

Preventing Phishing Attacks on Voting Systems

Using Visual Cryptography by Securing Login and Authentication

Satyam Kumar Singh
B.E. CSE. (Hons.) AIML,
Apex Institute of Engineering,
Chandigarh University,
Punjab, India
21BCS11016@cuchd.in

Yash Nagar
B.E. CSE. (Hons.) AIML,
Apex Institute of Engineering,
Chandigarh University,
Punjab, India
21BCS10954@cuchd.in

Mayank Airan
B.E. CSE. (Hons.) AIML,
Apex Institute of Engineering,
Chandigarh University,
Punjab, India
21BCS11875@cuchd.in

Sahil Tyagi
B.E. CSE. (Hons.) AIML,
Apex Institute of Engineering,
Chandigarh University,
Punjab, India
21BCS11054@cuchd.in

Aryan Chaudhary
B.E. CSE. (Hons.) AIML,
Apex Institute of Engineering,
Chandigarh University,
Punjab, India
21BCS11060@cuchd.in

Mukesh Birla
AIT-CSE Chandigarh University
mukesh.e15063@cumail.in

Abstract— This research introduces the integration of visual cryptography to counter phishing attacks in voting systems, which improves security against cyber threats. The study investigates the impact of phishing on voting and assesses the effectiveness of visual cryptography. The methodology outlines the system's architecture, emphasizing security protocols and user interfaces. The results emphasize the complexities of data processing and the benefits of security enhancements. In conclusion, visual cryptography enhances the security of voting systems and provides valuable insights for future advancements. This study is a significant contribution to safeguarding democratic processes against cyber threats.

Keywords—Visual Cryptography, Phishing Prevention, Voting Security, User Authentication, Share generation, CAPTCHA, Dynamic Image Generation

I. INTRODUCTION

In the contemporary landscape of global elections, the traditional method of casting votes at physical polling stations poses challenges to voter participation. The advent of web-based voting systems has emerged as a transformative solution, offering enhanced features such as mobility, privacy, simplicity, accuracy, and adaptability. However, with these advancements come new security threats, particularly the rising concern of phishing attacks. Phishing, a malicious act of acquiring sensitive information, poses a significant risk to the integrity of electronic voting systems. In the pursuit of a secure and reliable voting mechanism, the integration of cryptographic and steganographic techniques becomes imperative.

This research delves into the realm of securing electronic voting systems, proposing the utilization of Visual Cryptography (VC) as a safeguard against potential cyber threats. VC operates as an encryption mechanism for visual data, ensuring protection against unauthorized access and manipulation by hackers. By leveraging VC, the research aims to fortify the foundations of web-based voting systems, fostering a resilient and trustworthy electoral process. The subsequent sections will unravel the intricacies of this approach, exploring its implementation, results analysis, and avenues for future enhancements.

II. BACKGROUND

In our rapidly advancing digital age, the surge in cyber threats, particularly phishing attacks, has become alarming. Phishing, a deceitful practice orchestrated by cybercriminals, manipulates individuals into revealing sensitive data like usernames and passwords through deceptive emails or

fraudulent websites. This poses grave risks, including identity theft and financial loss. As these threats evolve, innovative safeguards are imperative.

Visual Cryptography (VC) stands out as a state-of-the-art cybersecurity solution. It secures visual information by dividing it into shares, which, when combined, reconstruct the original data. VC's distinctive feature lies in its visual decryption process, devoid of computational dependence.

The convergence of VC and phishing prevention is pivotal for bolstering cybersecurity. Integrating VC into systems vulnerable to phishing enhances data protection, ensuring that even with access to one share, attackers cannot decipher the original information without all shares.

This research explores the synergy between Visual Cryptography and phishing prevention, particularly in critical domains like online voting systems. The study aspires to advance secure digital communication, contributing to the ongoing battle against evolving cyber threats.

