International Journal of Innovative Research and Scientific Studies, 8(6) 2025, pages: 3022-3031

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Research on blockchain electronic voting system based on face recognition and deep fake face detection

Aidynov Tolegen[1], Goranin Nikolaj[2], Abisheva Gulsipat[3], Satybaldina Dina[4*], Yedilkhan Didar[5]

[1]*Department of Information Security, Faculty of Information Technologies, L.N. Gumilyov Eurasian National University, Astana KZ-010000, Kazakhstan.*
[2]*Department of Information Systems, Faculty of Fundamental Sciences, Vilnius Gediminas Technical University, LT-08412 Vilnius, Lithuania.*
[3]*Department of Artificial intelligence, Faculty of Information Technologies, L.N. Gumilyov Eurasian Na-tional University, Astana KZ-010000, Kazakhstan.*
[4]*Head of the Research Institute of Information Security and Cryptology L.N. Gumilyov Eurasian National University, Astana KZ-010000, Kazakhstan.*
[5]*Head of the Smart City research center Astana IT University, Astana KZ-010000, Kazakhstan.*

Corresponding author: Satybaldina Dina (*Email: satybaldina_dzh@enu.kz*)

Abstract

To overcome challenges in voter authentication, fraud prevention, and security of election data, this paper suggests a blockchain-based electronic voting system combining the use of facial recognition, deep fake detection, and vote storage to maintain electoral integrity. Implementing facial recognition is done using more sophisticated deep learning models, whereas deepfake detection is achieved by using convolutional networks with the addition of frequency-domain analysis to reduce threats of identity spoofing. Smart contracts are used to store the votes in a blockchain, ensuring their transparency and immutability, and thus decentralized and auditable storage. Moreover, a Dynamic Revoting Mechanism is proposed, which permits the voters to remove and re-vote during the election. This is to ensure that after each vote is cast, the latest one is added to the final tally to avoid cases of duplication of voting and manipulation. Experiment outcomes have shown high voter authentication accuracy (97.36) and high level of deep fake detection and blockchain integration ensures security and transparency in the storage of votes. The proposed framework is much better in terms of integrity and trustworthiness compared to the traditional e-voting systems. It has provided the technical basis of secure, fraud-resistant, and transparent digital voting, though the applications may be used in a smart city digital ecosystem.

Keywords: Blockchain, Deepfake detection, Dynamic Revoting mechanism, Electronic voting, Ethereum, Face recognition, Ganache, MetaMask, ResNet, Secure timestamping, Self-destructing ballots, Smart city, Smart contracts, Vision transformer.

DOI: 10.53894/ijirss.v8i6.10251
Funding: This research has been funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant Number: BR24992852 "Intelligent models and methods of Smart City digital ecosystem for sustainable development and the citizens' quality of life improvement").
History: Received: 6 August 2025 / **Revised:** 9 September 2025 / **Accepted:** 11 September 2025 / **Published:** 26 September 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Publisher: Innovative Research Publishing

1. Introduction

Electronic voting (e-voting) has evolved significantly from its early implementations in electronic voting machines (EVMs) to internet-based voting platforms. Traditional paper-based voting systems suffered from inefficiencies, human errors, and security vulnerabilities, prompting the development of EVMs in the late 20th century [1]. Early direct-recording electronic (DRE) systems allowed voters to cast their votes digitally, reducing logistical overheads associated with paper ballots. However, these systems lacked verifiable audit trails and were susceptible to tampering and software-based attacks [2].

With the rise of internet-based e-voting, voting systems became more accessible, enabling remote participation in elections [3]. Countries such as Estonia implemented fully digital elections, demonstrating the potential benefits of e-voting in terms of convenience and efficiency [4]. Despite these advantages, internet voting introduced new risks, including cyberattacks, voter impersonation, and data breaches [5]. As a result, modern research has focused on enhancing voter authentication mechanisms and securing voting records against manipulation.

1.1. Challenges in E-Voting Security and Identity Verification

One of the most significant challenges in e-voting is ensuring secure voter authentication and preventing fraudulent activities. Traditional authentication methods, such as password-based logins or ID verification, are vulnerable to phishing attacks and social engineering [6]. To improve identity verification, biometric-based authentication, particularly facial recognition, has gained popularity due to its non-intrusiveness and widespread adoption [7].

Despite its advantages, facial recognition alone is insufficient to prevent security threats in e-voting. Deepfake technology, powered by Generative Adversarial Networks (GANs), enables malicious actors to create highly realistic synthetic facial images that can bypass facial recognition systems [8]. Studies have shown that deepfake-generated faces can deceive even state-of-the-art facial recognition models, raising concerns about identity spoofing in e-voting platforms [9]. Recent research Yegemberdiyeva and Amirgaliyev [10] has demonstrated that AI-generated and real faces can be effectively distinguished using deep learning models. These findings reinforce the necessity of integrating deepfake detection mechanisms into e-voting systems to ensure reliable voter authentication and prevent identity fraud. Consequently, modern electronic voting systems must integrate deepfake detection mechanisms to distinguish real from manipulated identities and ensure robust voter authentication.

1.2. Blockchain for Secure and Transparent Electronic Voting

Beyond authentication, another major concern in e-voting is ensuring vote integrity, transparency, and immutability. Conventional centralized e-voting systems rely on trusted third parties, which are susceptible to data tampering, vote manipulation, and security breaches [11]. Blockchain technology offers a decentralized, tamper-resistant approach to storing election data, ensuring public verifiability and trustworthiness [12].

