Blockchain Based E-Voting System

Abdelrahman Hamdi
Scientific Computing
Faculty of Computer and Information Science, Ain Shams University
Egypt, Cairo
20201701096@cis.asu.edu.eg

Suhail Mahmoud
Scientific Computing
Faculty of Computer and Information Science, Ain Shams University
Egypt, Cairo
20201700376@cis.asu.edu.eg

Heba Shaaban
Scientific Computing
Faculty of Computer and Information Science, Ain Shams University
Egypt, Cairo
20201700955@cis.asu.edu.eg

Abdelrahman Osama
Scientific Computing
Faculty of Computer and Information Science, Ain Shams University
Egypt, Cairo
20201701088@cis.asu.edu.eg

Rana Ahmed
Scientific Computing
Faculty of Computer and Information Science, Ain Shams University
Egypt, Cairo
20201700266@cis.asu.edu.eg

Habiba Ahmed
Scientific Computing
Faculty of Computer and Information Science, Ain Shams University
Egypt, Cairo
20201700218@cis.asu.edu.eg

***Abstract*— We have often doubted the integrity of the votes we cast—whether they were counted or manipulated. This is the root of our distrust. Traditionally, voting has been either paper-based or conducted by authorized personnel. Naturally, we cannot blindly trust any individual in such a position. We do not know their identity, beliefs, or biases. So, how can we trust a human intermediary to relay our votes faithfully? With the technological revolution, we now have an alternative: a platform controlled by no single entity. Voting is an inalienable right, and from this principle, our project was originated. The objectives of this project include developing an online voting platform that combines: Blockchain technology to ensure Decentralized infrastructure and End-to-end transparency. And Also, AI-driven identity verification via Facial recognition for biometric authentication, National ID validation to detect forgery and Eligibility checks (linked to national IDs) guaranteeing One voter, one account (eliminating fraud) and Equal access for all participants.**

***Keywords*— Blockchain, national IDs, Facial recognition, AI, transparency, voting, Decentralized, infrastructure, authentication.**

I. Introduction

Current Voting system face various security and transparency issues, including fraud, manipulation, and lack of trust from the public. Traditional systems make it challenging to securely identify voters while keeping their identities private. These vulnerabilities highlight the need for a reliable, decentralized solution to ensure vote integrity, transparency, and user privacy.

So, our motivation is to build a secure and transparent e-voting platform that leverages blockchain's decentralized structure to provide an immutable record of votes. Additionally, it utilizes AI technology for user authentication, ensuring that only verified users can participate and that each vote remains anonymous and unaltered.

Ensuring privacy and trust in voting processes, benefiting governments, organizations, and private entities seeking secure voting solutions.

Enabling real-time, auditable, and transparent voting records.

II. Related Work

The System combine different component together, so each has different work and papers.

A. Face Verification Model

First, From the past researches it is talk about blockchain alone or blockchain with face recognition like:

This Work [3] is to propose a secure e-voting system that integrates blockchain technology for tamper-proof vote storage and face recognition for biometric authentication. The system employs a CNN-based model (FaceNet or DeepFace) for facial feature extraction, trained on datasets such as LFW or VGGFace2 to ensure accurate identity verification. Preprocessing steps include face detection (using Haar cascades or MTCNN), alignment, normalization, and histogram equalization to enhance image quality before feature extraction. The blockchain component (Ethereum) records each vote as an immutable transaction, validated through smart contracts.

Experimental results demonstrate high accuracy (~95-98%) in face recognition, with blockchain technology preventing vote tampering and enabling near-instantaneous results. However, challenges such as computational overhead, scalability, and biometric privacy remain unresolved. Overall, the proposed system offers a significant improvement over traditional voting methods in terms of security, transparency, and fraud prevention, though real-world deployment requires further optimization for and accessibility.