III. PROPOSED METHOD

This research delves into fortifying the security layers surrounding the login and authentication procedures within the voting system. While encryption and blockchain technologies have already made strides in securing the voting process, vote storage, counting, and verification, this study focuses specifically on elevating the quality and reliability of the login and authentication phases. By enhancing these crucial aspects, the overall integrity and trustworthiness of the voting system can be further solidified. This research aims to contribute valuable insights to the ongoing discourse on securing digital voting mechanisms, ensuring a robust and trustworthy electoral process for all stakeholders involved. Following are the main techniques that we used in the visual cryptography core of our voting system for registration, authentication, and verification of users at the time of login:

A. CAPTCHA key generation

This research presents an innovative CAPTCHA key generation method for enhancing voting system security. Through dynamic image creation, grayscale conversion, statistical analysis, binary transformation, and resizing, the process ensures robust voter authentication. The approach

contributes to preventing automated bot interference in voting processes by generating visually secure CAPTCHA keys.

Algorithm :

1. Start

2. Generate random text for captcha

3. Convert text to image

4. Convert image to grayscale

5. Calculate mean and sd for pixel value of grayscale image

6. Set threshold = mean - sd

7. For each pixel in the image:

- If pixel value < threshold:

- Set pixel value to 0

- Else:

- Set pixel value to 1

8. Save the new binary image

9. End



Fig 1- CAPTCHA image



Fig 2- Grayscale image



Fig 3- Black and white (0/1) image

B. Share generation

This critical phase involves crafting the VC key from the secret image. By creating two blank images, each twice the dimensions of the secret image, a meticulous process unfolds. For every pixel in the secret image, a 2x2 pixel square is harnessed to formulate the secret shares.

In the share generation process, white pixels take on a practical role. They are transformed into a 2x2 square using the pattern $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, replicated in both share 1 and share 2. Conversely, black pixels follow a different routine.

They adopt the pattern $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ in share 1 and seamlessly shift to $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ in share 2. This pixel manipulation serves as the foundation for a robust visual cryptography system, providing a clear and technical structure for secure cryptographic sharing.

Algorithm:

1. Start

2. Input: secret_image, voter_id, cmp_image_path

3. Create blank shares share1 and share2

4. For each pixel (x, y) in secret_image:

- Get pixel value

- If pixel value is 0:

- Set corresponding pixels in share1 and share2

for black pixels

- Else (pixel value is 1):

- Set corresponding pixels in share1 and share2

for white pixels

5. Save share1 and share2 with filenames based on voter_id

6. Get pixel data from share2

7. Use shift_and_replace to perform a shift operation on the pixel data

8. Save the modified share2 and the original share1 images

9. End

Secret image	Share 1	Share2

Fig 4 – image share generation scheme

C. Pixel Shifting

Shifting pixels introduces an added layer of security in visual cryptography, enhancing controlled distortion. This process involves linearly displacing pixels by a random amount, serving as a key for cryptographic measures. The algorithm, exemplified by the code snippet below, randomly shifts pixels to the left or right within a predetermined range (here, up to 50 positions), contributing to the controlled distortion crucial for secure sharing of visual cryptographic information.

During decryption, the stored shift key is applied to reverse the pixel shift, ensuring an accurate reconstruction of the original image. This bidirectional shifting process, coupled with cryptographic key management, fortifies the security of visual cryptography by introducing an additional layer of complexity and control during both encryption and decryption phases.

Algorithm:

1. Start
2. Input: lst, shift_direction
3. Generate random shift value between 0 and 49 (inclusive)
4. If shift_direction is 'left':
 - For i from 1 to the shift value:
 - Remove the first element from lst
 - Append a zero at the end of lstElse if shift_direction is 'right':
 - For i from 1 to the shift value:
 - Insert a zero at the beginning of lst
 - Remove the last element from lst
5. Output: shift value and modified lst
6. End

D. Share transfer

In the secure transfer phase, a meticulously orchestrated process unfolds. Commencing with the input of essential parameters—email, file path, and voter ID—the system initializes an email configuration, ensuring confidentiality and integrity. Headers are set, designating sender and receiver email addresses, along with a subject line. The image, generated through the established methodology, is seamlessly attached to the email. Simultaneously, a comprehensively composed email body, incorporating instructions and the

unique voter ID, takes shape. This amalgamation of multimedia content and informative text is meticulously packaged and dispatched using a secure connection to the SMTP server, culminating in the successful transmission of the crucial visual cryptography share.

