hamming weight  $H = two$  and the pixel expansion  $m$  equals one.

**2) Shares Generation Phase:** If the pixel color is white, choose one block at random from the two blocks in the codebook that are peer to the white pixel shown in **Figure 2**, assign one element to share 1 and the other element to share 2. If the pixel is black, choose one block at random, repeat the process that peer to the black pixel shown in **Figure 2**. When every pixel of the secret image is scanned, the two shared images will be created.

**3) Recovery Phase:** The original secret image is recovered by stacking the shared images using the bitwise XOR method, as shown in **Figure 3**.

Pixel	Share 1	Share 2	XORed Pixel
			
			
			
			

**Figure 2.** The codebook of the proposed scheme.



**Figure 3.** Example of the output.

*Advantages and Results Analysis:*

- Because the reconstructed images are the same size as the original secret image, the pixel expansion equals one.
- As a result, it saves voters' and servers' storage space and allows for quick transmission through public networks, and other communication channels.
- The image created by stacking the shared photographs is accurate and has no information loss. The PSNR and MSE are mathematically expressed in **Figure 4**.
- Lower variance between the secret image and the reconstructed image with good visual quality is indicated by a greater PSNR and lower MSE. When the PSNR value is equal to and the MSE is zero, the technique gives the best visual quality possible, with no discernible difference between the recovered image and the original secret image.
- **Figure 5** demonstrates the MSE and PSNR values obtained between the original and recovered images for two voters: voter 1 provided the original share, whereas voter 2 submitted a suspected share. These findings show the present scheme's efficiency and effectiveness by approaching typical MSE and PSNR values. As a result, it is an appropriate strategy for RVS authentication.

As a result, the proposed method could cut operational costs and time while still fulfilling the security requirements for high-performance RVSSs.

**3.2. Pixel Shuffling Method**

Paper [3] discussed VC techniques that are used for privacy protection. By implementing a cryptographic encryption methodology utilizing pixel shuffling with interchanging their location to generate the ciphered image, it would make it difficult to decipher the image without prior knowledge of the algorithm and the secret key used.

**3.2.1. Error Diffusion Technique**

The quantization error of each pixel is filtered and sent back to a group of upcoming input samples. The output quantized pixel value is the sum of the input

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N (h_{ij} - h'_{ij})^2$$

$$PSNR = 10 \times \log \frac{R^2}{MSE}$$

**Figure 4.** Equation of MSE and PSNR.

Measures	Voter 1	Voter 2
MSE	0	1.5259e-05
PSNR	∞	48.1648

**Figure 5.** MSE and PSNR results.

pixel value and the “diffused” past errors, as shown in **Figure 6**. The error filter in **Figure 6** filters the error to give us the original image. In the error diffusion approach, the erroneous value is spread on a fractional basis to neighboring pixels in this case the error is calculated and added to the pixel to the right of the currently processed pixel. The suggested VC privacy scheme uses the error diffusion technique to simply spread the error values across neighboring pixels.

### 3.2.2. Expansion Less Share Technique

Secret data is divided into two components known as shares in VC. The original secret is revealed by stacking these two shares together using a logical XOR function. Hierarchical VC, on the other hand, encrypts the secret at multiple levels. As a result, the encryption is less expandable. The initial secret size is preserved at all levels of the shares. Secret information is encrypted at two levels in this method. Four shares are created using hierarchical VC, and three shares will be combined to make the key share. Implementing hierarchical VC, first the secret is encrypted with expansion ratio 1:2, resulting in two shares S1 and S2. If both shares are independently encrypted with the same expansion ratio, the resulting four shares will be expanded from the shares S1, and S2.

