Deep Learning-Based Biometric Voter Verification System with Facial Recognition and Fingerprint Fallback Authentication

Karthika.S[#1], Karunyashri. S[*2], Suganthi. A[#3], Mahalakshmi. S[#4],Abinaya. M[#5]

[#1]*Assistant Professor,* [*2, #3,# 4, #5] *UG Student, Department of Electronics and Communication Engineering, V V College of Engineering, Tisaiyanvilai, Tuticorin district, Tamil Nadu, India*

[1]karthika@vvcoe,org, [2]shrikarunya2@gmail.com , [3]a.suganthi1110@gmail.com

Abstract—With the increasing demand for secure and transparent electoral processes, biometric-based voter authentication has gained significant importance. Traditional voter verification methods relying on manual identity checks are vulnerable to impersonation, duplicate voting, and lack of reliable identity verification. This paper proposes a Secured Biometric Voter Verification System that integrates deep learning–based facial recognition with fingerprint authentication as a secondary verification mechanism. The facial recognition module performs face detection and alignment using pre-trained models, followed by deep convolutional neural network-based feature extraction to generate discriminative 128-dimensional facial embeddings for identity matching. In cases of facial mismatch or poor image quality, fingerprint verification is triggered to maintain authentication reliability and system continuity. The proposed multimodal framework enhances robustness by combining two biometric traits at the decision level, thereby strengthening authentication security compared to unimodal systems. Biometric templates are securely stored in a protected PostgreSQL database to preserve voter privacy and data integrity. The system is implemented as a scalable web-based prototype suitable for real-time deployment in electronic voting environments. Functional validation under controlled conditions demonstrates reliable authentication performance and effective prevention of duplicate voting, highlighting the practical feasibility of multimodal biometric verification in modern digital election infrastructures.

Keywords—biometric authentication, electronic voting, facial recognition, fingerprint verification, multimodal biometrics, deep learning, decision-level fusion

I. INTRODUCTION

With the rapid advancement of information technology and increasing concerns over electoral transparency, the demand for secure and reliable electronic voting systems has grown significantly. Traditional voting systems that rely on manual identity verification and paper-based processes are vulnerable to impersonation, duplicate voting, administrative errors, and operational delays. To address these limitations, researchers have explored the integration of biometric authentication mechanisms into voting infrastructures to enhance security and ensure voter authenticity [1]–[6]. Biometric systems provide a reliable alternative by leveraging unique physiological characteristics such as facial features, fingerprints, palmprints, and iris patterns for identity verification.

Unimodal biometric systems, which rely on a single biometric trait, have demonstrated effective authentication performance under controlled conditions [1], [7], [9]. In particular, advances in deep learning have significantly improved face recognition accuracy through convolutional neural networks (CNNs) and discriminative loss functions [7], [11], [13]. Large-scale datasets such as VGGFace2 have contributed to improving robustness across variations in pose, age, and illumination [10]. Despite these advancements, unimodal systems remain sensitive to noise, spoofing attempts, sensor limitations, and environmental variations [8], [24]. Furthermore, concerns related to biometric template security, data protection, and privacy preservation continue to pose challenges in real-world deployments [14], [22], [23].

In the domain of electronic voting, several biometric-enabled electronic voting machine (EVM) systems have been proposed to mitigate impersonation and fraudulent voting [2], [3]. Many of these systems rely primarily on fingerprint authentication or a single biometric modality for voter verification. While such approaches enhance identity validation compared to manual verification methods, dependence on a single trait increases susceptibility to spoofing attacks and false rejections in practical scenarios. Recent research has also examined the integration of cryptographic techniques with biometric verification to strengthen the security of online voting platforms [4]. Additionally, secure vote transmission and storage mechanisms, including secret image sharing schemes, have been explored to enhance election confidentiality [5]. Comprehensive surveys on electronic voting systems continue to highlight persistent challenges such as authentication reliability, privacy preservation, scalability, and resistance to cyber-attacks [6].

To overcome the limitations associated with unimodal authentication, *multibiometric* systems combine two or more biometric traits to enhance robustness and reliability. Foundational studies indicate that multimodal fusion at the feature, score, or decision level can significantly improve authentication consistency under varying conditions [16]–[18]. For example, likelihood ratio-based score fusion techniques have demonstrated measurable improvements in verification stability [16]. Extensive multibiometric research further confirms that combining complementary modalities improves system resilience against spoofing and environmental variability [19]. However, increased system

complexity, computational overhead, and implementation cost remain practical considerations in real-world deployments.

Fingerprint recognition has long been regarded as a mature and reliable biometric modality, supported by standardized evaluation methodologies and well-established performance benchmarks [15], [20]. Similarly, face recognition technology has evolved from traditional handcrafted feature-based approaches to deep learning–driven embedding-based models with enhanced discriminative capability [21], [25]. Nevertheless, each modality possesses inherent limitations when used independently, reinforcing the importance of complementary authentication mechanisms.

Motivated by these observations, this paper proposes a Secured Biometric Voter Verification System that integrates *deep learning–based facial recognition* as the primary authentication mechanism with fingerprint verification as a secondary fallback modality. The system performs face detection, alignment, and embedding-based identity matching using a *128-dimensional feature representation*, while fingerprint authentication ensures continuity in cases of facial recognition failure or poor image quality. Biometric templates are securely stored using appropriate protection mechanisms to preserve data integrity and voter privacy. By combining multimodal biometric verification with structured database management, the proposed framework aims to provide a scalable, reliable, and practically deployable solution for modern electronic voting infrastructures.