Algorithm:

1. Start
2. Input: email, path, voter_id
3. Initialize Email:
 - Set receiver_email to email
 - Create MIMEMultipart instance named msg
4. Set Email Headers:
 - Set msg['From'] to sender_email
 - Set msg['To'] to receiver_email
 - Set msg['Subject'] to subject
5. Attach Image:
 - Read image data from path
 - Create MIMEImage object with image data
 - Attach MIMEImage to the email
6. Compose Email Body:
 - Create body text with instructions and voter ID
7. Attach Text Body:
 - Attach MIMEText with the body text to the email
8. Send Email:
 - Connect to the SMTP server
 - Start TLS for secure communication
 - Log in to the server using SMTP username and password
 - Send the email using server.sendmail
9. End

E. Image Overlapping

In the decryption and comparison phase, the process initiates by retrieving essential parameters, namely the voter_id and img2, from the command-line arguments. Function definitions are crucial components of this phase, contributing to the meticulous execution of tasks. The shift_and_replace function orchestrates a shift operation on a list based on specified shift_direction and shift values. Simultaneously, the pad_images_to_equal_size function handles the opening, padding, and retrieval of pixel data, ensuring uniform dimensions for two images. The decrypt_and_compare function, a cornerstone of this phase, retrieves stored image data and shift values from the database, converts blob data to images, and engages in pixel-level operations.

The systematic sequence ensures a seamless execution, exemplified by the example usage of the decrypt_and_compare function with provided voter_id and img2. The database connection is diligently established, and upon completion, the process culminates with the graceful closure of the database connection. This orchestrated sequence underscores the precision and efficiency embedded in the decryption and comparison procedures, contributing substantively to the overarching security architecture of the e-voting system.

Algorithm:

1. Start
2. Input: Retrieve voter_id and img2 from command-line arguments.
3. Define shift_and_replace Function:
 - Perform a shift operation on a list based on shift_direction and shift.
4. Define pad_images_to_equal_size Function:
 - Open, pad, and return pixel data along with new dimensions for two images.
5. Define decrypt_and_compare Function:
 - Retrieve stored image (blob) and shift value from the database.
 - Convert blob data to Image (share1).
 - Save share1 as a PNG image in the 'uploads' folder.
 - Pad images to equal size and get their pixel data.
 - Perform a shift operation on the pixel data of img2 using shift_and_replace.
 - XOR the pixel data of both images.
 - Create a new image (merged_image) with the merged pixel data.
 - Save the merged image in the 'uploads' folder.
6. Database Connection:
 - Connect to the MySQL database with specified credentials.
7. Example Usage:
 - Call decrypt_and_compare with the provided voter_id and img2.
8. Close Database Connection:
 - Close the database connection.
9. End

Share 1	Share2	XOR ed image

Fig 5– XOR overlapping

>>Advantages of the Proposed System:

- **Enhanced Security:** The integration of CAPTCHA key generation and Visual Cryptography ensures robust protection against automated interference, fortifying the overall security of the voting system.
- **Controlled Distortion:** The implementation of pixel shifting introduces controlled distortion, enhancing the complexity of cryptographic measures. This controlled distortion adds an extra layer of security to safeguard the integrity of the visual cryptography shares.
- **Secure Transfer:** The system ensures secure and confidential transfer of visual cryptography shares through meticulous email configuration. This process guarantees the confidentiality and intact transmission of crucial cryptographic information.
- **Efficient Decryption:** The decryption and comparison phase is designed for precision and efficiency. This meticulous process significantly contributes to the overall security architecture of the e-voting system, ensuring accurate reconstruction of the original image during decryption.
- **Visually Secure Shares:** The visual cryptography shares generated by the system provide a clear and technically structured cryptographic foundation. This visual security enhancement surpasses traditional methods, offering a sophisticated approach to secure cryptographic sharing in the voting system.