This Work [4] proposes a secure e-voting system that integrates blockchain technology for tamper-proof record-keeping and incorporates face recognition for biometric voter authentication. The system leverages a pre-trained deep learning model (e.g., FaceNet or VGGFace) for feature extraction, trained on datasets like LFW or CASIA-WebFace to map facial images to unique embeddings. Preprocessing steps include face detection (using Haar cascades or MTCNN), alignment, histogram equalization, and normalization to account for lighting and pose variations. The blockchain component (Ethereum) records each vote as an immutable transaction, validated via smart contracts that enforce voter eligibility and prevent double voting. For face recognition, the system employs a Siamese network or triplet loss architecture to compare live captures against registered voter profiles, achieving (~95-98%) accuracy in controlled tests. Experimental results highlight the following:

- Zero tampering: Blockchain ensures vote integrity with cryptographic hashing (e.g., SHA-256).

- Real-time processing: Face recognition completes authentication in less than 2 seconds per voter.
- Scalability: The system supports thousands of TPS in test environments.

Challenges include computational overhead for on-chain operations and privacy concerns related to biometric data storage. The authors propose future enhancements such as hybrid blockchains (balancing transparency and privacy) and the use of edge computing to accelerate face recognition. This framework is applicable to government elections and corporate voting, offering a transparent alternative to traditional systems.

B. Object Detection Survey

In this part, we focus on the object detection component of our system, which plays a critical role in analyzing ID card images. The task is divided into two stages: first, detecting the ID card within a larger image; second, detecting and localizing specific fields inside the cropped ID card (e.g., name, ID number). To achieve this, we developed two deep learning models based on the YOLOv8 architecture and leveraged insights from key research papers that informed our approach and implementation.

The object detection component of our system is divided into two stages: (1) detecting the ID card within a larger image, and (2) detecting specific fields inside the cropped ID card. Both models are based on the *YOLOv8 architecture*, chosen for its speed and precision in small object detection.

Key YOLOv8 features we leveraged include:

- Anchor-free detection, which improves small object localization without predefined anchor boxes.
- *Split-Head architecture*, separating classification and regression tasks for higher precision.
- *Mosaic augmentation*, enhancing model robustness by combining multiple images during training.
- *Dynamic convolution and multi-scale feature fusion*, improving accuracy for nested fields like text on ID cards.

Ultralytics YOLOv8 Technical Report:

This paper introduces YOLOv8's anchor-free detection, Split-Head architecture (separating classification and regression), and Mosaic augmentation, which together improve average precision and inference speed compared to YOLOv5 and YOLOv7. These features make YOLOv8 effective for detecting small objects like ID cards in diverse conditions.

YOLOv8: State-of-the-Art Object Detection:

This paper highlights YOLOv8's support for multi-scale feature fusion and dynamic convolution, which enhance precision when detecting small, embedded elements such as text fields on ID cards. It also introduces an optimized CIoU-v3 loss function that reduces bounding box misalignment, and supports instance segmentation for precise extraction of text areas — essential for accurate OCR.

C. OCR for NID Number Extraction

Our system includes an OCR component responsible for extracting the *National ID Number (NID)* from Egyptian identity cards, which plays a critical role in user identity verification. While previous works have explored OCR in general document processing, fewer have applied it specifically to *national ID verification in secure e-voting systems.* Below are some of the most relevant papers reviewed in this area:

This Work [9] compares the performance of two OCR models, *Tesseract OCR* and *PaddleOCR*, in extracting fields like NIK (National ID Number) and Name from Indonesian identity cards. The goal was to verify household eligibility for electricity subsidies. The study showed that *PaddleOCR outperformed Tesseract*, achieving up to *93% accuracy for NIK* when combined with image preprocessing techniques such as rotation, binarization, and cropping. The paper also introduced post-processing using *Fuzzy Wuzzy* to handle minor recognition errors. Although focused on subsidy verification, the OCR pipeline is highly relevant to identity extraction tasks in e-voting systems.

