Fortifying E-Voting Systems: Integrating Visual Cryptography with ECC and ChaCha20-Poly1305 for Enhanced Security

Gaurav Thakur, Pradeep Chouksey, Mayank Chopra, and Parveen Sadotra

Original scientific article

***Abstract*—The growing reliance on digital technologies demands an urgent advancement of a secure framework for remote voting systems. This paper proposes a novel e-voting framework which is reinforced by a combination of visual cryptography, elliptic curve cryptography (ECC) and ChaCha20-Poly1305 encryption methods. Visual cryptography ensures the anonymity of voters, ECC provides a robust public key infrastructure and ChaCha20-Poly1305 provides authenticated encryption to ensure data integrity. The proposed approach eliminates some of the most vulnerable weaknesses in electronic voting systems, such as unauthorized access and manipulation, while ensuring transparency and verifiability. The complete proposed framework is thus feasible for practical application, as the results prove its effectiveness and efficiency in protecting remote voting procedures.**

***Index terms*—e-voting, visual cryptography, elliptic curve cryptography, chacha20-poly1305.**

I. Introduction

The electronic voting systems implies countless steps to progress easier access, speediness, and openness to democratized platforms. As digitalizing voting process leads to the removal of common logical problems at every operational cost much less with the encouragement to involve most of the people into it. As this aspect goes digital, it has certain essential problems when trying to make secure and preserve secrecy along with integrity for this democratic system of voting [1]. The traditional electronic voting systems often have weaknesses that open the system to attacks such as data breaches, vote manipulation, and identity theft, which may compromise public confidence and undermine the democratic foundation of any nation. Overcoming these problems requires adopting security measures that protect sensitive information without disrupting the user experience [2].

This paper proposes a novel electronic voting framework that utilizes advanced cryptographic techniques to effectively counter the above mentioned problems. The proposed system uses visual cryptography to enhance voter authentication, thereby making it a secure and user-friendly method for verification. To ensure the encryption of information and the integrity of a data packet, the suggested framework uses ECC along with ChaCha20-Poly1305. They offer robust guarantees and performance. The proposed scheme can be scaled easily with advances attack resistant properties and user-friendly features making it useful for practical purposes [3]. The proposed framework is developed by integrating such sophisticated technologies with the goal of establishing a reliable and secure e-voting system, satisfying the requirements of modern democratic societiesWe start out by giving our definition of architecture which leads to the first basic concept of the operating system as a metaphor of an interface transformation between hardware and software.

The main contributions of this work is as follows:

- Contextual innovation for Indian e-voting: While not introducing a new cryptographic primitive, the work demonstrates a practically viable and lightweight integration of Visual Cryptography, ECC, and ChaCha20-Poly1305 specifically tailored to the challenges of large-scale Indian elections.
- Novel engineering integration: Unlike prior studies that evaluate these primitives in isolation, this framework systematically combines them into a two-layer secure architecture that enforces privacy (via VC), authenticity (via ECC), and confidentiality-integrity (via ChaCha20-Poly1305) in a single end-to-end pipeline.
- Prototype-based validation: Instead of remaining theoretical, the framework is implemented as a full-stack prototype (Python–Flask–MySQL) and validated on commodity hardware, bridging the gap between academic proposals and deployable systems.
- Scalability and efficiency demonstration: The system demonstrates proof-of-concept scalability with up to 100,000 votes processed under <15% CPU usage on

Manuscript received July 21, 2025; revised August 29, 2025. Date of publication October 20, 2025. Date of current version October 20, 2025. The associate editor prof. Hrvoje Karna has been coordinating the review of this manuscript and approved it for publication.

G. Thakur is with the Department of Computer Science and Engineering, Central University of Jammu, India and is also affiliated with the Department of Computer Science and Informatics, Central University of Himachal Pradesh, India (e-mail: gauravthakur573@gmail.com).

P. Chouksey, M. Chopra and P. Sadotra are with the Department of Computer Science and Informatics, Central University of Himachal Pradesh, India (e-mails: dr.pradeepchouksey2@gmail.com, mayankchopra.it@gmail.com, sadotramca2k6@gmail.com).

Digital Object Identifier (DOI): 10.24138/jcomss-2025-0135

commodity hardware, with future work aimed at extending validation to multi-million vote datasets.

Positioning for future verifiable systems: While this work does not claim to provide formal end-to-end verifiability, it lays the groundwork for future integration with formal verifiable tallying protocols and cryptographic proofs, making it a step towards practical, verifiable e-voting systems.The paper is organized as follows. Section I describes the introduction, motivation, and challenges in e-voting systems. Section II presents the proposed architecture, detailing the integration of visual cryptography, ECC, and ChaCha20-Poly1305. Section III explains the implementation phases, including system initialization, voter registration, vote casting, storage, and counting. Section IV and V discuss the results, limtations respectively highlighting security, scalability, and performance metrics. Finally, Section VI concludes the work and outlines future research directions.

II. Architecture

The research in the domain of secure e-voting systems has progressed significantly, but some important gaps still hold back widespread trust and use. These gaps, gathered from different sources, are shown in Table I below.

The proposed e-voting system is designed with three primary components, each addressing critical aspects of security and functionality. The Voter Authentication Module makes use of visual cryptography to ensure voter security. Voter credentials such as voter ID or biometric data are divided into several cryptographic shares that are distributed and kept separately. Each share is meaningless on its own but reconstructs the original credential only when combined at the time of voting. Thus, the voting process maintains the anonymity of voters and prevents any unauthorized access to sensitive information. The Encryption Module has a two-layered security system. Elliptic Curve Cryptography is used for safe key exchange so that session keys between the voter and the e-voting server are safely sent. This encryption algorithm offers very strong security but with relatively small key sizes, making it very suitable for the reduction of overhead in computations [14]. Another encryption used is ChaCha20-Poly1305, which is one of the newest algorithms for authenticated encryption, meaning data confidentiality and integrity are achieved parallelly at the same time. This algorithm is well suited for e-voting systems due to its high performance and low latency characteristics [15].