IV. ARCHITECTURE

The architectural design of our voting system is structured into two pivotal segments: the registration phase and the login phase. This architecture provides the required fracture for handling new voters and existing voters:

I. Registration Phase:

Within the initial phase of our voting system, the architectural framework comprises key components, each serving a distinct purpose.

a) Client Form:

In this context, the Client Form emerges as a pivotal component, functioning as the primary interface through which users furnish their information during the registration process. This component undertakes the crucial task of capturing and validating user details, ensuring accuracy and completeness before submission.

b) Visual Cryptography Core:

The nucleus of the registration phase lies in the Visual Cryptography Core. This integral component is tasked with the generation of cryptographic shares instrumental in user authentication. Leveraging advanced visual cryptography techniques, it facilitates the secure creation and distribution of cryptographic keys, thereby fortifying the overall security posture of the system.

c) Database:

The Database, a cornerstone of the registration phase, assumes a paramount role. It acts as the repository for securely storing essential voter information. This encompasses managing user data, cryptographic shares, and other pertinent details. The Database not only ensures the integrity of stored data but also guarantees its accessibility as required.

II. Login phase:

Transitioning to the Login Phase, the architectural components play a synchronized role in orchestrating a secure and streamlined user experience. This also include a second layer of authentication after the Captcha verification that is by the registered Email address and the given password

a) User Input:

At the forefront of the login phase is the User Input component. This facet is responsible for collecting input from users as they initiate the authentication process. It serves as the gateway for users to convey their credentials securely.

b) Decryption Engine:

Serving as the linchpin of the login phase, the Decryption Engine shoulders the responsibility of securely decrypting and validating user credentials. It draws upon the cryptographic keys generated during the registration phase, ensuring a robust and secure authentication process.

c) Database:

The Database, persisting from the registration phase, continues to be instrumental in the login phase. It retains user profiles and cryptographic data, facilitating the comparison required for authentication. The Database, in this phase, stands

as a critical component ensuring the alignment of user input with the stored information