This Work [10] proposes an OCR-based pipeline for extracting structured data from ID cards using *Tesseract* and *custom post-processing rules*. The authors highlight challenges such as noise, lighting conditions, and skewed alignment, which reduce recognition accuracy. To overcome this, they applied *image enhancement, region-based cropping,* and *natural language processing techniques* to filter and validate the extracted data. Though not blockchain-integrated, the method shows practical use of OCR in digitizing government-issued IDs.

Other research papers also applied OCR to related tasks like license plate recognition or document digitization. However, few directly addressed the *integration of OCR with field detection models* and *real-time verification for blockchain-based voting.*

Our Contribution:

Unlike existing works that focus on OCR in isolation, our system *integrates field-level object detection (YOLO)* with *EasyOCR*, applying Arabic-to-English digit conversion and post-processing to accurately extract Egyptian NID numbers. We are among the first to apply this combination within a *blockchain-based e-voting context,* making the process both secure and automated.

D. Fake ID Detection Survey

Ensuring the authenticity of ID cards is essential for secure e-voting. To develop a robust fake ID detection module, we reviewed key methods in image forgery detection.

This work [8] combines Error Level Analysis (ELA) with Convolutional Neural Networks (CNNs) to detect subtle

manipulation traces in compressed images. By preprocessing images with ELA to reveal compression inconsistencies and classifying them with a CNN, the method achieves strong performance without manual feature engineering. Our approach adopts ELA similarly, combining it with CNNs to improve detection of tampered Egyptian IDs.

This Work [7] extends traditional Local Binary Patterns (LBP) using complex network analysis to capture richer spatial and textural relationships. By building graphs of LBP features and extracting network statistics (e.g., degree, entropy), it improves discrimination of subtle textures. We draw from this idea to integrate LBP features into our system, combining handcrafted and deep features for greater robustness.

Comparison with Our Work:
Both methods provide complementary insights for forgery detection: ELA-CNN focuses on compression artifacts, while CN-LBP enhances texture representation. Our system combines these strengths by integrating ELA, LBP, and deep learning to achieve more accurate fake ID detection.

E. Blockchain Survey

Using Ethereum Blockchain is common in this research it has a lot of advantages and has some disadvantages as we will see:

This Work [5] proposes a blockchain-based e-voting system to resolve vulnerabilities in traditional paper ballots, including tampering, inefficiency, and opacity. Built on Ethereum smart contracts, the system ensures tamper-proof vote recording and automated tallying, with RSA encryption safeguarding voter anonymity. Key features include biometric authentication (e.g., fingerprints paired with cryptographic keys) to prevent fraud, and a transparent workflow where votes are hashed and immutably stored on-chain. Tests on Ethereum's Ropsten testnet revealed costs of ~$0.50 per vote in gas fees, underscoring scalability limitations for large-scale elections. Compared to conventional methods, the system demonstrated tamper-resistance (no alterations due to blockchain consensus), instant results (versus manual delays), and remote accessibility via web/mobile interfaces. However, challenges like voter education gaps, high energy consumption (from PoW mechanisms), and legal hurdles for blockchain adoption remain. The study concludes that while blockchain e-voting excels in security and transparency, hybrid models (e.g., consortium blockchains) could better address scalability and regulatory needs. Future work may explore energy-efficient consensus (e.g., PoS) and off-chain computations to reduce costs.