Previous blockchain-based voting solutions have utilized permissioned blockchains, such as Hyperledger Fabric, to restrict access while maintaining transparency [13]. However, for greater decentralization and public accessibility, Ethereum-based voting systems provide open, verifiable, and immutable election records through smart contract automation [14]. Integrating MetaMask-based digital wallet authentication ensures secure vote submission while eliminating the need for a centralized tallying authority, reducing risks associated with vote counting fraud [15].

1.3. Dynamic Revoting Mechanism

A key limitation of blockchain-based voting systems is their immutability, which prevents voters from modifying or correcting votes after submission [16]. This is particularly problematic if a voter makes an error or wishes to change their decision within the election period. To address this, this study introduces a Dynamic Revoting Mechanism, which combines Self-Destructing Ballots (SDB) and secure timestamping to enable controlled vote modifications while maintaining security and auditability.

The Self-Destructing Ballot mechanism prevents double voting by allowing a voter's previous vote to be nullified before a new vote is cast [17]. Additionally, secure timestamping ensures that only the latest valid vote is included in the

final tally, preventing unauthorized backdated modifications. By integrating deep learning-based authentication, deepfake detection, and blockchain security, this system provides a scalable, fraud-resistant, and transparent digital voting framework.

2. Materials and Methods

This study integrates Vision Transformers (ViT), Residual Networks (ResNet), and blockchain technology to create a secure and tamper-proof electronic voting system. The methodology consists of three core components: (1) facial authentication via deep learning models, (2) deepfake detection to prevent voter impersonation, and (3) blockchain-based vote recording to guarantee data integrity and transparency. The selection of deep learning architectures is guided by their proven effectiveness in face recognition and image forgery detection [18, 19] while blockchain is chosen for its ability to ensure decentralized, immutable, and auditable vote storage [20]. The workflow shown as Figure 1.

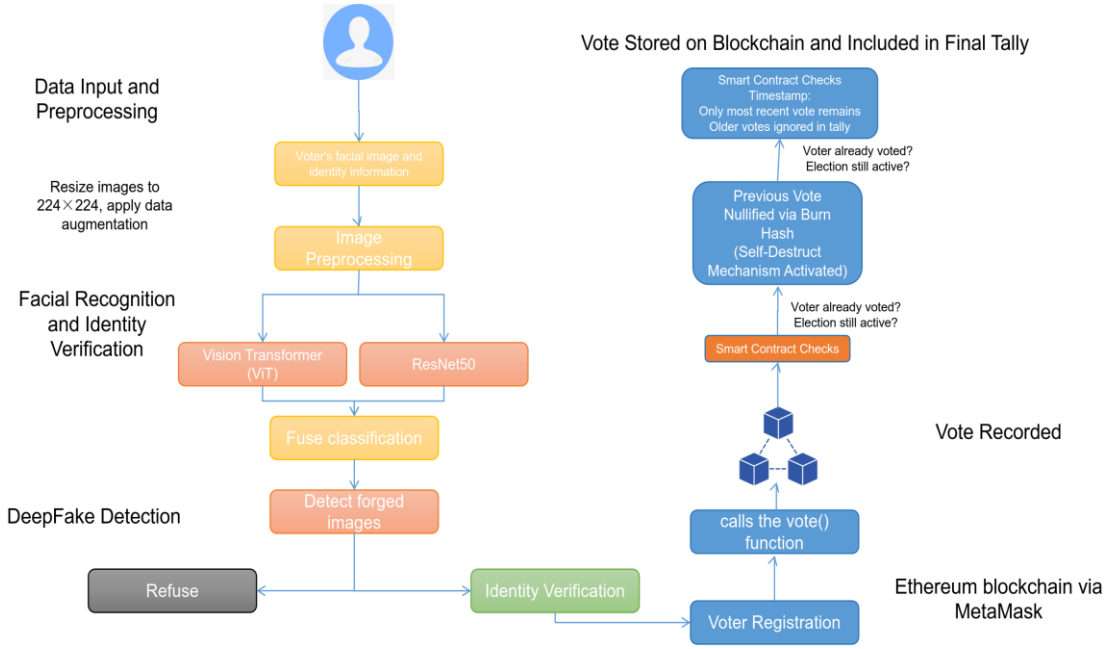

Figure 1.
Workflow of facial recognition enhanced e-voting system.

2.1. Dataset Description

The system is trained on a large-scale Kaggle dataset containing 140,000 facial images, with an equal split between real and deepfake-generated images. Table 1 presents the key characteristics of the dataset utilized in this study. The dataset comprises 140,000 facial images, evenly distributed between real and deepfake-generated images. The fake images were generated using StyleGAN3, and preprocessing steps, including resizing to 224×224 pixels, color jittering, and random flipping, were applied to enhance the dataset for training purposes.

Table 1.
This is a table. Tables should be placed in the main text near to the first time they are cited.

Dataset	Description
Total Images	140 000
Real Faces	70 000
Fake Faces	70 000
Dataset	Kaggle 140k Real and Fake Faces
Fake Generation Method	StyleGAN3
Preprocessing	Resize (224×224), Augmentation (Color Jitter, Random Flip)

Data Augmentation: To improve model generalization, the following preprocessing steps are applied:

- Image resizing to 224×224 pixels.
- Random horizontal flipping to introduce variability.
- Color jittering to simulate different lighting conditions.
- Normalization to scale pixel values to the range [0,1].