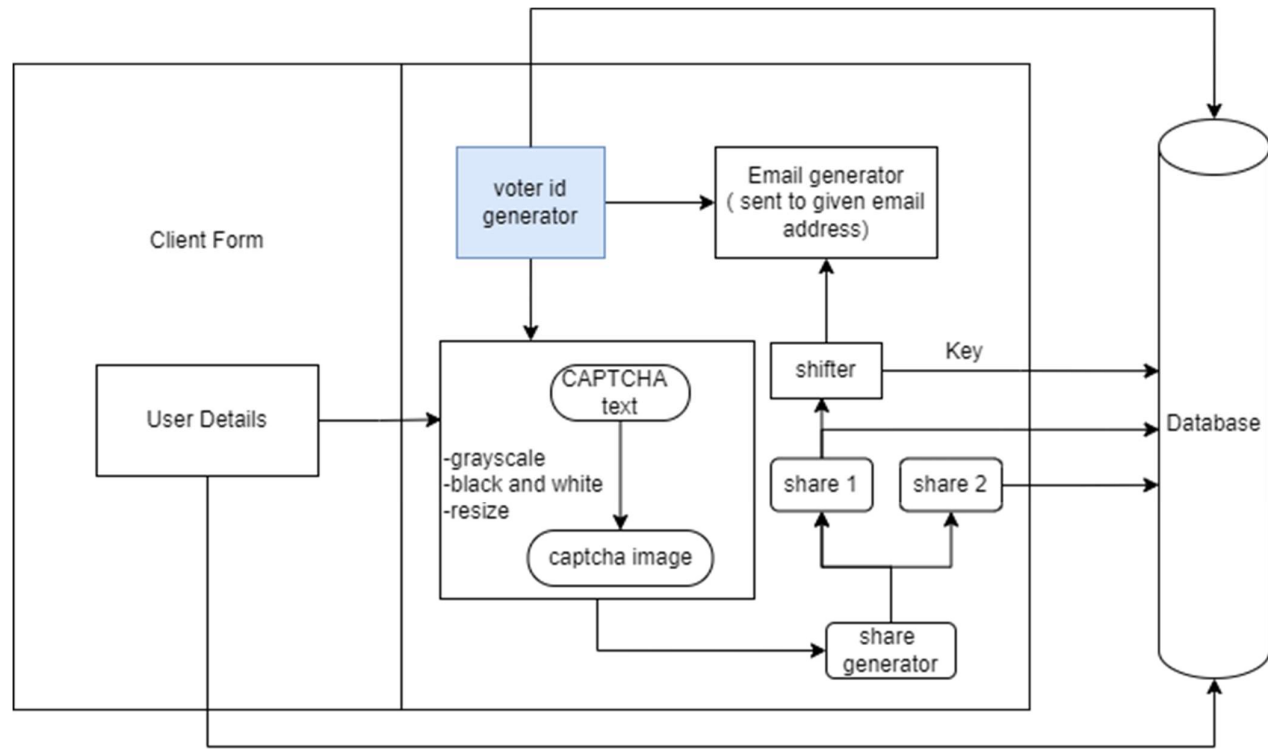


Fig 6 – Architecture for registration phase

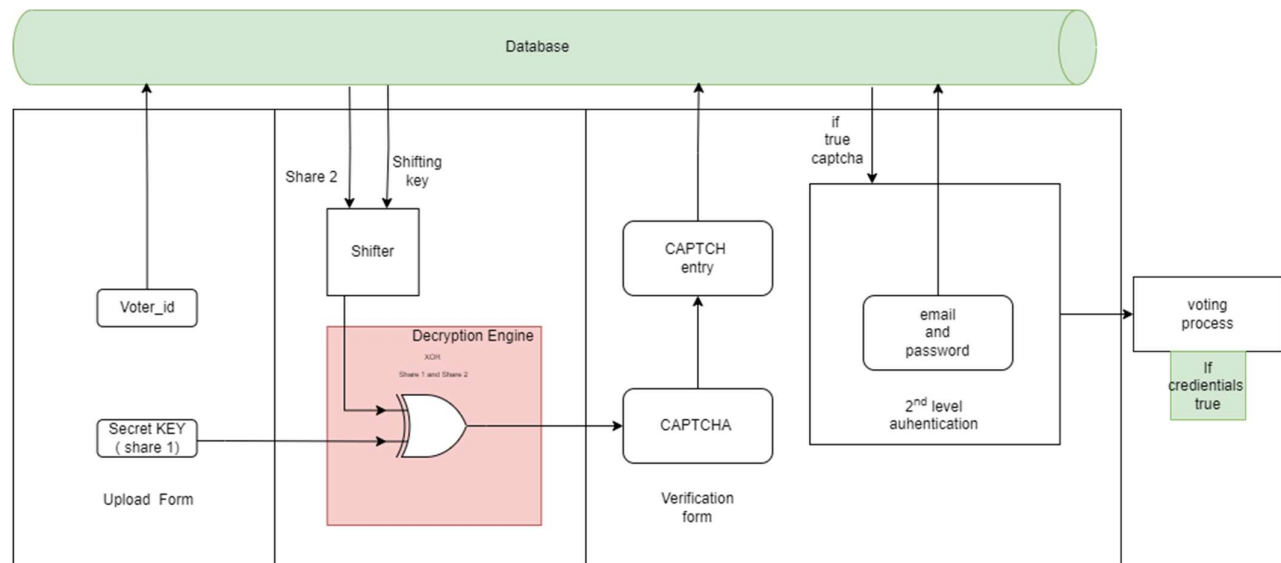


Fig. 7-Architecture for Login Phase

V. IMPLEMENTATION

This section details the practical deployment of the proposed voting system architecture, translating conceptual frameworks into a functioning system.