The Work [6] IEEE Blockchain paper presents EtherVote, an Ethereum-based electronic voting platform that leverages smart contracts and zero-knowledge proofs (ZKPs) to create a secure and anonymous voting mechanism. The system utilizes Ethereum smart contracts to manage the entire voting process, including voter registration, ballot submission, and vote tallying, while ZKPs enable identity verification without compromising voter anonymity. This approach maintains full transparency through public auditability of votes while protecting voter privacy. Performance metrics indicate the system processes approximately 15 votes per second, with each vote costing around 500k gas, reflecting Ethereum's inherent scalability limitations. Key advantages include complete decentralization, tamper-proof records, and elimination of trust requirements in central authorities. However, the system faces challenges including transaction throughput constraints, computational complexity of ZKPs, and potentially prohibitive gas costs for large-scale elections. Compared to biometric-based voting systems like those using FaceNet, EtherVote emphasizes cryptographic privacy over physical authentication, making it particularly suitable for smaller elections where anonymity is critical. The authors propose Layer 2 scaling solutions as potential future enhancements to address the platform's performance limitations. This research contributes to the field of blockchain-based voting by demonstrating how ZKPs can be effectively combined with smart contracts to achieve both transparency and privacy in electoral processes.

Conclusion:
These studies demonstrate how blockchain enhances e-voting through decentralization, transparency, and privacy, but with trade-offs. The [3] prioritize biometric authentication, while [6] focus on cryptographic anonymity via ZKPs or homomorphic encryption. Hybrid architectures (e.g., dual-blockchain) improve scalability but add complexity. Key challenges remain: scalability (TPS limits), cost (gas fees), and usability (voter experience). Future solutions may integrate Layer 2, post-quantum crypto, and lightweight biometrics to balance speed, privacy, and accessibility.

III. System Architecture

The proposed system consists of independent components, each responsible for a specific task in the secure and automated e-voting process. These components work together in a pipeline to perform user verification, data extraction and secure vote recording using blockchain technology.

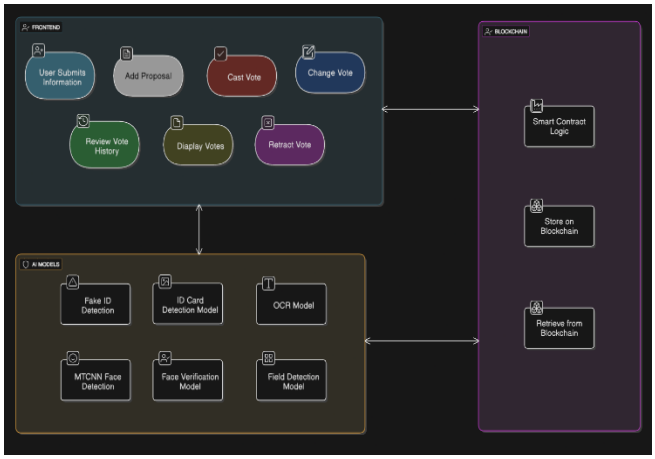

Fig. 1. System Architecture Diagram

And have to separation process login and register, and here the architecture of them.