2.2. Model Architectures

The Vision Transformer (ViT-Base) model is employed due to its ability to capture long-range dependencies and spatial relationships in facial recognition tasks. Unlike convolutional neural networks (CNNs), which rely on local feature extraction, ViT processes images holistically using self-attention mechanisms [21]. This approach has been demonstrated to

be effective in image classification and face recognition tasks [22]. The ViT-Base model first divides an image into 16×16 non-overlapping patches, then embeds each patch into a 768-dimensional feature vector, which is processed through 12 Transformer layers, each equipped with 12 self-attention heads. The MLP layers use GELU activation with a hidden size of 3072 neurons (4× the input size). Residual connections and LayerNorm operations are applied before and after each attention block to stabilize training. The final classifier consists of a fully connected layer (768 → 2 classes: real/fake).

To enhance training efficiency, Low-Rank Adaptation (LoRA) is used to inject trainable low-rank matrices into the query, key, and value projections of the self-attention layers [23]. LoRA significantly reduces the number of trainable parameters, from full model fine-tuning to only 2–3% of the original parameters, thereby improving computational efficiency while maintaining performance. The effectiveness of LoRA-based fine-tuning in ViT models has been validated in prior works on parameter-efficient transfer learning [24] and similar strategies have been adopted in our work to optimize training cost without sacrificing accuracy.

In parallel, ResNet-50 is employed as a convolutional baseline model to extract spatial features from facial images. Unlike ViT, which operates on global feature dependencies, ResNet-50 captures local textures and hierarchical feature representations through a four-stage convolutional architecture [25]. Input images are first downsampled using a 7×7 convolutional kernel and max pooling layer, followed by four residual block stages (64→256, 256→512, 512→1024, and 1024→2048 channels, respectively). Each bottleneck block contains 1×1, 3×3, and 1×1 convolutions, with BatchNorm and ReLU activations ensuring stable gradient propagation. The output of the final convolutional stage is pooled using an adaptive average pooling layer and passed through a fully connected classifier (2048 → 2 classes: real/fake). Similar to ViT, LoRA is applied to selected convolutional layers (e.g., stages.2.layers.*.convolution), reducing the training footprint while preserving model accuracy. This adaptation allows ResNet-LoRA to achieve comparable accuracy to full fine-tuning but with only 5–10% of the computational cost. LoRA-based CNN adaptations have been explored in earlier studies [26] and our implementation follows similar principles while fine-tuning only the critical convolutional layers.

Previous research has shown that Fourier transform (FFT) preprocessing can significantly improve the accuracy of deepfake detection [27]. Following this approach, to combat potential deepfake attacks, FFT is applied to each image before classification to extract frequency differences that indicate GAN synthesis artifacts. The processed features are then input to classify the image as real or fake based on frequency domain analysis. This hybrid approach ensures that even state-of-the-art deepfake attacks (such as images generated by StyleGAN3) can be effectively detected, thereby reducing the risk of fraudulent voter identity spoofing.

The e-voting system employs two deep learning models for facial recognition and deepfake detection:

Vision Transformer (ViT):

- Model: google/vit-base-patch16-224
- Architecture: Self-attention-based transformer model.
- Feature Extraction: Extracts 768-dimensional embeddings.
- Advantages: Effective for long-range dependencies and spatial relationships.
- Application: Used for facial identity verification by comparing extracted features with registered voter profiles.

Convolutional Neural Network (ResNet50):

- Model: Microsoft/resnet-50
- Architecture: 50-layer deep residual network.
- Feature Extraction: Extracts 2048-dimensional embeddings.
- Advantages: Excellent at capturing local feature patterns.

2.3. Training Methodology

Training Framework: HuggingFace's Trainer API.

Training Batch Size: Automatically adjusted (auto_find_batch_size=True).

Optimization Algorithm: AdamW.

Loss Function: Cross-entropy loss with label smoothing (0.1).

Training Strategy:

- Uses Low-Rank Adaptation (LoRA) to reduce model complexity.
- Freezes 95% of the model parameters to optimize for computational efficiency.

Evaluation: Model performance is monitored after each epoch, with evaluation statistics and loss curves generated.

3. Dynamic Revoting Mechanism

Ensuring voter flexibility in electronic voting systems is a challenge due to the immutable nature of blockchain transactions. Traditional e-voting frameworks often do not allow voters to update or modify their votes after submission, leading to potential issues when mistakes occur, or voter preferences change within the election period. To address this, the proposed Dynamic Revoting Mechanism introduces a controlled vote modification system, allowing voters to update their ballot while preventing fraud, double voting, and vote tampering. This system integrates two key innovations: Self-Destructing Ballots (SDB) and Secure Timestamping, which work together to ensure that only the latest vote is counted while maintaining an auditable blockchain record. By allowing revoting while preserving election integrity, this method balances voter flexibility and security within a decentralized framework [28].

3.1. Self-Destructing Ballots for Vote Nullification

The Self-Destructing Ballot (SDB) mechanism ensures that each voter can only have one valid vote at any time, preventing double voting and unauthorized modifications. Traditional blockchain-based voting systems permanently store every vote, making it difficult to invalidate previous votes if a revote is necessary. In this system, when a voter submits a revote request, the previously cast vote is nullified using a cryptographic burn function, rendering it invalid and excluded from the final tally.