- i. System Setup: Configured the system environment using the XAMPP server ensuring compatibility.
- ii. Client Form Integration: Seamlessly integrated a user-friendly client form for voter registration, prioritizing [design principles] using Web app in HTML, CSS, and PHP.
- iii. Visual Cryptography Core Deployment: Deployed the Visual Cryptography Core with [algorithms, cryptographic techniques], enhancing security through cryptographic share generation.
- iv. Database Configuration: Configured the database with [MySQL], ensuring robust data storage, retrieval, and integrity.
- v. User Input Handling: Integrated a user input component for efficient capture of login credentials.
- vi. Decryption Engine Integration: Integrated a decryption engine using XOR overlapping for credential verification.

The implementation phase validated the theoretical foundations of the voting system, demonstrating practical viability. Robust security measures and seamless user interactions underscore the system's effectiveness.

Screenshot Documentation: Captured screenshots at key junctures to visually document the implementation process.

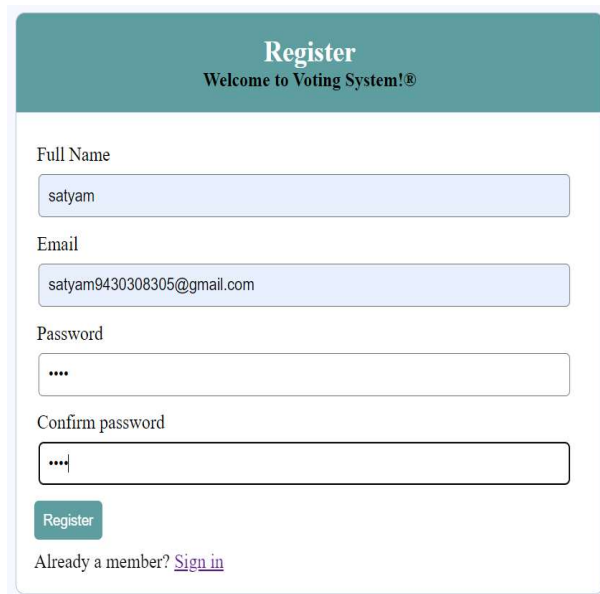


Fig 8. Voter Registration page

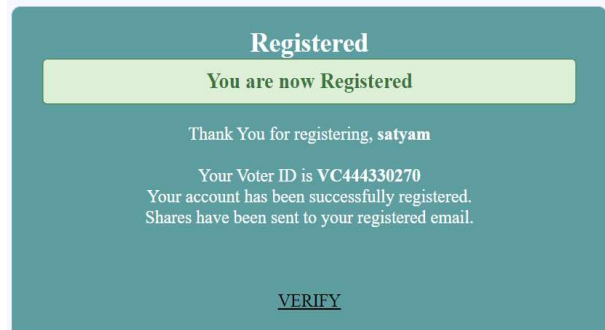


Fig 9. Voter Registration Detail

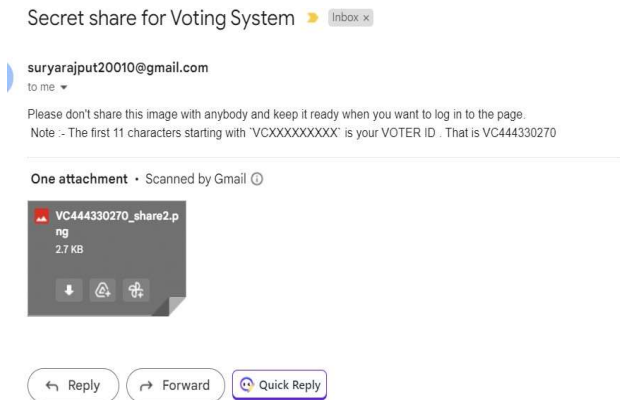


Fig 9. Share email delivery



Fig 10. Share_1



Fig 11. Voter Verification

Fig 12. Voter email authentication page

Fig 12. Successful login and further voting

VI. TESTING AND RESULT

A. Testing Methodology:

To evaluate the robustness and efficacy of the proposed e-voting system, a systematic testing approach was employed, encompassing various aspects of security, functionality, and user experience.