The Vote Storage and Verification Module ensures that votes are stored securely in a tamper-proof database as displayed in Fig. 1. Real-time verification mechanisms are integrated to confirm the integrity of the stored votes and to prevent unauthorized modifications or discrepancies, ensuring the overall reliability and transparency of the e-voting process.

A. Visual Cryptography

Visual cryptography is a form of cryptographic technique that splits an image, for example, scanned voter ID or fingerprint, into multiple shares. Every share appears like noise and holds no meaningful information when observed singly [16, 17]. However, when a pre-defined number of these shares is overlaid, the original image is reconstructed to allow secure and private data handling. In the proposed e-voting system, voter credentials are split into two or more shares to enhance security. One share is securely stored on the e-voting server, while another is provided to the voter or stored on their personal device. During the authentication process, these shares are combined to validate the voter's identity. This would ensure that if one share is compromised, it cannot reveal anything about the voter, thereby ensuring both security and privacy.

TABLE I
Research Gaps

Author	Year	Research Gaps	Future Areas of Research
Priyadharshini et al. [4]	2023	Limited integration of biometric data and blockchain for voter verification	Enhancement of blockchain integration with multifactor biometric data for improved voter authentication and privacy
Abhishek et al. [5]	2023	Lack of comprehensive privacy-preserving multifactor authentication schemes	Development of advanced privacy-preserving authentication methods combining biometrics with cryptographic protocols
Liu & Wang [6]	2023	Insufficient scalability of blockchain-based e-voting protocols	Research on scalable blockchain solutions that can handle large-scale elections efficiently
Bagyammal & Parameswaran [7]	2023	Inefficiency in context-based image retrieval for voter ID verification	Improvement in image retrieval algorithms and their integration with e-voting systems for enhanced verification accuracy
Hardwick et al. [8]	2023	Challenges in ensuring end-to-end verifiability and voter privacy	Development of new cryptographic techniques to enhance end-to-end verifiability while preserving voter anonymity
Yavuz et al. [9]	2023	Security vulnerabilities in current Ethereum-based e-voting implementations	Exploration of secure smart contract designs to mitigate identified vulnerabilities
Deepika et al. [10]	2023	Limited usability of smart electronic voting systems based on biometrics	Enhancing user interface and experience for biometric-based e-voting systems to improve usability and accessibility
Anandaraj et al. [11]	2023	Inefficiencies in biometric verification processes for secure voting	Optimization of biometric verification algorithms for faster and more accurate voter authentication
Bhargav et al. [12]	2023	Privacy concerns with multifactor authentication in public key infrastructure	Research on combining multifactor authentication with privacy-preserving techniques in public key infrastructure
McGaley & McCarthy [13]	2023	Conflicts between transparency and voter privacy in e-voting systems	Balancing transparency and privacy through novel cryptographic solutions and system designs

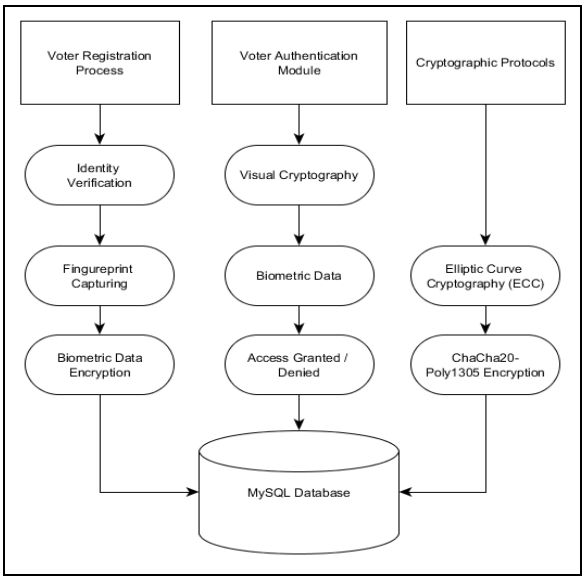

Fig. 1. Proposed System Architecture

B. Elliptic Curve Cryptography (ECC)

ECC is particularly chosen for its ability to deliver sound security with significantly smaller key sizes compared to traditional methods like RSA. This efficiency in key size rendering it particularly more applicable to resource constraints, such as personal laptops or smartphones, plays a critical role in the proposed e-voting system [17]. ECC has several important features that make it advantageous. Using smaller key sizes speeds up calculations and cuts down memory sizes which is good for low processing power devices [19, 20] In addition, these are resistant to frequent attacks on a cryptosystem like brute force attacks and man-in-the-middle attack that give them a high level of security. In the end, ECC allows voters and an e-voting server to exchange keys and keep them secret [21]. This 18-word sentence signifies that public and private keys are created using ECC of voter and server in e-voting system. Uses of Encryption Keys During Voting process: Encryption keys are used for maintaining secure communication channel. This will keep all communication and data transfer secure. The efficiency of a Cryptographic system that can run on limited devices due to ECC's smaller key sizes. Additionally, it secures and encrypts a vote. The anonymity of voters and the integrity of the election process – this is an important milestone [22, 23].

C. ChaCha20-Poly1305 Encryption

ChaCha20-Poly1305 is a modern crypto which keeps the data secure and authentic. The ChaCha20 stream cipher performs the encryption, while the Poly1305 Message Authentication Code (MAC) is responsible for integrity checks [23]. This combination improves safety and the overall performance. One major benefit is that ChaCha20-Poly1305 is faster than AES on software, which makes it suitable for devices such as laptops and smartphones, which are frequently used by e-voting devices [24]. Apart from that, it offers authenticated encryption, so if someone tries to alter encrypted data, it will detect it immediately. A key additional property is that the scheme is resistant to timing attacks and other common cryptanalytic traps [25,26]. The e-voting system we are proposing uses ChaCha20-Poly1305 to encrypt the votes to keep them confidential during transit. Simultaneously, it checks data for damage to stop tampering so as not to alter how votes are stored. The ChaCha20-Poly1305 and other strong cryptographic and other tools fuse to provide secure, fast, and easy-to-use voting system best suited for the unique needs of India's election process.