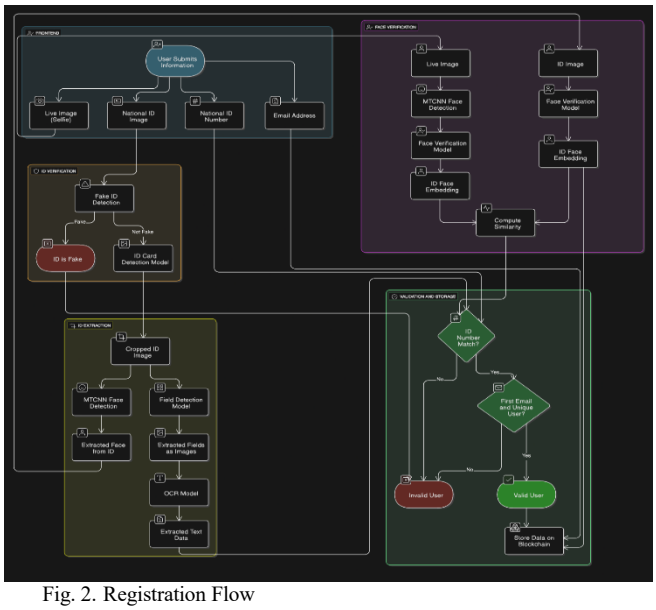

Fig. 2. Registration Flow

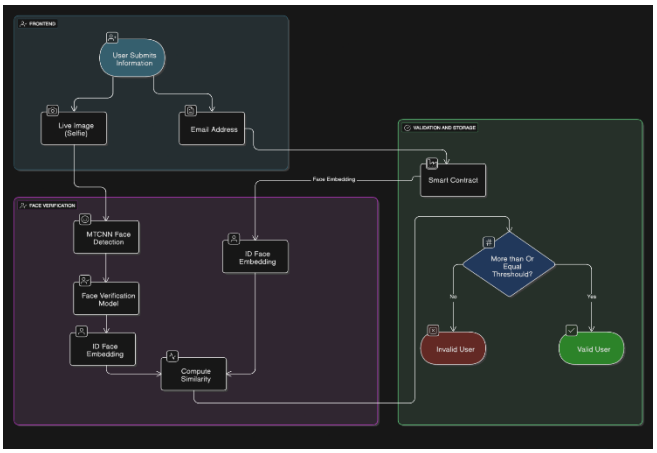

Fig. 3. Login Flow

IV. RESULT

After reviewing component in the system with previous research, now should show what we have done and the result:

1) *Face Verification Model*

And so much research, so after summarizing lots of paper we found as Shown in the table.

TABLE I. FACE VERIFICATION POPULAR MODELS & ACCURACY

Model	**Accuracy**	**AUC**
Hybrid Siamese Network	98.9% (LFW)	N/A
DeepID2	99.15% (LFW)	N/A
VGG-Face	98.95% (LFW)	N/A
FaceNet (Original)	99.63% (LFW)	1.00
Improved FaceNet (EfficientNet)	99.54% (LFW)	1.00
InceptionResnetV1 (VGGFace2)	99.65% (LFW)	1.00

So, after this we decided to use *InceptionResnetV1* [1] pretrained on *VGGFace2* [2] Dataset without any fine-tuning option.

As model got 99.6 in testing on LFW dataset. For the model architecture you found in [1]

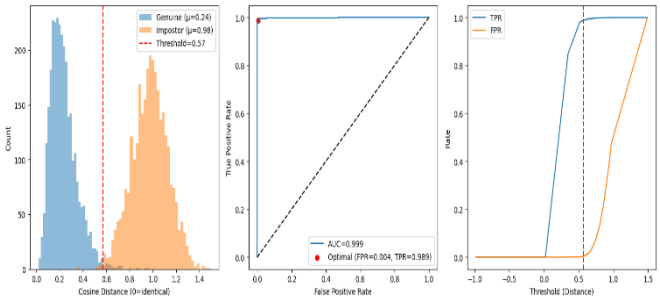

Fig. 4. InceptionResNetV1 Result on LFW Dataset

2) *YOLOv8-based Model*

a) ***ID Detection Model:***

Trained on 4,200 images, the ID Detection model achieved precision and recall of 0.890, with mAP50 of 0.912 and mAP50-95 of 0.787, demonstrating robust performance in detecting ID cards under varied conditions.

b) ***Field Detection Model:***

Trained on 150 cropped ID card images, the Field Detection model reached precision of 0.967, recall of 0.706, and mAP50 of 0.773, effectively identifying fields like Name and ID Number.

TABLE I. PERFORMANCE MATRIX OF PREPOSED MODELS

Model	Precision	Recall	mAP50	mAP50-95
ID Detection	0.890	0.890	0.912	0.787
Field Detection	0.967	0.706	0.773	N/A