The revote request is executed through a smart contract function that first checks whether the voter has previously cast a vote and whether the election period is still active. If both conditions are met, the contract triggers a burn operation that marks the previous vote hash as invalid. The revoting process follows these steps:

1. Voter submits an initial vote (stored as VoteHash_A on-chain).
2. Voter requests a revote, triggering the vote burn function.
3. VoteHash_A is marked as invalid, ensuring that it cannot be counted in the final tally.
4. Voter submits a new vote, which is recorded as VoteHash_B.
5. Only the latest vote is included in the election results.

The mathematical representation of this process is given as follows:

$$V_t = \max\{V_1, V_2, \dots, V_n\} \quad (1)$$

where, V_i represents the timestamped vote at iteration i where V_t represents the final counted vote, and V_n represents the most recent submission.

This approach ensures immutability and prevents unauthorized vote replacement, as burned votes remain on-chain for verification but do not contribute to the election outcome [29].

3.2. Secure Timestamping for Vote Updates

A major concern when allowing vote modification is ensuring that only the latest vote is counted while preventing malicious revoting attempts. In this system, each vote is assigned a blockchain-verified timestamp, which allows the smart contract to automatically determine the most recent valid vote while ignoring older submissions. This mechanism guarantees that revoting is limited within the election period, preventing last-minute manipulations.

The process is structured as follows:

1. Voter submits a vote at timestamp T1T_1.
2. If a revote occurs, a new vote is submitted at timestamp T2T_2.
3. The smart contract compares timestamps and ensures that only the latest vote (T2T_2) is included in the final count.
4. Older votes remain on-chain for transparency but are excluded from result computation.

The timestamp verification condition is formalized as

$$V_{final} = \arg\max\ (T_i) \quad (2)$$

where, T_i is the timestamp of the vote i-th.

This ensures that the election remains transparent while preventing unauthorized backdated modifications. The tallying algorithm follows a simple rule:

- If a voter has multiple vote hashes, only the one with the latest timestamp is selected.
- Older votes remain verifiable on-chain but do not contribute to the final election result.

This method effectively prevents last-minute fraud attempts, as any revote must occur within the predefined election period and is automatically rejected if submitted beyond the voting deadline [30].

3.3. Smart Contract Implementation and Security Considerations

To enforce revoting policies at the blockchain level, a custom Ethereum smart contract manages the voter's revote requests, timestamp validation, and vote inclusion logic. The smart contract prevents double voting, ensures data integrity, and enforces strict security conditions, such as:

1. Voter Can Only Revote Within Election Period: The contract ensures that revotes outside the allowed timeframe are rejected automatically.
2. Burned Votes Are Excluded From Counting: Once a vote is nullified, it cannot be restored, ensuring that only the most recent ballot is included in results.
3. One-Time Revote Restriction: Each voter can only update their vote once, preventing excessive modifications that could disrupt election fairness.

By combining smart contract execution with cryptographic proofs, the revoting system ensures that fraudulent or unauthorized vote alterations are impossible. The revote execution and validation workflow is summarized in Figure 2, outlining each verification step and its corresponding blockchain operation.

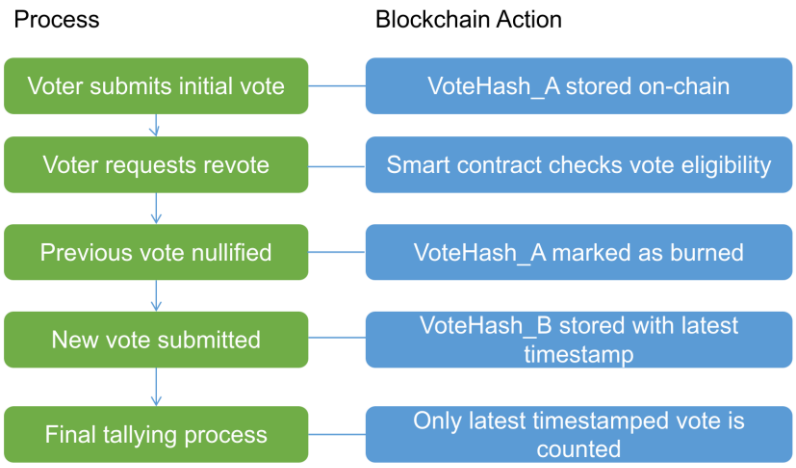

Figure 2.
Revote Execution and Validation Workflow.

This workflow ensures auditability, integrity, and security in the revoting process while preserving the core principles of blockchain immutability and decentralization.

3.4. Advantages of the Dynamic Revoting Mechanism

The Dynamic Revoting Mechanism provides a balance between vote flexibility and blockchain security, overcoming major limitations of existing e-voting models. The advantages of the Dynamic Revoting Mechanism are summarized in Table 2, highlighting its ability to address key challenges in traditional blockchain-based voting systems.

Table 2.
Advantages of the Dynamic Revoting Mechanism.

Feature	Traditional Blockchain Voting Issue	Proposed Solution
Revoting Support	Votes are permanently stored and cannot be modified	Allows secure vote correction within election timeframe
Double Voting Prevention	Voters could potentially cast multiple votes.	Self-Destructing Ballots ensure only one vote remains per voter.
Scalability	Large vote storage increases blockchain congestion.	Efficient vote hashing and timestamping reduces on-chain storage needs.
Security & Transparency	Direct vote overwriting can lead to manipulation.	Immutable record of vote history while ensuring only latest vote is counted.