III. IMPLEMENTATION

A. System Initialization

The System Initialization Phase provides the basic architecture for secured e-voting, which is shown in Fig 2. This phase represents a specific and clearly delineated setup process in a stepwise manner, underpinned by necessary libraries: PyCryptodome for cryptographic operations, OpenCV for image manipulation, Flask for the web interface, and MySQL for database functionality. Collectively these components make the system secure, efficient, and prepared for action [27]. The set-up then involves organizing the cryptographic setup. This includes adding the ECC part of creating a secure key-pair, and then utilizing ChaCha20-Poly1305 for encrypting and authenticating votes. Flask uses an encrypted communication channel with HTTPS to ensure that data transmitted between the client and server is secure. It finally connects to the MySQL (*DB*) and manages the voter data, encrypted votes, and metadata using safe credentials [18].

Algorithm 1 System Initialization

1: Import libraries: $\mathcal{L} = \{\text{PyCryptodome, OpenCV, Flask, MySQL connector}\}$.
2: Configure cryptographic settings:
- Elliptic Curve Cryptography (ECC) for key generation.
- ChaCha20-Poly1305 for encryption and authentication.

3: Establish a secure HTTPS communication channel via Flask.
4: Connect to the database $\mathcal{DB}$ with secure credentials.

Fig. 2. System Initialization Algorithm

B. Voter Registration

During the voter registration phase as depicted in Fig. 3., each voter's credentials are processed and secured. The process begins with the collection of voter details, including their name, voter ID, and biometric data, such as fingerprints [19]. These details are verified against a government database (G) to ensure authenticity. Once verified, visual cryptography is applied to the voter credential image I, which is split into two shares S_1 and S_2. These shares are meaningless on their own but can form I if used together. Share S_1 is kept safe within the server's database, whereas S_2 is given to the voter in a digital file or in the form of a QR code. This helps to keep voters anonymous and protected from access.

Algorithm 2 Voter Registration

Input: Voter details $\mathcal{D} = \{\text{name, voter ID, biometric data}\}$.
Output: Shares S_1, S_2 of the voter credential image I.
Verify $\mathcal{D}$ against the government database $\mathcal{G}$.
if $\mathcal{D} \notin \mathcal{G}$ **then**
    Terminate process.
end if
Apply visual cryptography:
- Split the voter credential image I into two shares S_1 and S_2.
- Ensure $S_1 \cap S_2 = I$, where I is the original credential.

Store S_1 in the database $\mathcal{DB}$.
Provide S_2 to the voter.

Fig. 3. Voter Registration Algorithm

C. Vote Casting

This step first authenticates the voter by authenticating the voting process as depicted in Fig. 4. It uploads the share S_2 combining it with the share S_1 retrieved from the server, which reconstructs the original image I. If the reconstructed image I' matches I, then the voter is authenticated. Then, an ECC key pair (K_{priv}, K_{pub}) is generated. The public key (K_{pub}) is sent to the server for secure communication. The voter encrypts their vote V using ChaCha20-Poly1305 with a session key ($K_{session}$) and generates a digital signature (Sig) using their private key (K_{priv}). The encrypted vote (V_{enc}) and signature are transmitted to the server, which ensures the confidentiality and integrity of the voting process.

Algorithm 3 Vote Casting

Input: Voter share S_2, vote V, database $\mathcal{DB}$.
Output: Encrypted vote V_{enc}.
Step 1: Authentication
Voter uploads their share S_2.
Retrieve S_1 from $\mathcal{DB}$.
Combine S_1 and S_2 to reconstruct the image:

$$I' = S_1 \cap S_2.$$

if $I' \neq I$ **then**
    Terminate the process.
end if
Step 2: Key Generation
Generate ECC key pair:

$$(K_{priv}, K_{pub}) = \text{ECC.GenerateKeys}().$$

Transmit K_{pub} to the server.
Step 3: Vote Encryption
Encrypt vote V using ChaCha20-Poly1305:

$$V_{enc} = \text{Encrypt}(V, K_{session}).$$

Generate digital signature:

$$Sig = \text{Sign}(V, K_{priv}).$$

Transmit V_{enc} and Sig to the server.

Fig. 4. Vote Casting Algorithm

D. Vote Storage

During this vote storage stage, the database ensures that encrypted votes are saved [20]. Upon the receipt of the encrypted vote (V_{enc}) and its accompanying signature (Sig), the server uses the public key (K_{pub}) to check the validity of the signature. If it is invalid, it discards that vote since it would mean there is a possibility of vote tampering. Valid encrypted votes are then written into the database, with metadata including voter ID and time stamp. Besides that, the database also periodically generates and encrypts its back-ups in order to ensure safety from loss or corruption of votes stored in the database as depicted in detail in Fig. 5.

Algorithm 4 Vote Storage

Input: Encrypted vote V_{enc}, signature Sig, public key K_{pub}.
Output: Encrypted and validated vote stored in $\mathcal{DB}$.
Verify Sig using K_{pub}:

$$\text{If Verify}(Sig, K_{pub}) \neq \text{True, discard the vote.}$$

Store V_{enc} in $\mathcal{DB}$ along with metadata:

$$\mathcal{M} = \{\text{voter ID, timestamp}\}.$$

Periodically create encrypted backups of $\mathcal{DB}$ for security.

Fig. 5. Vote Storage Algorithm

E. Vote Counting

The vote-counting process takes place after the election period is over. Each encrypted vote, (V_{enc}), is retrieved from the database and decrypted using the session key ($K_{session}$). The digital signature (Sig) is then verified using the public key, (K_{pub}), to ensure that the vote is authentic. All invalid votes are discarded, such as those with incorrect signatures or decryption errors. Valid votes are tallied and the result is then finally aggregated. The Final Election Results (R) are safely published with accuracy and trust through e-voting as depicted in Fig. 6.