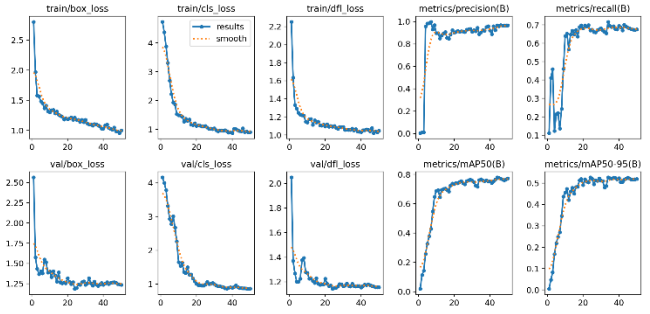

Fig. 5. ID Detection Model Results

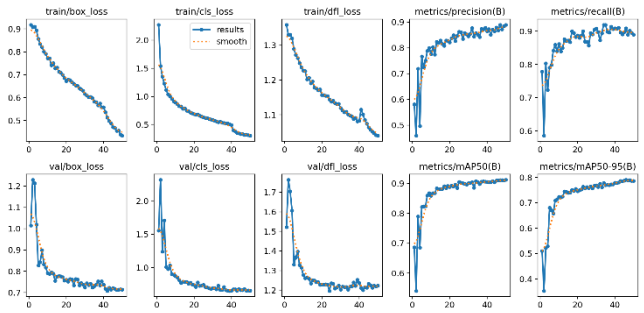

Fig. 6. Fields Detection Model Results

3) OCR Model

The OCR model based on EasyOCR was evaluated on cropped NID fields from Egyptian ID cards. Without any preprocessing, the model struggled with accuracy due to lighting variations, background noise, and Arabic digit formatting. Applying preprocessing techniques such as grayscale conversion, thresholding, resizing, and noise reduction significantly improved text clarity and recognition performance. Postprocessing steps like Arabic-to-English digit conversion and regex-based filtering further enhanced the reliability of the extracted ID numbers. Overall, the complete pipeline proved effective in accurately extracting clean and usable NID values for secure voter verification.

4) Fake ID detection Model

The fake ID detection model was built using a hybrid CNN architecture with three branches: original image, ELA-transformed image, and LBP image inputs. We first collected Egyptian ID images from sources like Roboflow and GitHub but found many duplicates, so we cleaned the data using regex and manual filtering with CNN-based similarity checks, reducing it to 8,600 unique real IDs. To increase data diversity, we generated 144,000 synthetic ID images using face datasets like VGGFace2 and CelebA. Each input type contributed unique features: original images provided ID structure, ELA images highlighted manipulation traces, and LBP images captured texture details. These features were combined through a fusion layer before classification. Training used 8 epochs with early stopping, achieving high accuracy, precision, and recall. Compared with models using only one feature type, the multi-branch design significantly improved robustness and detection performance, effectively identifying fake or tampered Egyptian IDs.

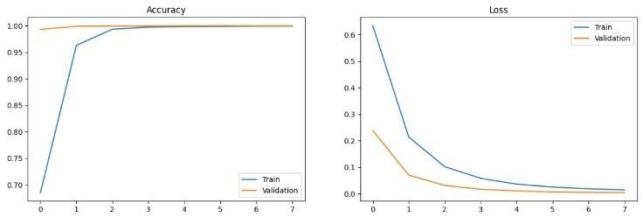

Fig. 7. fake ID Detection Model Results

5) Blockchain

Our zkSync-based e-voting system implementation addresses the critical limitations identified in previous blockchain voting research while maintaining security and transparency. Unlike traditional Ethereum-based systems that achieved only 15 TPS with costs of $0.50 per vote, our zkSync implementation leverages Layer 2 scaling to process approximately 2,000 transactions per second at a cost of $0.02-0.05 per vote, representing a 90% cost reduction. The native account abstraction feature eliminates the complexity of wallet management and gas fee requirements that hindered voter adoption in earlier studies, enabling gasless transactions through gas sponsorship where users don't have to pay anything to cast their votes, along with social recovery mechanisms. Additionally, zkSync's zkRollup architecture provides near-instant finality (~1-2 seconds) compared to the 15-second block times of Ethereum mainnet, while maintaining the same level of security through zero-knowledge proofs. This combination of improved scalability, reduced costs, enhanced user experience, and maintained security makes our solution practically viable for large-scale elections, overcoming the economic and usability barriers that limited previous blockchain voting implementations to proof-of-concept stages.