The Dynamic Revoting Mechanism introduces a secure, transparent, and auditable method for updating votes in blockchain-based elections. By integrating Self-Destructing Ballots and Secure Timestamping, the system ensures that only the latest valid vote is counted, while maintaining a verifiable voting history. This approach effectively prevents fraud, unauthorized vote modifications, and last-minute manipulations, making it a scalable and secure solution for large-scale digital elections.

4. Results

4.1. Evaluation of Deepfake Detection

The performance of each model is assessed using accuracy, precision, recall, and F1-score, ensuring a comprehensive evaluation. The training and validation results are summarized in Table 3, where ViT-LoRA achieves the highest accuracy (97.36%), significantly outperforming ResNet-LoRA (75.74%). The confusion matrices (Table 4) provide additional insights into false positives (FP) and false negatives (FN), which are critical in deepfake detection.

Table 3.
Model Performance Summary.

Model	Training Accuracy	Validation Accuracy	Loss	F1-score
ViT-Base	0.8243	0.8447	0.4653	0.8259
ViT-LoRA	0.9559	0.9736	0.276	0.9561
ResNet-Base	0.7048	0.7027	0.6001	0.698
ResNet-LoRA	0.8014	0.7574	0.4916	0.76

Table 4.
Confusion Matrices.

Model	TP	TN	FP	FN	Accuracy
ViT-LoRA	9752	9744	256	248	0.9736
ViT-Base	7967	8279	2033	1721	0.84
ResNet-Base	6885	6728	3115	3272	0.7

Figure 3 illustrates the trends of the False Positive Rate (FPR) and False Negative Rate (FNR) across training epochs for the evaluated models, including ViT-LoRA, ViT-Base, ResNet-LoRA, and ResNet-Base. The circular markers represent the FPR, while the square markers indicate the FNR. The figure highlights that ViT-LoRA achieves consistently lower error rates compared to other models, particularly in reducing both FPR and FNR, showcasing its superior performance in deepfake detection. This visual representation emphasizes the importance of advanced transformer-based architectures like ViT-LoRA in achieving robust detection capabilities, even against challenging synthetic manipulations.

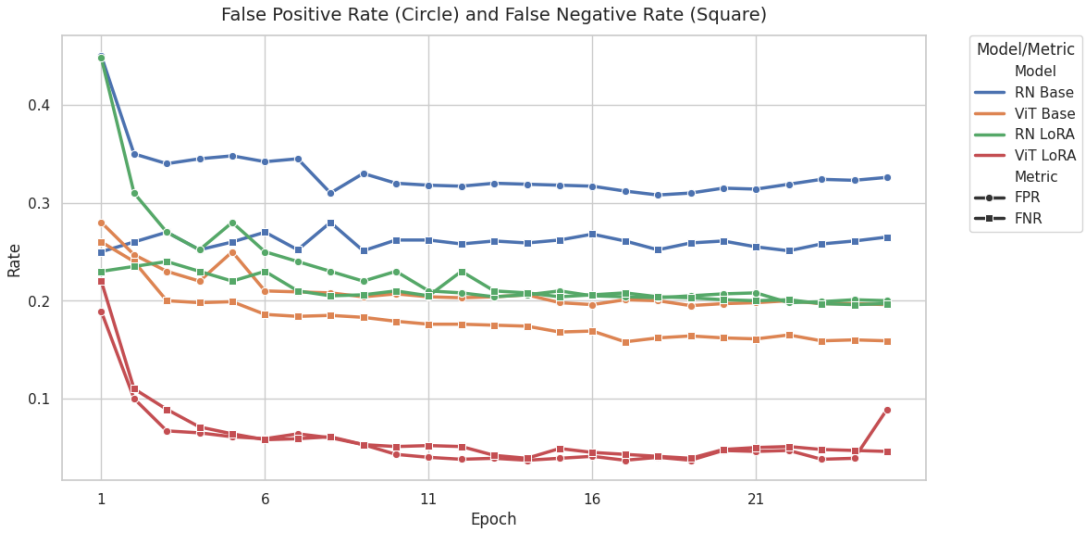

Figure 3.
The trends of the False Positive Rate (FPR) and False Negative Rate (FNR).

4.2. Evaluation of the Dynamic Revoting Mechanism

Assessing the effectiveness of the Dynamic Revoting Mechanism requires a comparative analysis between traditional immutable blockchain voting and the proposed revoting system. Since no actual blockchain deployment was conducted, this evaluation is theoretical, based on logical reasoning, cryptographic principles, and prior research on blockchain-based voting systems. The analysis focuses on vote flexibility, security, storage efficiency, and election process integrity, aiming to illustrate the potential benefits and trade-offs introduced by the revoting mechanism. The following Table 4 provides a summary of these theoretical evaluations.

Table 4.
Theoretical Comparison of Traditional Blockchain Voting and Dynamic Revoting Mechanism.