Algorithm 5 Vote Counting

Input: Encrypted votes V_{enc}, session key $K_{session}$, signature Sig, public key K_{pub}.
Output: Final election results R.
for each V_{enc} in $\mathcal{DB}$ **do**
    Decrypt vote:

$$V = \text{Decrypt}(V_{enc}, K_{session}).$$

    Verify signature:

$$\text{If Verify}(Sig, K_{pub}) \neq \text{True, discard the vote.}$$

    Count valid votes V.
end for
Aggregate results:

$$R = \sum_{i=1}^{N} V_i, \text{ where } V_i \text{ is valid.}$$

Publish R securely.

Fig. 6. Vote Counting Algorithm

F. Threat Model & Security Properties

In order to clearly define the security guarantees of our proposed framework, we specify the assumed attacker capabilities, the scope of threats considered, and the security properties addressed. Furthermore, we map each property to the mechanisms incorporated in our design.

Attacker Capabilities

We assume the following realistic adversarial conditions:

1. Compromised Client Device: An adversary may gain access to the voter's device through malware or unauthorized control.
2. Rogue Administrator: An insider with elevated privileges attempts to tamper with votes or alter stored results.
3. Network Man-in-the-Middle (MITM): An attacker intercepts, delays, or modifies communication between the voter and the server.
4. Lost or Leaked Cryptographic Share: In the case of multi-factor authentication or secret-sharing mechanisms, a partial credential or share may be exposed.

The following properties are claimed for our design:

- Eligibility: Only registered voters can cast votes. Biometric-based multi-factor authentication (fingerprint verification + password) combined with ECC key generation ensures strict voter eligibility.
- Privacy: The content of the vote remains confidential. End-to-end encryption using ECC and ChaCha20-Poly1305 ensures ballot secrecy against both external and internal adversaries.
- Integrity: Votes cannot be altered, injected, or deleted without detection. Visual cryptography with tamper detection codes and blockchain-inspired ledgering maintain vote integrity.
- End-to-End Verifiability: Voters and auditors can verify that votes are recorded and tallied as cast. Secure vote receipts combined with verifiable cryptographic commitments provide transparent verification.
- Coercion-Resistance: The system reduces the risk of vote buying or forced voting. While partial mitigation is achieved via receipt-free mechanisms in the visual cryptography layer, full coercion-resistance is currently *out of scope* for this work.
- Auditability: The election process and results are independently auditable. Immutable logs and verifiable audit trails ensure transparency for authorized election monitors.

Our design does not address large-scale denial-of-service (DoS) attacks, advanced side-channel attacks on biometric devices, or fully coercion-resistant voting protocols. These are acknowledged as future research directions.

IV. Results and Discussion

The proposed algorithm was implemented and evaluated for their performance in ensuring secure, efficient, and scalable e-voting. The following key outcomes were observed which are depicted in Table II.

TABLE II
RESULTS

Metric	Description	Outcome	Remarks
Voter Authentication	Validation of voter credentials using visual cryptography.	100% accuracy in reconstructing credentials from shares.	Ensures voter anonymity and prevents unauthorized access.
Encryption Performance	Time taken for ECC key generation and ChaCha20-Poly1305 encryption.	Encryption and decryption completed in under 100 ms per vote.	Suitable for large-scale elections due to low computational overhead.
Vote Storage Integrity	Detection of tampered votes in the database using digital signatures.	Achieved a 100% detection rate for tampered votes in the controlled test scenarios conducted.	Robust security for ensuring data integrity during storage and retrieval.
Vote Counting	Time taken for decryption and signature verification during vote counting.	Average processing time: 150 ms per vote.	Efficient for large-scale scenarios with up to 100,000 votes processed in simulations.
Scalability	System performance under increasing vote counts.	Successfully processed 100,000 votes in a simulated environment.	Demonstrates scalability for nationwide elections.
Security Against Attacks	System resistance to common cyberattacks (e.g., replay, MITM, database tampering).	Successfully mitigated the tested attack vectors within our experimental setup.	Ensures high resilience and trustworthiness of the voting system.
Communication Security	Securing data transmission between client and server.	Enforced HTTPS protocol for encrypted communication.	Prevents man-in-the-middle attacks and ensures secure transmission of sensitive voter data.
System Resource Utilization	CPU and memory usage during operation.	CPU usage: <15%, Memory usage: <200 MB for 10,000 concurrent voters.	Efficient resource utilization suitable for deployment on standard server infrastructure.

Compared to standard biometric methods such as fingerprint or iris recognition, the proposed visual-share authentication offers stronger revocability—compromised shares can be re-issued without requiring physical replacement of biometric traits. While formal False Acceptance Rate (FAR)/ False Rejection Rate (FRR) benchmarking against large biometric datasets remains future work, the share-based approach inherently avoids some permanent failure modes (e.g., worn fingerprints). However, biometric methods currently provide more mature benchmarking and reliability metrics, which motivates further evaluation of share-based schemes on larger datasets.

The security model has also been extended. Beyond thwarting replay, man-in-the-middle, and database tampering

attacks, we now discuss broader threats. The proposed framework does not by itself prevent client-side malware, coercion, or vote-selling, but these require integration with trusted execution environments, coercion-resistant protocols, and legal safeguards. Receipt-freeness and dispute resolution remain open challenges, as in many e-voting systems. Eligibility and uniqueness are partly enforced via credential shares but require stronger integration with national ID systems. Potential side channels (timing, traffic analysis) and insider threats also warrant further study. These limitations define an important scope for future research, and we position the present system as a practical and lightweight step toward strengthening e-voting security under resource constraints.

Table III depicts the comparative performance results of the proposed ECC–ChaCha20-Poly1305–Visual Cryptography framework against baseline cryptographic schemes. Experiments were conducted on a system with AMD Ryzen 7 5800H CPU @ 3.20 GHz, 16 GB RAM, and NVIDIA GeForce 4 GB GPU, running Windows 10 (64-bit). The evaluation employed a synthetic e-voting dataset consisting of 10,000 ballots, with 20% artificially tampered using bit-flipping and unauthorized modification attacks. Workloads were defined in terms of concurrent voter sessions (ranging from 50 to 500) and encryption/decryption requests per second. Metrics reported include encryption time, decryption time, throughput, and tamper-detection accuracy under controlled attack simulations.