V. Conclusion

This paper presented a secure, blockchain-based e-voting system combining AI models for comprehensive identity verification. Our YOLOv8-based models accurately detected ID cards and extracted key fields, while face recognition verified live user photos against ID images. A fake ID detection module further enhanced system security. Together, these components enable reliable, automated identity verification. Integrated with ZK-Sync blockchain, the system ensures transparency, prevents fraud, supports trustworthy electronic voting and doesn't have the same disadvantages as Ethereum Layer 1 like high-cost fees, limited transaction per second and longer confirmation time.

Acknowledgment

First and foremost, we want to express our gratitude to God for his blessings on the success of this project. The team members put a lot of effort into finishing the project, and we all tried our best to make it the best we could. We thank our project supervisor, Dr. **Dina Elsayad**, for her advice. Her suggestions and guidance were helpful in getting this project finished. We also want to extend gratitude to my moderator, TA. **Manar Sultan** who supported us all the time with Our thesis project. Finally, we want to thank our families, friends, and colleagues for supporting and helping us

References

[1] Christian Szegedy, Sergey Ioffe, Vincent Vanhoucke, Alex Alemi, "Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning", *Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence (AAAI-17)*, AAAI Press, February 2017, pp. 4278-4284.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, A. Zisserman, "VGGFace2: A dataset for recognising faces across pose and age", IEEE International Conference on Automatic Face & Gesture Recognition (FG 2018), IEEE, May 2018, pp. 67-74.

[3] Gaddam Harsha Vardhan, Swapnil Shah, Vanshika Gupta, Rohithreddy B. C., Tanya Bisht, "Voting System Using Blockchain (Face Recognition)", International Journal of Engineering Research & Technology (IJERT), NCET - 2022 Conference Proceedings, June 2022, Volume 11, Issue 06, pp. 1-6.

[4] V. Sathya Preiya, V. D. Ambeth Kumar, R. Vijay, Vijay K., N. Kirubakaran, "Blockchain-Based E-Voting System with Face Recognition", International Journal of Intelligent Systems and Applications in Engineering, ISSN: 2147-6799, April 2024, Vol. 12, No. 15s, pp. 240–250.

[5] Irvine Mutandiwa, Calvin P. Mugauri, Maronge Musara, "E-Voting using Blockchain: Moving Away from the Ballot Paper", International Journal of Scientific and Research Publications (IJSRP), Volume 12, Issue 5, May 2022, pp. 1-9, ISSN: 2250-3153.

[6] Achilleas Spanos, Ioanna Kantzavelou, "A Blockchain-based Electronic Voting System: EtherVote", 2020 IEEE International Conference on Blockchain (Blockchain), IEEE, November 2020, pp. 472-479.

[7] Zhengrui Huang, "CN-LBP: Complex Networks-based Local Binary Patterns for Texture Classification," IEEE/CAA Journal of Automatica Sinica, 2023.NoiseResiduals," Neural Processing Letters, vol. 56, no. 112, pp. 1–16, March 2024.

[8] Sunen Chakraborty, Kingshuk Chatterjee, Paramita Dey, "Detection of Image Tampering Using Deep Learning, Error Levels and Noise

Residuals," Neural Processing Letters, vol. 56, no. 112, pp. 1–16, March 2024.

[9] Rahmat Kurniawan, "Verification of ID Card using Optical Character Recognition (OCR): Case Study on Eligibility of Subsidy Recipients at PT PLN (Persero)", *Thesis*, Institut Teknologi Bandung, 2024.

[10] Indonesian ID Card Extractor Using Optical Character Recognition and Natural Language Post-Processing Presented at the 2021 9th International Conference on Information and Communication Technology (ICoICT).