### 3.2.3. Image Captcha Base Authentication Technique

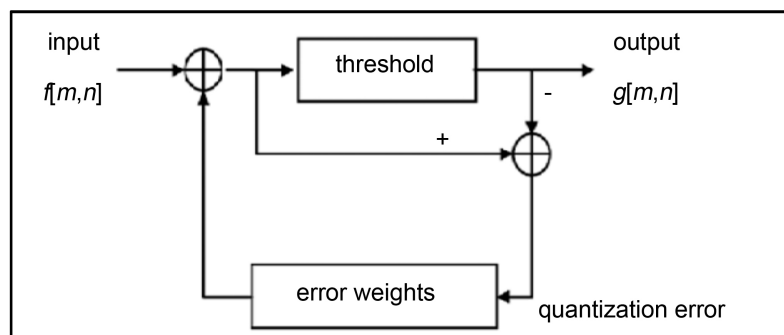
For the anti-phishing there are two phases:

1) **Registration:** During the registration process, the user enters a key, as well as the server, then a captcha image is generated. The image has been separated into two pieces that, when put together, should restore the original captcha. Flow is shown in **Figure 7**.

2) **Authentication:** Actual authentication takes place at the login step as shown in **Figure 8**. The authentication process is designed to detect phishing attacks of any form.

### 3.3. CAPTCHA and Image as Share Based Online Voting System Method

The authors of paper [4] developed an online voting system for an Indian association named “Maharashtra Carrom”. The system incorporates both a CAPTCHA



**Figure 6.** Error diffusion diagram.

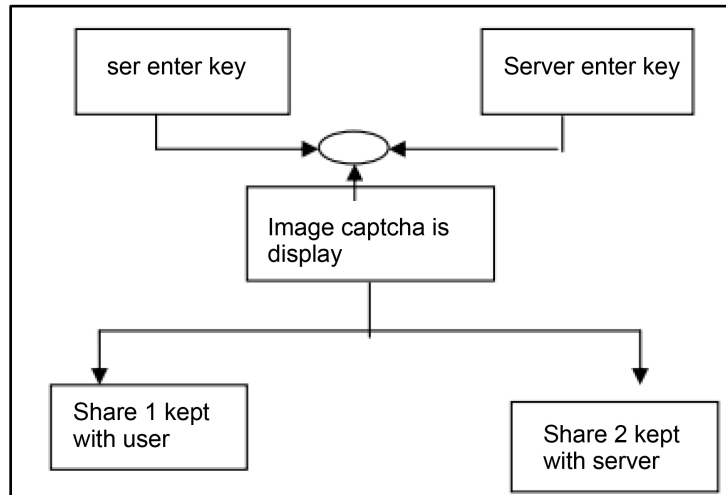


Figure 7. Registration phase.

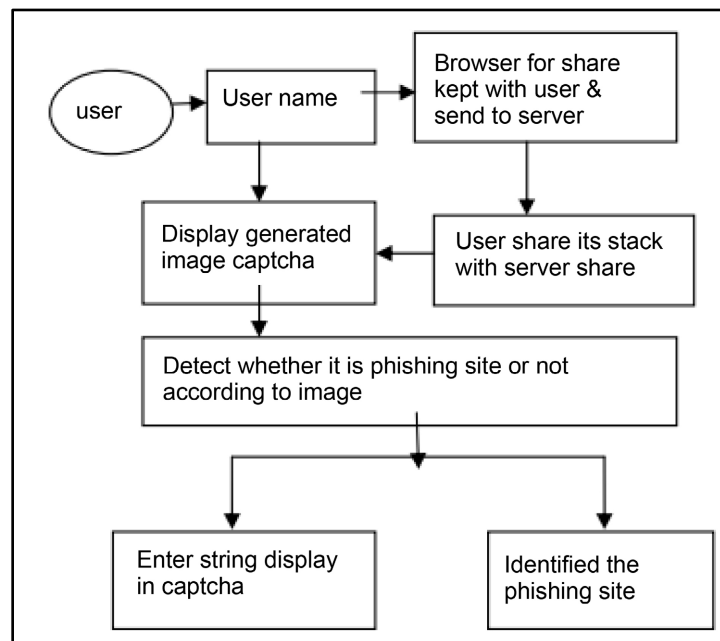
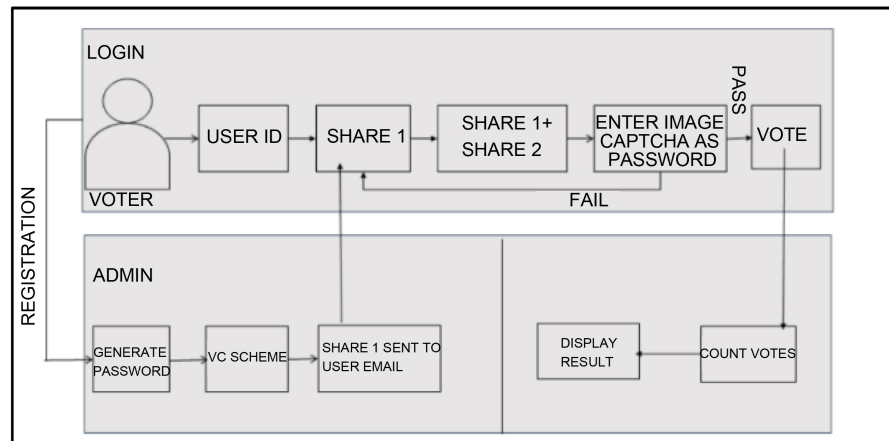