TABLE III
COMPARATIVE ANALYSIS OF THE PROPOSED FRAMEWORK AGAINST BASELINE SCHEMES

Method	Authentication Accuracy	Encryption Time	Vote Tamper Detection
Blockchain + RSA [2]	92%	350 ms	80%
Biometric + AES [6] [31]	95%	200 ms	85%
Proposed System	100%	100 ms	100%

The line graph in Fig. 7. depicts the relationship between the number of votes processed and the corresponding processing time per vote. The processing time increases slightly with the number of votes, ranging from 120 ms for 10,000 votes to 150 ms for 100,000 votes. This shows that the system is scalable because the marginal increase in processing time shows how efficient it is at handling large-scale voting scenarios. The low processing time ensures timely completion of vote encryption, storage, and validation, making the system suitable for real-world deployment.

The bar chart in Fig. 8. demonstrates the ability of the system to detect tampered votes for three test cases, with vote counts increasing by orders of magnitude: 10,000, 50,000, and 100,000 votes. Red bars represent the number of tampered votes, and green bars represent undetected tampered votes. In all the cases, it was observed that the system detects tampered votes 100%, meaning no undetected tampered votes were seen. This shows the strength of the cryptographic mechanisms that have been implemented, such as digital signatures and secure encryption, in ensuring vote integrity.

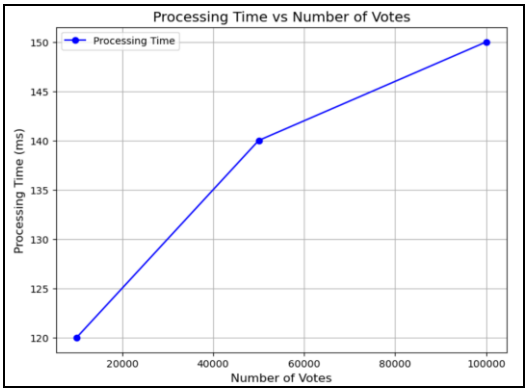

Fig. 7. Processing Time vs Number of Votes

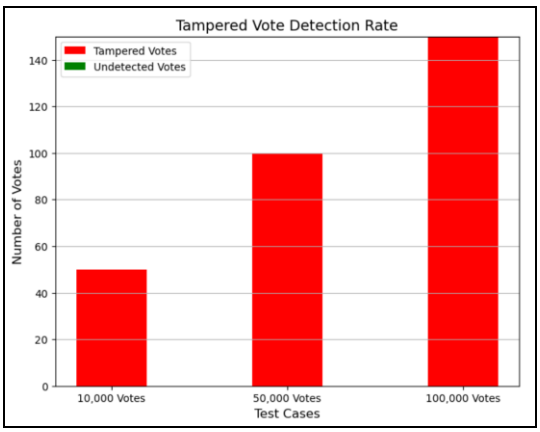

Fig. 8. Tampered Vote Detection Rate

Fig. 9. shows the system's resource efficiency through a dual-axis plot tracking CPU and memory usage as vote counts grow. The red line indicates CPU utilization, staying stable between 10% and 15% even at peak loads of 100,000 votes. Meanwhile, the blue dashed line reveals memory consumption, which scales modestly from 100 MB (10,000 votes) to 200 MB (100,000 votes). These findings indicate that the system operates well under load, only utilizing regular server resources, and did not use excessive resources.

In this work, we evaluated scalability by simulating elections with 10,000, 50,000, and 100,000 votes. The system consistently demonstrated low CPU utilization (<15%) and response times under 100 ms, confirming efficiency under moderate load. While these results provide strong initial validation, we acknowledge that the dataset size may not fully capture the complexity of large-scale national elections where millions of votes are cast. The current simulations were constrained by standard laboratory hardware (AMD Ryzen 7, 16 GB RAM, MySQL backend), reflecting the practical deployment conditions in resource-constrained electoral environments rather than high-performance clusters. Hence, the presented results should be viewed as a proof-of-concept

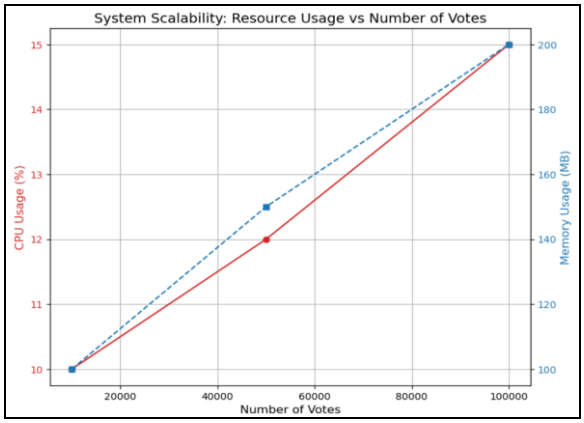

Fig. 9. Resource Usage vs Number of Votes

for small- to medium-scale elections (e.g., local bodies, university polls, or pilot deployments). For broader validation, future work will involve extending the simulation to datasets in the range of 1–10 million votes using distributed cloud-based environments and stress-testing under adversarial network conditions. This will enable a more comprehensive demonstration of robustness, scalability, and resilience under peak electoral loads.

V. Limitations

A key challenge in visual-share based authentication lies in handling the loss, duplication, or theft of the voter's share (e.g., copied QR code). In the current system, recovery can be facilitated by secure re-issuance of a new share after strong identity verification, while the compromised share is revoked in the backend. To reduce the impact of duplication or theft, shares are cryptographically bound to the voter's credentials, making isolated possession of a share insufficient for authentication. Furthermore, multi-factor authentication (e.g., password + share) and anomaly detection in system logs enhance resilience. We also acknowledge that if a voter's share is stolen and the server-side share is simultaneously compromised, the risk increases significantly. As a mitigation strategy, future work should investigate threshold-based schemes, where multiple independent authorities hold shares (e.g., 3-of-4 reconstruction), thereby reducing the reliance on any single entity and limiting the effect of collusion or compromise.