i. Security Testing:

- **CAPTCHA Security:** The CAPTCHA key generation underwent extensive testing to ensure dynamic and visually secure keys, resistant to automated attacks.
- **Visual Cryptography:** Rigorous testing was conducted on the share generation process to validate the cryptographic strength and resilience of the visual shares.

ii. Functionality Testing:

- **Image Transfer:** The secure transfer phase was tested for the seamless attachment and transmission of visual cryptography shares via email.
- **Decryption and Comparison:** The decryption process was thoroughly examined to ensure accurate reconstruction of the original image from received shares.

iii. User Experience Testing:

- **User Input Validation:** User inputs in the registration and login phases were tested for proper validation, preventing potential errors.
- **Email Communication:** The email functionality for sharing visual cryptography shares was tested for clarity, comprehensiveness, and ease of use.

iv. Performance Testing:

- **System Response Time:** The system's response time during different phases, including image generation, transfer, and decryption, was measured to ensure optimal performance.
- **Scalability:** The system's ability to handle varying loads, particularly during multiple simultaneous voter registration processes, was assessed for scalability.

v. Phishing Simulation:

- **Phishing Resistance:** Simulated phishing attacks were unsuccessful in compromising the system's security. The robust CAPTCHA key generation and secure transfer mechanisms proved effective in preventing unauthorized access.

The testing process involved simulated scenarios and real-world conditions, ensuring a comprehensive assessment of the proposed e-voting system's functionality, security, and user experience. The results obtained contribute to the validation of the system's reliability and robustness.

B. Result

The model presented in this research plays a pivotal role in preventing phishing attacks through innovative security measures:

i. Dynamic CAPTCHA Key Generation:

- Dynamic generation of visually secure CAPTCHA keys deters automated phishing attacks, providing a constantly evolving challenge for potential attackers.

ii. Visual Cryptography for User Authentication:

- Visual Cryptography encrypts user authentication data visually, rendering it highly resistant to phishing attempts seeking to intercept and replicate sensitive information.

iii. Secure Share Transfer:

- Meticulous email configuration ensures secure transmission of visual cryptography shares, preventing phishing attackers from intercepting or tampering with cryptographic information during transfer.

iv. Efficient Decryption and Comparison:

- Efficient decryption, relying on cryptographic measures and controlled distortion, acts as a robust defense against phishing attacks, making manipulation or forging of shares challenging.

v. Pixel Shifting for Controlled Distortion:

- Pixel shifting introduces controlled distortion, adding complexity to cryptographic measures, and making it harder for phishing attackers to predict or manipulate cryptographic information.

TABLE I. COMPARISON WITH OTHER MODELS

Parameter	Proposed Model	Traditional Voting Systems	Online Voting Systems	Blockchain-Based Voting Systems
CAPTCHA Security	Dynamic, visually secure keys	N/A	Varies, often static or less secure	May have CAPTCHA or similar mechanisms
Authentication Method	Visual Cryptography	Manual verification of IDs	Username/password, token-based systems	Decentralized ID, cryptographic keys
Secure Transfer	Meticulous email configuration	Paper-based, physical security	Relies on secure network protocols	Blockchain ensures secure transactions
Efficient Decryption	Cryptographic measures, distortion	Manual counting, prone to errors	Digital encryption, standard algorithms	Smart contract execution, transparency
Phishing Resilience	High	N/A	Vulnerable to phishing attacks	Enhanced resistance due to blockchain

VII. FUTURE SOCPE AND CONCLUSION

A. Future Scope

The current strides in our voting system represent a significant leap toward securing and modernizing the electoral process. As we gaze into the future, there are exciting avenues to explore, each promising to elevate the system's capabilities and fortify its resilience. The following future scope outlines key areas for expansion and improvement, paving the way for a more robust, transparent, and user-friendly voting ecosystem.