Figure 8. Login phase mechanisms for anti-phishing.

code and split-image in-share technology, as well as anonymous voting to guarantee private and secure voting process. VC is a safe method that divides a secret image into small fragments. Using two-out-of-two VC, authors propose an Internet voting system, in which users provide a secret image as a password, which is then split into two shares. One share is sent to each user’s email address as a password via VC, while the other is saved on the server. As illustrated in **Figure 9**, when users log in, they are asked to enter the share password they received through email therefore the system will add share 2, and if the password is correct, a CAPTCHA code will be generated and displayed.

The CAPTCHA code is the image converted into black and white then it will be split into shares. Each share is composed of equal numbers of black and white



**Figure 9.** Proposed method in action.

pixels. The shares will be merged at the time of voting, and the CAPTCHA will appear if the user is legitimate. Voters determined to be malicious will not be allowed to cast their votes, and the system will immediately log them out. Although the authors claim that using their proposed system will result in making people's life easier, the system not yet been implemented.

### 3.4. E-Ballot and Image as Share Method

This paper [5] addresses that the voters can vote only if they login to the system with the correct credentials. Share 1 is sent to the voter's e-mail address before the election and share 2 is provided in the system for the login process throughout the election. Voters will obtain the password to submit their vote by joining share 1 and share 2 using VC. To perform the required services as proposed in the system design stages by [5], the browser must communicate with the HTTP server. Then for users to submit their votes, an e-ballot (gadget used to cast votes in an election) is generated through steganography. The vote is casted using a database server and then encrypted via VC at the application server.

### 3.5. Web Browser and Email Oriented Share Method

In the proposed system of [6] a connection between the client and server must be established using an algorithm such as in **Figure 10**.

Afterwards the needed information, such as email address is obtained from the user on the registration page. Then an image is sent to the user to start the subsequent level of the process shown in **Figure 11**.

It highlights the utilization of VC algorithm to verify, authorize and authenticate user credentials to allow the user to cast their vote. The authors [6] suggested five working modules: initializing the server, sharing password, authenticating, casting the vote, and analyzing the result. The responsible party of the elections must submit the name of the nominees to the host, then the server system will initiate and receives votes. An email attached with a visual key share is sent to the user, while the other share is saved in the database. Authenticating

Algorithm:

1. Start
2. Image encryption
3. Input  $\leftarrow$  hidden Image
4. Output  $\rightarrow$  Encrypted Image
5. Choose input RGB image  
    Separate R-G-B Channels
6. Each channel encrypted  $\rightarrow$  receive 8 shares using key (ki)
7. From step 5, result 24 shares
8. 8 shares of each channel compress to 3 shares
9. Output: encrypted image
10. End