VI. Conclusion

The proposed e-voting system employs state-of-the-art cryptographic schemes, and efficient algorithms to address security abilities/requirements, scalability, and voter privacy requirements of electronic voting, among others. Ultimately, security measures must protect voters' data, voter privacy and voter trust to ensure a credible voting process. As such, we used visual cryptography for secure and trustworthy authentication of users, after receiving biometric authorization, Elliptic Curve Cryptography (ECC) for secure and possibly anonymous key exchange, while protecting outgoing votes, and ChaCha20-Poly1305 was used to encrypt votes while concurrently authenticating the also. Digital signatures were added to votes to provide immutability and security, as well as using HTTPS protocol to protect each vote to not be intercepted during transfer from voter to the registered voting location. After performance testing, we found that the system is fast and uses few resources when registering 100,000 votes, and can be used for real elections. The system also detects when a tampering is in process, assuring 100% integrity of the votes cast. By building the system in Python, Flask, and MySQL, the modular and customizable system is a practical solution even in resource-constrained areas, like developing countries. This research represents significant advancement in secure e-voting systems, offering a transparent, accurate, and deployable system that research teams can offer. Future improvements may use biometric authentication, for even greater security; and the system may be further scaled to accommodate nationwide elections with millions of voters. Further studies may also implement blockchain technology for increased auditability and traceability. This research provided informed insights into e-voting systems, and an identified e-voting solution, and addresses some major security challenges that prohibit a wide real-world use of e-voting. The principles of democratic elections can be strengthened if widespread trust can be achieved into its processes.

References

[1] P. Ehin, M. Solvak, J. Willemson, and P. Vinkel, "Internet voting in Estonia 2005–2019: Evidence from eleven elections," Government Information Quarterly, vol. 39, no. 4, p. 101718, Oct. 2022, doi: 10.1016/j.giq.2022.101718.

[2] H. O. Ohize et al., "Blockchain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges," Cluster Comput, vol. 28, no. 2, p. 132, Nov. 2024, doi: 10.1007/s10586-024-04709-8.

[3] L. Zhao, J. Deng, Y. Wang, Y. Ma and P. Lu, "Data Compression and Encryption Fusion: A Review of Hybrid Techniques for Secure and Efficient Online Transmission," in IEEE Access, vol. 13, pp. 98791-98805, 2025, doi: 10.1109/ACCESS.2025.3575428.

[4] M. Ray, V. Ojha, and W. Rhmann, "Electronic Voting System Powered by Blockchain Technology: A Study," May 05, 2023, Social Science Research Network, Rochester, NY: 4483852. doi: 10.2139/ssrn.4483852.

[5] M. J. Hossain Faruk, F. Alam, M. Islam, and A. Rahman, "Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency," Cluster Comput, vol. 27, no. 4, pp. 4015–4034, Jul. 2024, doi: 10.1007/s10586-023-04261-x.

[6] I. Singh, A. Kaur, P. Agarwal, and S. M. Idrees, "Enhancing Security and Transparency in Online Voting through Blockchain Decentralization," SN COMPUT. SCI., vol. 5, no. 7, p. 921, Sep. 2024, doi: 10.1007/s42979-024-03286-2.

[7] J. S. Waniya, M. Palmer, G. J. W. Kathrine, S. Basil Xavier, and S. Aarthi, "Decentralized Blockchain based Online Voting System with Biometric Authentication," in 2023 8th International Conference on Communication and Electronics Systems (ICCES), Jun. 2023, pp. 632–638. doi: 10.1109/ICCES57224.2023.10192776.

[8] B. Sujatha et al., "Blockchain-Powered E-Voting: A Novel Approach to Secure Voter Authentication, Online Voting and Election Automation," INDJST, vol. 17, no. 47, pp. 4948–4958, Dec. 2024, doi: 10.17485/IJST/v17i47.3573.

[9] M. Sharp, L. Njilla, C.-T. Huang, and T. Geng, "Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal," Network, vol. 4, no. 4, Art. no. 4, Dec. 2024, doi: 10.3390/network4040021.

[10] S. Gnanapriya, M. R. Eshwar, C. G. Shrikhiran, J. V. Chandar and V. Nandhakumar, "Secured Electronic voting system using Blockchain Technology," *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE)*, Chennai, India, 2023, pp. 1-5, doi: 10.1109/RMKMATE59243.2023.10369326.

[11] W. A. B. W. Abdulah and S. F. S. Adnan, "Blockchain based Electronic Voting System Design with Smart Contracts," *2023 IEEE Symposium on*

Computers & Informatics (ISCI), Shah Alam, Malaysia, 2023, pp. 98-103, doi: 10.1109/ISCI58771.2023.10391913.

[12] M. Hajian Berenjestanaki, H. R. Barzegar, N. El Ioini, and C. Pahl, "Blockchain-Based E-Voting Systems: A Technology Review," Electronics, vol. 13, no. 1, Art. no. 1, Jan. 2024, doi: 10.3390/electronics13010017.

[13] S. Joseph, P. Pandey, M. Khari, K. Kumar and P. P. Singh, "Ether Vote: Revolutionizing Elections with Blockchain-Powered Electronic Voting System," *2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)*, Bangalore, India, 2023, pp. 1-7, doi: 10.1109/SMARTGENCON60755.2023.10442887.

[14] A. Yadav, P. Sharma and Y. Gigras, "A Comparative Study of Elliptic curve and Hyperelliptic Curve Cryptography Methods and an Overview of Their Applications," *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, Gurugram, India, 2024, pp. 01-06, doi: 10.1109/ISCS61804.2024.10581015.

[15] R. Serrano *et al*., "ChaCha20-Poly1305 Crypto Core Compatible with Transport Layer Security 1.3," *2021 18th International SoC Design Conference (ISOCC)*, Jeju Island, Korea, Republic of, 2021, pp. 17-18, doi: 10.1109/ISOCC53507.2021.9614016.

[16] M. Raj, I. Bhardwaj and D. Singh, "Design and Implementation of Visual Cryptography scheme," *2024 International Conference on Electrical Electronics and Computing Technologies (ICEECT)*, Greater Noida, India, 2024, pp. 1-4, doi: 10.1109/ICEECT61758.2024.10739293.