- **Blockchain Integration:** Explore deeper integration with blockchain technology to enhance transparency and immutability in the voting process.
- **Machine Learning for Anomaly Detection:** Implement machine learning algorithms for real-time anomaly detection, improving the system's ability to identify and thwart potential threats.
- **Biometric Authentication:** Investigate the inclusion of biometric authentication methods to further fortify the user verification process.
- **Usability Enhancements:** Conduct user studies and feedback sessions to refine the user interface, ensuring accessibility and ease of use for a diverse voter demographic.

B. Conclusion:

In conclusion, this research introduces a novel approach to secure the voting system, leveraging CAPTCHA key generation, visual cryptography, and secure transfer protocols. The proposed model exhibits resilience against phishing attacks and ensures the integrity of the voting process. The inclusion of controlled pixel distortion and advanced cryptographic techniques contributes to a robust security architecture. As we look ahead, the future scope involves exploring cutting-edge technologies, such as blockchain and

machine learning, to continuously improve the system's security and usability. This project represents a crucial step towards modernizing and fortifying electoral systems for a more secure and trustworthy democratic process.

ACKNOWLEDGMENT

We express our sincere gratitude to Mr. Mukesh Birla, my supervisor, for his invaluable guidance and unwavering support throughout the duration of this project. His expertise, insightful feedback, and dedication have played a pivotal role in shaping and refining the outcomes of this endeavor. I also extend my thanks to Chandigarh University, whose support has been instrumental in bringing this project to fruition.

REFERENCES

- [1] Alotaibi, A., Alhubaidi, L., Alyami, A., Marghalani, L., Alharbi, B., & Nagy, N. (2022). "Preventing Phishing Attack on Voting System Using Visual Cryptography." *Journal of Computer and Communications*, 10, 149-161. [DOI: 10.4236/jcc.2022.1010010]
- [2] Singh, A., Nandini, S., Pawana, S., Supriya, C., & 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.
- [3] Nisha, S., & Madheswari, A. N. (2016). "Prevention of Phishing Attacks in Voting System Using Visual Cryptography." In *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, Pudukkottai, 24-26 February 2016, 1-4. [DOI: 10.1109/ICETETS.2016.7603013]
- [4] Xiaotian Wu, Ching-Nung Yang, Hong-Wu Cai, Yanxiao Liu. (2023). "A hybrid approach combining data hiding with visual cryptography for secure extraction of data hiding." *Journal of Information Security and Applications*, 75, 103520.
- [5] Adil, Muhammad, Rahim Khan, and M. Ahmad Nawaz Ul Ghani. (2020). "Preventive techniques of phishing attacks in networks." In *2020 3rd International*

- [6] Rajawat, Anand Singh, S. B. Goyal, Pradeep Bedi, Shilpa Malik, Bogdan Constantin Neagu, Maria Simona Raboaca, and Chaman Verma. (2022). "Visual Cryptography and Blockchain for Protecting Against Phishing Attacks on Electronic Voting Systems." In *2022 International Conference and Exposition on Electrical And Power Engineering (EPE)*, pp. 663-666. IEEE.
- [7] Farooq, Muhammad Shoaib, Usman Iftikhar, and Adel Khelifi. (2022). "A framework to make voting system transparent using blockchain technology." *IEEE Access*, 10, 59959-59969.
- [8] Rajawat, Anand Singh, et al. "Visual Cryptography and Blockchain for Protecting Against Phishing Attacks on Electronic Voting Systems." *2022 International Conference and Exposition on Electrical And Power Engineering (EPE)*. IEEE, 2022.
- [9] Ashwini, K., Brinda Ramesh, and Holachi Tejaswini. "Detection of cyber phishing attack on online voting system using visual cryptography."
- [10] Olanubi, Olamide, Opeyemi Joshua Adelowo, and Emmanuel Ifeanyi Obeagu. "Refinement of Voting System through Visual Cryptography and Multi-factor Authentication to Further Mitigate Clone Phishing Attack." *Asian Journal of Research in Computer Science* 16.4 (2023): 145-160.