**Figure 10.** Algorithm of proposed secure E-voting system using VC.

Algorithm:

1. Start
2. Send a cryptographic image to finish registration
3. Choose a random radiant
4. generates image of 97,122 measure
5. Image  $\rightarrow$  QR code
6. Image shares merged if image of the database is released
7. Image merge  $\rightarrow$  generate new unique Captcha code (nuCc)
8. Use nuCc (relevant password) for login or cast the vote
9. Verify the database
10. End

**Figure 11.** Algorithm for user authorization.

the sent visual key share with the one stored in the database is done by cross referencing via the server, which produces an image that must be inserted in the prompted page in **Figure 12**.

If the user is authenticated, they can progress to casting the vote without a chance of forgery. Also, analysis of election results is possible through the server end. This proposed system implements a combination of client, server, database, and cryptography method to ensure security and integrity as illustrated in **Figure 13**. The aspect of receiving the needed share through email is what makes this method suitable for preventing phishing attacks.

### 3.6. Combining Multi-Party Computation in Share Authentication

The proposed system aims to guarantee legitimacy, security, and confidentiality of votes casted by users. It is possible by combining biometric information in a multi-party computation, physical characteristics used to assure the identity of a person through electronic devices, with VC [7]. The system takes advantage of multi-party computation features to tally votes. There are four modules in the proposed system that consists of: voter registration, authentication, vote cast and record, and vote count and announcement of the result. In the registration module the algorithm in **Figure 14** is used for the authentication and enrollment of vote, which each voter must scan their fingerprint before casting a vote. One