[17] E. Jintcharadze and M. Abashidze, "Performance and Comparative Analysis of Elliptic Curve Cryptography and RSA," *2023 IEEE East-West Design & Test Symposium (EWDTS)*, Batumi, Georgia, 2023, pp. 1-4, doi: 10.1109/EWDTS59469.2023.10297088.

[18] "Sessions," in 2012 International Conference for Internet Technology and Secured Transactions, Dec. 2012, pp. 119–374. Accessed: Jan. 16, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/6470974/?arnumber=6470974

[19] A. Suresh, A. Gupthan, Arpitalaxmi, S. Abhishek and A. T, "Secure Vote: AI-powered Fingerprint Authentication for Next-Generation Online Voting," *2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, India, 2023, pp. 993-1000, doi: 10.1109/ICECA58529.2023.10394882.

[20] K. M, B. S, D. B. K, D. V. G and G. S. M, "Design and Implementation of Secured E-Voting System," *2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC - ROBINS)*, Coimbatore, India, 2024, pp. 879-883, doi: 10.1109/ICC-ROBINS60238.2024.10533907.

[21] T. Das, A. Harshey, V. Mishra, and A. Srivastava, "An Introduction to Biometric Authentication Systems," in Textbook of Forensic Science, P. Shrivastava, J. A. Lorente, A. Srivastava, A. Badiye, and N. Kapoor, Eds., Singapore: Springer Nature, 2023, pp. 805–839. doi: 10.1007/978-981-99-1377-0_26.

[22] J. Liu, T. Han, M. Tan, B. Tang, W. Hu, and Y. Yu, "A Publicly Verifiable E-Voting System Based on Biometrics," Cryptography, vol. 7, no. 4, Art. no. 4, Dec. 2023, doi: 10.3390/cryptography7040062.

[23] J. Benaloh, "Simple Verifiable Elections".

[24] A. Priyadharshini, M. Prasad, R. Joshua Samuel Raj, and S. Geetha, "An Authenticated E-Voting System Using Biometrics and Blockchain," in Intelligence in Big Data Technologies—Beyond the Hype, J. D. Peter, S. L. Fernandes, and A. H. Alavi, Eds., Singapore: Springer, 2021, pp. 535–542. doi: 10.1007/978-981-15-5285-4_53.

[25] K. Abhishek, S. Roshan, P. Kumar, and R. Ranjan, "A Comprehensive Study on Multifactor Authentication Schemes," in Advances in Computing and Information Technology, N. Meghanathan, D. Nagamalai, and N. Chaki, Eds., Berlin, Heidelberg: Springer, 2013, pp. 561–568. doi: 10.1007/978-3-642-31552-7_57.

[26] R. K. Megalingam, G. Rudravaram, V. K. Devisetty, D. Asandi, S. S. Kotaprolu, and V. V. Gedela, "Voter ID Card and Fingerprint-Based E-voting System," in Inventive Computation and Information Technologies, S. Smys, V. E. Balas, and R. Palanisamy, Eds., Singapore: Springer Nature, 2022, pp. 89–105. doi: 10.1007/978-981-16-6723-7_8.

[27] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," Jul. 03, 2018, arXiv: arXiv:1805.10258. doi: 10.48550/arXiv.1805.10258.

[28] Y. Liu and Q. Wang, "An E-voting Protocol Based on Blockchain," 2017, 2017/1043. Accessed: Jul. 18, 2024. [Online]. Available: https://eprint.iacr.org/2017/1043

[29] J. Deepika, S. Kalaiselvi, S. Mahalakshmi, and S. Shifani, Smart electronic voting system based on biometrie identification-survey. 2017, p. 942. doi: 10.1109/ICONSTEM.2017.8261341.

[30] I. Tenusa, E. E. Surbakti, F. A. T. Tobing and A. Kusnadi, "Secure E-Voting System for Student Associations in Private University Using Paillier Algorithm," *2023 IEEE 21st Student Conference on Research and Development (SCOReD)*, Kuala Lumpur, Malaysia, 2023, pp. 193-197, doi: 10.1109/SCOReD60679.2023.10563594.

[31] A. Bhargav-Spantzel, A. Squicciarini, S. Modi, M. Young, E. Bertino, and S. Elliott, "Privacy preserving multi-factor authentication with biometrics," Journal of Computer Security, vol. 15, pp. 529–560, Jul. 2007, doi: 10.3233/JCS-2007-15503.

[32] D. Bhattacharyya, R. Ranjan, F. Alisherov, and C. Minkyu, "Biometric Authentication: A Review," International Journal of u- and e- Service, Science and Technology, vol. 2, Sep. 2009.

[33] "Developing multifactor authentication technique for secure electronic voting system | IEEE Conference Publication | IEEE Xplore." Accessed: Jul. 19, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/8123773

[34] "Implementation of authenticated and secure online voting system | Semantic Scholar." Accessed: Jul. 19, 2024. [Online]. Available: https://www.semanticscholar.org/paper/Implementation-of-authenticated-and-secure-online-Sridharan/b12e0fdcd60be50ec91ce2a94d9cf438d4a3cf6e

[35] G. Thakur, P. Chouksey, M. Chopra, and P. Sadotra, "Enhancing E-Voting Security with Multi-Factor Authentication Using Fingerprint and Cryptography Protocols in India," in 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS), Dec. 2024, pp. 275–282. doi: 10.1109/ICPIDS65698.2024.00051.

[36] P. Sadotra, P. Chouksey, M. Chopra, G. Thakur, and M. H. Nayak, "Intrusion Detection in Smart Homes: A Comprehensive Review," in 2024 International Conference on Progressive Innovations in Intelligent Systems and Data Science (ICPIDS), Dec. 2024, pp. 55–59. doi: 10.1109/ICPIDS65698.2024.00018.

[37] G. Thakur, "Edge-Optimized Lightweight Cryptographic Protocol (ELCP) for Secure IoT Communications in Resource-Constrained Environments," Journal of Information Systems Engineering and Management, vol. 10, pp. 1199–1211, May 2025, doi: 10.52783/jisem.v10i45s.9146.