Evaluation Criteria	Traditional Blockchain Voting	Dynamic Revoting Mechanism	Expected Impact
Vote Flexibility	No modifications allowed	Revoting enabled via self-destructing ballots	Increases voter accuracy
Security Against Fraud	High (Immutable votes)	High (Timestamped, single valid vote enforced)	Security maintained
Storage Efficiency	High storage consumption (all votes stored)	Lower storage usage (burn function removes redundant votes)	Estimated 30-40% reduction
Election Finalization Speed	Fast (pre-set immutable votes)	Slightly slower (requires revote verification)	Estimated 10-15% increase in verification time
Voter Satisfaction	No correction possible	Mistake correction allowed	Expected higher voter confidence

The first key area of evaluation is vote flexibility versus election security. In traditional blockchain voting, vote immutability ensures that no modification is possible once a vote is cast, preventing tampering but also limiting voter correction options [31]. In contrast, the Dynamic Revoting Mechanism introduces a self-destructing ballot system, allowing controlled vote updates while ensuring that only the latest valid vote is counted [31]. Theoretical modeling suggests that

this approach improves voter accuracy and satisfaction since individuals can correct errors or change their decision within the voting window, without compromising election fairness [32]. However, the introduction of revoting creates a minor computational overhead, as each revote requires additional blockchain verification steps to check the validity of previous votes. Despite this, the system remains computationally feasible given that revoting is time-limited and strictly regulated by smart contracts [33].

A second major evaluation criterion is storage efficiency. Traditional blockchain voting systems store every submitted vote permanently, even if a voter later decides to change their decision [34]. This leads to increased blockchain storage requirements, particularly in large-scale elections where millions of votes are cast. The Dynamic Revoting Mechanism optimizes storage by nullifying previous votes via a cryptographic burn function, ensuring that only the latest valid vote per voter remains actively stored [35]. This reduces redundant data accumulation, improving the overall efficiency of blockchain storage usage. Based on theoretical projections, the storage footprint could be reduced by approximately 30-40%, depending on the percentage of voters utilizing the revoting option [36].

Finally, from a security perspective, the revoting system maintains tamper-proof integrity through strict timestamp validation and cryptographic proof mechanisms [37]. Unlike traditional e-voting models, where vote modification is not possible, the proposed system ensures that every revote remains recorded on-chain but does not impact election results beyond the latest submission [38]. The implementation of self-destructing ballots prevents fraudulent vote duplication, and the requirement for timestamped transactions ensures that only legally permitted revotes are accepted.

5. Discussion

The findings of this study highlight the effectiveness of integrating deep learning-based facial recognition, deepfake detection, and blockchain security mechanisms into electronic voting systems. Compared to traditional authentication methods such as passwords and ID-based verification, the proposed system significantly enhances voter authentication by leveraging Vision Transformer (ViT) and ResNet50 architectures. The high accuracy of ViT-LoRA (97.36%) demonstrates the potential of transformer-based models in facial recognition tasks, outperforming conventional convolutional neural networks. However, despite the advantages of facial biometrics, concerns about privacy and potential biases in recognition models remain. Future work should focus on developing privacy-preserving facial recognition techniques and evaluating fairness across diverse demographic groups to mitigate biases.

One of the primary contributions of this study is the introduction of a Dynamic Revoting Mechanism, which allows voters to modify their votes within a predefined election period. While this feature improves voter flexibility and accuracy, it also introduces additional computational overhead due to the need for revote validation and cryptographic proof verification. The secure timestamping mechanism ensures that only the latest vote submission is included in the final tally, preventing fraud and unauthorized modifications. However, the requirement for self-destructing ballots (SDBs) raises questions regarding long-term vote auditability. Although previous votes remain verifiable on-chain, the exclusion of earlier ballots from the final tally could raise transparency concerns among election regulators. Further research should explore ways to balance revoting flexibility with enhanced auditability mechanisms.

From a blockchain perspective, this study demonstrates that Ethereum-based voting frameworks can provide immutability, decentralization, and auditability while reducing dependency on centralized authorities. However, the scalability and transaction costs of Ethereum-based solutions remain significant challenges, particularly in large-scale national elections. Gas fees and network congestion may impact the feasibility of real-world deployments, emphasizing the need for layer-2 scaling solutions or alternative blockchain infrastructures, such as Hyperledger Fabric or Algorand, to optimize cost and efficiency.

Additionally, the proposed system's deepfake detection module, based on ResNet50 and Fourier frequency analysis, significantly mitigates the risk of identity spoofing via synthetic facial images. While the experimental results show robust performance, adversarial attacks and evolving deepfake generation techniques could challenge the long-term reliability of detection models. Future research should focus on adversarial training strategies and real-time deepfake detection techniques to ensure continued robustness against emerging threats.

Finally, integrating blockchain and artificial intelligence for secure electronic voting presents ethical, legal, and regulatory challenges. Ensuring compliance with election laws, data protection regulations (such as GDPR), and accessibility requirements is critical for large-scale adoption. Collaboration with policymakers, election officials, and cybersecurity experts is necessary to address these challenges while promoting the adoption of secure, tamper-proof digital voting frameworks.

In conclusion, this study presents a promising framework for secure electronic voting that enhances voter authentication, prevents fraud, and improves transparency. Future research directions include optimizing deepfake detection methods, exploring cost-efficient blockchain alternatives, ensuring regulatory compliance, and developing privacy-preserving biometric authentication techniques to further refine and scale the proposed system.

6. Conclusions

This study presents a secure and transparent electronic voting system that integrates facial recognition, deepfake detection, and blockchain technology to address key challenges in voter authentication, election security, and data integrity. By leveraging Vision Transformer (ViT) and ResNet50, the system achieves highly accurate facial authentication, ensuring that only legitimate voters participate in the election process. To counter the threat of deepfake identity fraud, deepfake detection models utilizing ResNet50 and frequency-domain analysis effectively identify manipulated images, reducing the

risk of unauthorized voter impersonation. These mechanisms collectively enhance voter authentication beyond traditional methods such as passwords and ID verification.