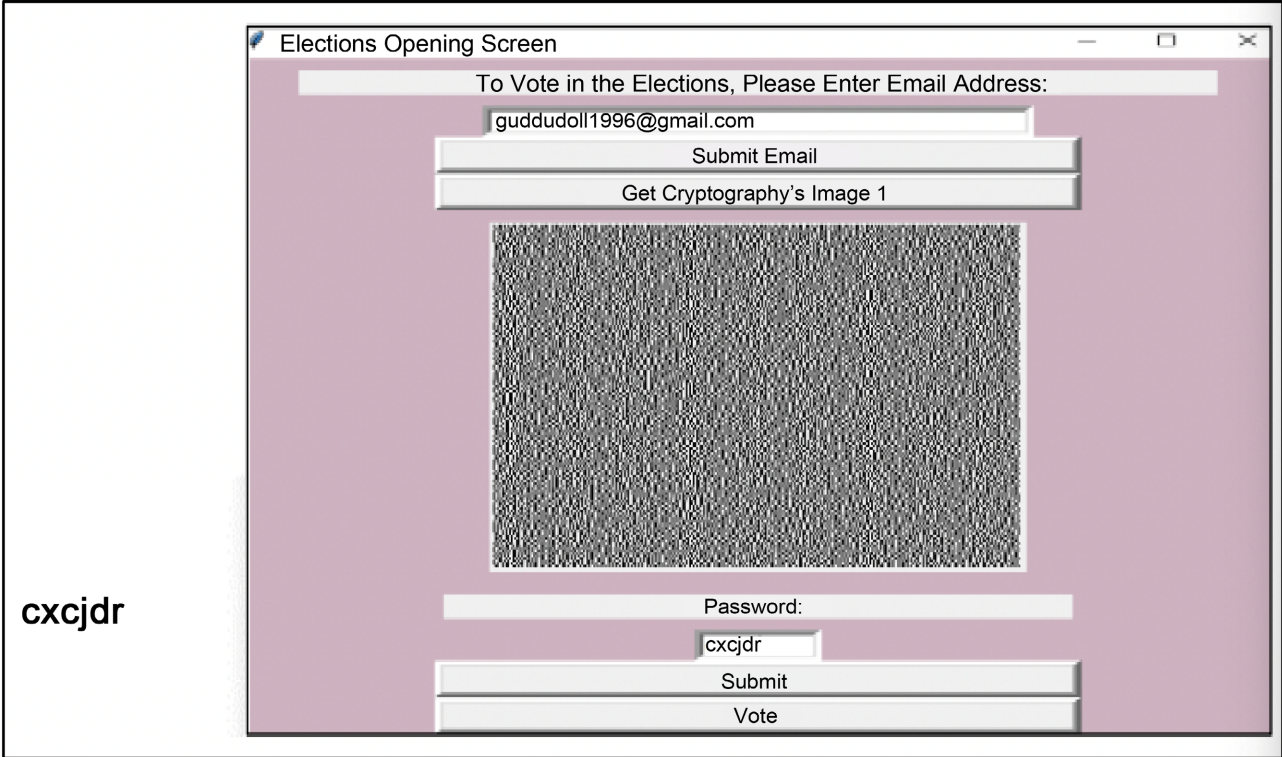


Figure 12. Generated CAPTCHA after merging of two codes.

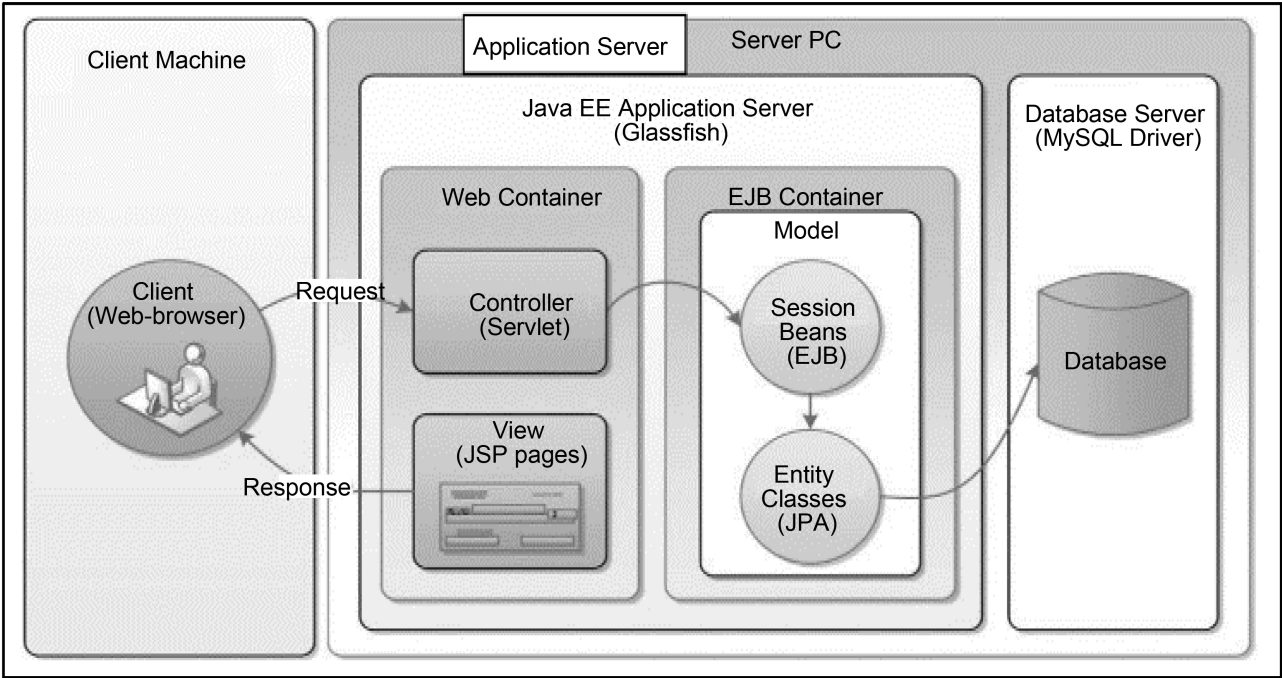


Figure 13. Suggested model for implementation.

of the shares that contains the biometric minutia is saved in the Voter Identification Card (VIC), while the other is stored in the database. The VIC contains private information belonging to the voter to be used for voting authentication,

it serves as a sufficient method for both security and convenience.