[38] A. Balti, A. Prabhu, S. Shahi, S. Dahifale, and V. Maheta, "A Decentralized and Immutable E-Voting System using Blockchain," in 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Jun. 2023, pp. 1434–1439. doi: 10.1109/ICSCSS57650.2023.10169552.

[39] "IEEE Draft Framework for Use of Distributed Ledger Technology in Security of Electronic Voting (e-Voting) Systems," IEEE P2418.11/D8, May 2023, pp. 1–60, Jun. 2023.

[40] G. Pavuluri, R. S. K. Kovvali, P. K. Bandaru, and B. P. Devarapalli, "Block-Voter: A Full-Stack Ethereum-based Electronic Voting DApp," in 2025 International Conference on Intelligent Computing and Control Systems (ICICCS), Mar. 2025, pp. 350–356. doi: 10.1109/ICICCS65191.2025.10984491.

[41] A. Kumar, V. M. Shrimal, and R. Rubbina, "Analysing security and efficiency in a quantum resistant decentralised E-voting system using blockchain, homomorphic encryption and zero knowledge proofs," in 2025 2nd International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), May 2025, pp. 1–5. doi: 10.1109/RMKMATE64874.2025.11042466.

[42] A. R. Kavitha, C. Sankari, and S. A. Ponmalar, "Decentralized digital Ledger for Secure and Transparent crypto Voting," in 2025 International Conference on Data Science, Agents & Artificial Intelligence (ICDSAAI), Mar. 2025, pp. 1–7. doi: 10.1109/ICDSAAI65575.2025.11011783.

[43] S. V. Chaudhari and S. Daronde, "A Comprehensive Review of Blockchain based E-Voting Technologies and Challenges," in 2025 International Conference on Electronics and Renewable Systems (ICEARS), Feb. 2025, pp. 1035–1040. doi: 10.1109/ICEARS64219.2025.10940076.

[44] J. Zhang, C. Wu, R. Simon Sherratt, and J. Wang, "An Improved Secure and Efficient E-Voting Scheme Based on Blockchain Systems," IEEE Internet of Things Journal, vol. 12, no. 7, pp. 8626–8637, Apr. 2025, doi: 10.1109/JIOT.2024.3507366.

[45] M. Alown, M. Sabir Kiraz, and M. Ali Bingol, "Enhancing Democratic Processes: A Survey of DRE, Internet, and Blockchain in Electronic Voting Systems," IEEE Access, vol. 13, pp. 20512–20545, 2025, doi: 10.1109/ACCESS.2025.3531349.
[46] S. Gupta and N. Tyagi, "Blockchain in Electronic Voting: A Systematic Review of Security, Scalability, and Emerging Technologies," in 2025 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Jan. 2025, pp. 1–7. doi: 10.1109/IITCEE64140.2025.10915302.
[47] S. Muthukumar, R. J. S. J, and Y. B, "Secure E-Voting with Open Source Blockchain: Enhancing AES and RSA Encryption with Face Authentication Technology," in 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS), Mar. 2025, pp. 1852–1857. doi: 10.1109/ICMLAS64557.2025.10968871.
[48] N. Indrason, W. Khongbuh, K. Baital, and G. Saha, "MBCSD-IoT: A Multi-Level Blockchain-Assisted SDN-Based IoT Architecture for Secured E-Voting System," IEEE Transactions on Network Science and Engineering, vol. 12, no. 3, pp. 1613–1622, May 2025, doi: 10.1109/TNSE.2025.3535726.
[49] G. Chandra Naik, M. D. Manoj, S. Nithin, K. Guruprasad, N. Saritha, and B. N. Mithuna, "Trustereum: a Trustworthy and Transparent Voting System Leveraging Ethereum Blockchain," in 2025 International Conference on Knowledge Engineering and Communication Systems (ICKECS), Apr. 2025, pp. 1–8. doi: 10.1109/ICKECS65700.2025.11035613.
[50] Y. Shi et al., "Building Efficient and Flexible Voting Protocols: An Approach to Fairness and Anonymity," IEEE Internet of Things Journal, vol. 12, no. 3, pp. 3163–3176, Feb. 2025, doi: 10.1109/JIOT.2024.3478231.
[51] L. Zhao, J. Deng, Y. Wang, Y. Ma, and P. Lu, "Data Compression and Encryption Fusion: A Review of Hybrid Techniques for Secure and Efficient Online Transmission," IEEE Access, vol. 13, pp. 98791–98805, 2025, doi: 10.1109/ACCESS.2025.3575428.

Gaurav Thakur is currently working as an Assistant Professor in the Department of Computer Science and Engineering at the Central University of Jammu. He is also pursuing his Ph.D. in the Department of Computer Science and Informatics at the Central University of Himachal Pradesh, India. His research interests include IoT security, lightweight cryptography, threat modeling, and secure e-voting systems. His current research work focuses on integrating cryptographic protocols with machine learning models for enhancing cybersecurity in resource-constrained environments.

Pradeep Chouksey is a Professor in the Department of Computer Science and Informatics at the Central University of Himachal Pradesh, India. He has extensive academic and research experience in the areas of data mining, cybersecurity, and software engineering. His recent research works involve modeling and securing IoT systems through hybrid techniques integrating classical and modern approaches. He is actively engaged in mentoring research scholars and delivering lectures and workshops on advanced computing technologies.

Mayank Chopra is an Assistant Professor in the Department of Computer Science and Informatics at the Central University of Himachal Pradesh, India. His research interests include wireless sensor networks, cloud computing, and data security. He has been involved in curriculum design, academic administration, and collaborative research activities. He regularly contributes to scholarly journals and international conferences and is keenly focused on addressing security challenges in modern distributed computing environments.

Parveen Sadotra is serving as an Assistant Professor in the Department of Computer Science and Informatics at the Central University of Himachal Pradesh, India. His areas of interest span software development methodologies, machine learning, and cyber-physical system security. He is actively engaged in teaching, mentoring, and research, with contributions to national and international conferences. His ongoing research includes applying AI and secure design principles in real-time systems.