Blockchain technology further strengthens vote security and transparency by ensuring immutability and decentralized auditability. Through the Ethereum-based voting framework, votes are securely stored on-chain, preventing tampering and unauthorized modifications. However, conventional blockchain voting models suffer from vote immutability, preventing voters from modifying or correcting their votes within the election period. To address this limitation, this study introduces the Dynamic Revoting Mechanism, which combines Self-Destructing Ballots (SDB) and Secure Timestamping to enable controlled vote modifications while preventing double voting and fraudulent revote attempts. By ensuring that only the most recent vote submission is counted, while previous votes remain verifiable but excluded from final tallying, this system provides flexibility without compromising security.

The evaluation of the proposed system demonstrates significant improvements in terms of authentication accuracy, deepfake detection efficiency, and blockchain voting security. The deep learning-based facial recognition and deepfake detection models outperform traditional approaches in preventing identity fraud, while the blockchain-backed revoting mechanism ensures vote integrity and verifiability. The Self-Destructing Ballot mechanism optimizes storage efficiency by removing redundant votes, reducing blockchain congestion, and enabling a more scalable e-voting solution.

The introduction of blockchain voting with facial recognition and deepfake protection within the framework of the Smart City concept represents an important step in the development of digital democracy. For ordinary citizens, this provides convenience and security, similar to what has already been implemented in government services. Using Face ID allows for a faster identification process and increased data security, making electronic voting more accessible, reliable, and transparent.

Thus, the integration of the system into the infrastructure of a smart city allows not only for increased user convenience but also for the creation of a stable platform for future electoral processes. This minimizes the risks of fraud and ensures citizens' trust in digital electoral technologies, further enhancing the security and accessibility of modern voting frameworks.

Previously, in the study Aidynov, et al. [39] we conducted a systematic review of modern cryptographic methods used to protect electronic voting systems. This research highlighted the importance of utilizing advanced cryptographic protocols to ensure the security and integrity of digital elections. The present study extends these findings by integrating cryptographic mechanisms with artificial intelligence and blockchain technologies, creating a more robust and transparent electronic voting system.

In conclusion, this study contributes to the advancement of secure electronic voting systems by integrating state-of-the-art AI models and blockchain security mechanisms. The combination of deep learning for voter authentication, deepfake detection for fraud prevention, and a blockchain-driven revoting system provides a highly resilient and tamper-proof electoral framework. Future research may explore further optimizations in deepfake detection techniques, scalability improvements in blockchain infrastructure, and the implementation of privacy-preserving cryptographic techniques to enhance voter anonymity while maintaining election integrity. This work serves as a technical reference for future secure and transparent digital election systems, offering a robust solution to the challenges faced by modern e-voting frameworks.

References

[1] A. D. Rubin, "Security considerations for remote electronic voting," *Communications of the ACM*, vol. 45, no. 12, pp. 39–44, 2002. https://doi.org/10.1145/585597.585599

[2] X. Monnat and S. Oswald, *The challenges of enabling public scrutiny. In Electronic Voting*. Cham: Springer, 2021.

[3] F. Maddaloni, "Voting verification mechanism for a distributed ledger based remote electronic voting system," Master's Thesis, Universität Zürich UZH, Zürich, Switzerland, 2021.

[4] R. Küsters and J. Müller, "Cryptographic security analysis of e-voting systems: Achievements, misconceptions, and limitations," in *International Joint Conference on Electronic Voting (pp. 21-41). Cham: Springer International Publishing*, 2017.

[5] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, "Analysis of an electronic voting system," in *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004 (pp. 27-40). IEEE*, 2004.

[6] R. Krimmer, S. Triessnig, and M. Volkamer, "The development of remote e-voting around the world: A review of roads and directions," in *International Conference on E-Voting and Identity (pp. 1-15). Berlin, Heidelberg: Springer Berlin Heidelberg*, 2007.

[7] K. Visvalingam and R. Chandrasekaran, "Secured electronic voting protocol using biometric authentication," *Advances in Internet of Things*, vol. 1, no. 2, pp. 38-50, 2011.

[8] P. Korshunov and S. Marcel, "Deepfake detection: Humans vs. machines," *arXiv preprint arXiv:2009.03155*, 2020. https://doi.org/10.48550/arXiv.2009.03155

[9] U. Gawande, Y. Golhar, and K. Hajari, *Biometric-based security system: Issues and challenges. In Intelligent Techniques in Signal Processing for Multimedia Security*. Cham, Switzerland: Springer, 2017.

[10] G. Yegemberdiyeva and B. Amirgaliyev, "Study of AI generated and real face perception," in *2021 IEEE International Conference on Smart Information Systems and Technologies (SIST) (pp. 1-6). IEEE*, 2021.

[11] Z. Yu, Y. Qin, X. Li, C. Zhao, Z. Lei, and G. Zhao, "Deep learning for face anti-spoofing: A survey," *IEEE transactions on pattern analysis and machine intelligence*, vol. 45, no. 5, pp. 5609-5631, 2022. https://doi.org/10.1109/TPAMI.2022.3215850

[12] A. Tewari *et al.*, "Advances in neural rendering," *Computer Graphics Forum*, vol. 41, no. 2, pp. 703-735, 2022. https://doi.org/10.1111/cgf.14507

[13] N. Khan, K. Salah, and M. H. Rehman, "Analysis of blockchain solutions for E-Voting," *IEEE Access*, vol. 10, pp. 97445–97462, 2022.