The two shares are reassembled to produce the original fingerprint image, which is used to compare with a new fingerprint image obtained from a scanner. If there is a match the voter is legitimate, therefore allowed to vote as in **Figure 15**.

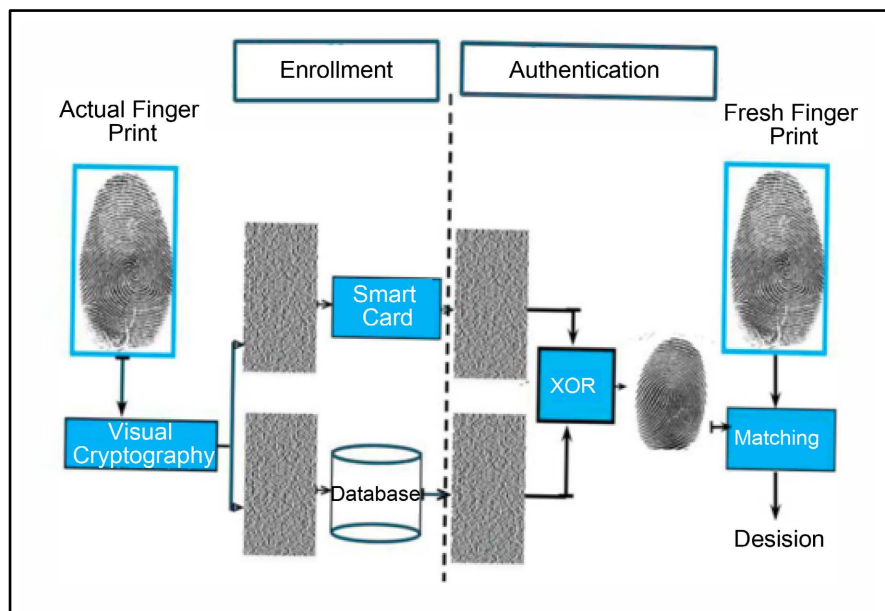
```

Algorithm: The XOR algorithm is given below:


---


S=size (Input image)
for i=1 to S
if (pixel ==1)
    if (randomNumber3999999==1)
        Share1= [1 0]
        Share2= [1 0]
    Else
        Share1= [0 1]
        Share2= [0 1]
    else
        if (randomNumber==1)
            Share1= [1 0]
            Share2= [0 1]
        else
            Share1= [0 1]
            Share2= [1 0]
    end
end of Loop
    
```

**Figure 14.** Share production, dissemination, and result reconstruction algorithm.



**Figure 15.** Phase of enrollment and authentication.

There will be a voting machine with buttons to record the votes for each nominee, each press by the user generated a signal in binary. However, storing the vote directly in this form is insecure and a new system is proposed by the authors [8] to be more secure. Where “D” is a number greater than sum of number of voters, and “n” is the number of candidates. Let  $(R_1 * d)$ ,  $(1 + R_2 * d)$ ,  $(R_3 * d)$ , ..., and  $(R_n * D)$ . The database would look like that in **Figure 16**, and each column symbolizes a vote for each nominee.

### 3.7. Discussion and Analysis

Phishing is a prevalent attack targeted on voters using e-voting systems, the severity of damages done by it calls for the use of secure schemes. Due to its importance, several proposed systems were published in the past decade. Most of the methodologies adopted VC as an integral part of its system in addition to some improvements, such as in paper [2] [3] [5] [6] [8]. In paper [2] and [8] a variation of an XOR algorithm was used for verification, which can benefit e-voting systems. However, it can be easily bypassed with proper knowledge. Whereas papers [5] and [6] adopted basic VC schemes, along with email authentication. Implementing a simple combination of authentication methods could pose to be a tremendous security disadvantage. In case the database that stores the image shares becomes compromised, a malicious entity could deceive the authentication. The vantage point in paper [8] pairing fingerprint scanners in the process of registration and authentication for e-voting. This method ensures a lower chance of false authentication, which is an improved security mechanism. As for paper [3] it implemented three VC schemes with two of them discussed anti-phishing in particular expansion less share, and image captcha base authentication.

Candidat $e_1$	Candidat $e_2$	.....	Candidat $e_n$
$(0+R_{11} * d)$	$(0+R_{12} * d)$	.....	$(1+R_{1n} * d)$
$(0+R_{21} * d)$	$(1+R_{22} * d)$	.....	$(0+R_{2n} * d)$
$(1+R_{31} * d)$	$(0+R_{32} * d)$	.....	$(0+R_{3n} * d)$
.	.	.....	.
.	.	.....	.
.	.	.....	.
$(1+R_{m1} * d)$	$(0+R_{m2} * d)$	.....	$(0+R_{mn} * d)$

**Figure 16.** Encrypted votes casting and recording.

## 4. Conclusion

In conclusion, the suggested methods of all the discussed papers focused on visual cryptography techniques for privacy protection and user validation. With the help of such schemes, it is possible to conduct election processes confidentially with the highest accuracy to reduce the risk of falsification on e-voting systems. The applicability, cost-efficiency, improved performance, and security of visual cryptographic methods is what distinguishes it from other approaches. In the examined methods it was apparent VC could be enhanced by pairing it with other authentication means such as biometric devices, error diffusion scheme, image CAPTCHA, and expansion less share. In despite of the efficiency and convenience of e-voting systems, it has still not been embraced internationally. We suggest for future works that an e-voting system framework should combine a variance of biometric authentication, image CAPTCHA, and an adequate security system for databases or data centers that store essential image shares for the processes.

## Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

## References

- [1] Nisha, S. and Madheswari, A.N. (2016) Prevention of Phishing Attacks in Voting System Using Visual Cryptography. 2016 *International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, Pudukkottai, 24-26 February 2016, 1-4. <https://doi.org/10.1109/ICETETS.2016.7603013>
- [2] Hodeish, M. and Humbe, V. (2017) A New XOR-Based Visual Cryptography Scheme for Authentic Remote Voting System. <https://api.semanticscholar.org/CorpusID:53470499>
- [3] Nayan, A. and Ardak, P. (2022) Visual Cryptography Scheme for Privacy Protection. <https://ijcsit.com/docs/Volume%205/vol5issue02/ijcsit20140502239.pdf>
- [4] Rane, S.S., AdwaitPhansalkar, K., Shinde, M.Y. and Kazi, A. (2020) Avoiding Phishing Attack on Online Voting System Using Visual Cryptography. 2020 *International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore, 22-24 January 2020, 1-4. <https://doi.org/10.1109/ICCCI48352.2020.9104071>
- [5] Singh, A., Nandini, S., Pawana, S., Supriya, C. and Biswagar, D. (2021) Prevention of Phishing Attacks on Online Voting Using Visual Cryptography. *Journal of University of Shanghai for Science and Technology*, **23**, 246-249. <https://jusst.org/wp-content/uploads/2021/06/Prevention-of-Phishing-Attacks-on-Online-Voting-using-Visual-Cryptography.pdf>
- [6] Tiwari, M.G.D. and Kakelli, A.K. (2021) Secure Online Voting System Using Visual Cryptography. *Walailak Journal of Science and Technology*, **18**. <https://doi.org/10.48048/wjst.2021.8972>
- [7] Walake, A. and Chavan, P. (2015) Efficient Voting System with (2, 2) Secret Sharing Based Authentication. *IJCSIT*, **6**, 3739-3743.

- [8] Naidu, P.S., Kharat, R., Tekade, R., Mendhe, P. and Magade, V. (2016) E-Voting System Using Visual Cryptography & Secure Multi-Party Computation. 2016 *International Conference on Computing Communication Control and Automation (ICCUBEA)*, Pune, 12-13 August 2016, 1-4.  
<https://doi.org/10.1109/ICCUBEA.2016.7860062>