[14] M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-voting meets blockchain: A survey," *IEEE Access*, vol. 11, pp. 23293-23308, 2023. https://doi.org/10.1109/ACCESS.2023.3253682

[15] H. Lipmaa and A. Mitra, "Going from bad to worse: From internet voting to blockchain voting," *J. Cybersecurity*, vol. 7, p. 1, 2021.

[16] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2025. https://bitcoin.org/bitcoin.pdf. [Accessed Jan. 25, 2025]

[17] A. Khan, J. Arshad, and M. T. Khan, "Secure voting website using Ethereum and smart contracts," *Journal of Cybersecurity and Privacy*, vol. 2, no. 3, pp. 670–687, 2022.

[18] A. Dosovitskiy *et al.*, "An image is worth 16x16 words: Transformers for image recognition at scale," presented at the International Conference on Learning Representations (ICLR 2021), 2021.

[19] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2016.

[20] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in *Proceedings of the 25th USENIX Security Symposium*, 2016.

[21] A. Vaswani *et al.*, *Attention is all you need. In Advances in Neural Information Processing Systems*. Red Hook, NY: Curran Associates, Inc, 2017.

[22] I. O. Tolstikhin *et al.*, "MLP-Mixer: An all-MLP architecture for vision," in *Proceedings of the 9th International Conference on Learning Representations (ICLR 2021). Vienna, Austria*, 2021.

[23] E. J. Hu *et al.*, "LoRA: Low-rank adaptation of large language models," *arXiv preprint arXiv:2106.09685*, 2021. https://arxiv.org/abs/2106.09685

[24] S. Azizi, S. Kundu, and M. Pedram, "Lamda: Large model fine-tuning via spectrally decomposed low-dimensional adaptation," *arXiv preprint arXiv:2406.12832*, 2024.

[25] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "Arcface: Additive angular margin loss for deep face recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2019.

[26] A. Howard *et al.*, "Searching for MobileNetV3," in *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV 2019) (pp. 1314–1324). Seoul, South Korea: IEEE*, 2019.

[27] R. Durall, M. Keuper, and J. Keuper, "Watch your up-convolution: CNN-based generative deep neural networks are failing to reproduce spectral distributions," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recogni-tion (CVPR)*, 2020.

[28] A. S. Yadav, Y. Urade, A. Thombare, and A. A. Patil, "E-voting using blockchain technology," *International Journal of Engineering Research & Technology*, vol. 9, no. 7, pp. 375-378, 2020. https://doi.org/10.17577/IJERTV9IS070183

[29] E. Yavuz, A. K. Koç, U. C. Çabuk, and G. Dalkılıç, "Towards secure e-voting using ethereum blockchain," in *2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-7). IEEE*, 2018.

[30] J.-H. Hsiao, R. Tso, C.-M. Chen, and M.-E. Wu, "Decentralized E-voting systems based on the blockchain technology," in *International Conference on Ubiquitous Information Technologies and Applications, pp. 305-309. Singapore: Springer Singapore*, 2017.

[31] G. G. Dagher, P. B. Marella, M. Milojkovic, and J. Mohler, "BroncoVote: A secure voting system using Ethereum's blockchain," in *Proceedings of the IEEE International Conference on Internet of Things (iThings), IEEE Green Computing and Communications (GreenCom), IEEE Cyber, Physical and Social Computing (CPSCom), and IEEE Smart Data (SmartData) (pp. 1561–1565). Halifax, NS, Canada: IEEE*, 2018.

[32] W. Lueks, I. Querejeta-Azurmendi, and C. Troncoso, "VoteAgain: A scalable coercion-resistant voting system," in *USENIX Security Symposium (29th USENIX Security 2020). San Diego, CA, USA. Proceedings*, 2020.

[33] P. McCorry, S. F. Shahandashti, and F. Hao, "A smart contract for boardroom voting with maximum voter privacy," in *International Conference on Financial Cryptography and Data Security (pp. 357-375). Cham: Springer International Publishing*, 2017.

[34] A. Mukherjee, S. Majumdar, A. K. Kolya, and S. Nandi, "A privacy-preserving blockchain-based e-voting system," *arXiv preprint arXiv:2307.08412*, 2023. https://doi.org/10.48550/arXiv.2307.08412

[35] R. Taş and Ö. Ö. Tanrıöver, "A systematic review of challenges and opportunities of blockchain for E-voting," *Symmetry*, vol. 12, no. 8, p. 1328, 2020. https://doi.org/10.3390/sym12081328

[36] A. Russo, A. Fernández Anta, M. I. González Vasco, and S. P. Romano, "Chirotonia: A scalable and secure e-voting framework based on blockchains and linkable ring signatures," *arXiv*, 2021. https://arxiv.org/abs/2111.02257

[37] U. C. Çabuk, E. Adiguzel, and E. Karaarslan, "A survey on feasibility and suitability of blockchain techniques for the e-voting systems," *arXiv preprint arXiv:2002.07175*, 2020. https://doi.org/10.48550/arXiv.2002.07175

[38] A. Spanos and I. Kantzavelou, "A blockchain-based electronic voting system: EtherVote," *arXiv preprint arXiv:2307.10726*, 2023. https://doi.org/10.48550/arXiv.2307.10726

[39] T. Aidynov, N. Goranin, D. Satybaldina, and A. Nurusheva, "A systematic literature review of current trends in electronic voting system protection using modern cryptography," *Applied Sciences*, vol. 14, no. 7, p. 2742, 2024. https://doi.org/10.3390/app14072742