II. Related Work

Recent advancements in biometric identification systems show a clear transition from unimodal to multimodal authentication frameworks. In [1], a multimodal system integrating face, palmprint, and iris features using deep learning–based feature extraction demonstrated improved identification performance compared to unimodal approaches, although the system involved higher computational complexity and was evaluated mainly on controlled datasets.

Biometric authentication has also been widely explored in electronic voting systems. The biometric-based electronic voting machine in [2] utilized fingerprint verification to reduce impersonation and duplicate voting, while [3] integrated biometric authentication into voting infrastructures to enhance voter validation. Further improvements were proposed in [4] and [5], where biometric verification was combined with cryptographic mechanisms and multi-secret image sharing techniques to improve vote security and confidentiality. A comprehensive survey in [6] highlighted persistent challenges in electronic voting systems, including authentication vulnerabilities, scalability limitations, and security threats.

Deep learning has significantly improved face recognition systems. Convolutional neural network (CNN)–based approaches have achieved higher recognition accuracy than traditional feature-based methods [7]. However, face recognition systems remain vulnerable to spoofing attacks and environmental variations [8], while studies such as [9] emphasize the importance of robust feature learning for reliable performance.

Large-scale datasets and advanced architectures have further enhanced recognition accuracy. The *VGGFace2* dataset [10] improved model generalization under variations in pose and illumination, while the *FaceNet* architecture [11] introduced embedding-based face recognition using triplet loss. Subsequent approaches such as *ArcFace* [13] further improved feature separability, and studies such as [12] emphasized the importance of data augmentation for improving robustness.

To overcome limitations of unimodal systems, multibiometric approaches combine multiple biometric traits to improve authentication reliability. Research in [17] and [18] demonstrated that multimodal fusion significantly reduces false acceptance and false rejection rates, while score-level fusion strategies such as likelihood ratio methods [16] further enhance verification performance. Comprehensive discussions on multibiometric architectures and fusion techniques are provided in [19].

Security and privacy remain critical considerations in biometric systems. Template protection and privacy risks associated with biometric data storage have been analyzed in [14], [22], and [23], while vulnerability analysis in [24] identified potential attack points such as sensor spoofing and template compromise. Fingerprint recognition remains a reliable biometric modality with established evaluation methodologies [15], [20], while embedding-based face recognition techniques continue to evolve [21], [25].

Despite significant progress, many electronic voting systems still rely on single biometric modalities and lack integration into scalable real-world infrastructures. To address these limitations, the proposed system integrates deep learning–based facial recognition with fingerprint verification as a fallback mechanism within a secure web-based architecture, enhancing authentication reliability and voter verification security.

III. Proposed System Methodology

The proposed Secured Biometric Voter Verification System is designed to provide a scalable and secure authentication framework for electronic voting environments. The system integrates facial recognition as the primary authentication modality and fingerprint verification as a secondary fallback mechanism. A web-based architecture is adopted to support real-time authentication and centralized database management. The overall framework consists of five primary components: voter enrollment, face detection and alignment, facial feature extraction and matching, fingerprint verification, and secure database management.

A. Voter Enrollment Module

The enrollment phase establishes the biometric identity of each voter and forms the foundation of the authentication process. During registration, the voter's facial image and fingerprint data are captured using appropriate acquisition devices. The captured facial image undergoes preprocessing operations such as resizing, normalization, and illumination adjustment. Facial landmark detection is then applied to ensure geometric alignment before feature extraction. A deep convolutional neural network (CNN)–based model converts the processed image into a fixed-length facial embedding vector.

Fingerprint data is processed to extract distinctive minutiae features, including ridge endings and bifurcations. The resulting facial embeddings and fingerprint templates are

ISSN: 3107-6513

securely stored in a PostgreSQL database. Each voter is assigned a unique identification number to associate biometric records with electoral information while minimizing exposure of raw personal data.

B. Face Detection and Alignment

During authentication, facial recognition operates as the primary verification mechanism. A pre-trained deep learning–based detector identifies the facial region within the captured image. Modern detection frameworks provide improved robustness under variations in illumination and pose.

The facial recognition pipeline is implemented using pre-trained models from the *Dlib machine learning library*. A lightweight face detection model is used to localize facial regions efficiently in real time. Following detection, a *68-point facial landmark model* extracts key structural points corresponding to the eyes, nose, mouth, and jawline. These landmarks enable geometric alignment of the face, reducing variations caused by head pose, scaling, and rotation.

Aligned facial images are *normalized* to ensure consistent input dimensions for the embedding network. Such preprocessing enhances robustness against environmental variations commonly encountered in operational voting environments.

C. Facial Feature Extraction and Matching

Following alignment, the normalized facial image is processed by a deep CNN-based embedding model to generate a fixed-length feature vector representing the voter's facial characteristics. Embedding-based face recognition approaches provide compact and discriminative representations suitable for scalable verification.

In the proposed implementation, Dlib's pre-trained face recognition model is employed to generate a 128-dimensional embedding vector. Authentication is performed by computing the Euclidean distance between the live embedding and the stored template corresponding to the claimed voter identity. The similarity between two embedding vectors is calculated using the Euclidean distance metric defined in (1).

$$\mathrm{d}(\mathrm{A},\mathrm{B}) = \sqrt{\sum_{i=1}^{128}(a_i - b_i)^2} \quad (1)$$

where $\mathrm{A} = (a_1, a_2, \ldots, a_{128})$ represents the embedding vector of the captured facial image and $\mathrm{B} = (b_1, b_2, \ldots, b_{128})$ represents the stored template vector in the database. Authentication is granted if the computed distance satisfies a predefined similarity threshold.

The decision threshold is empirically selected during prototype testing to balance acceptance and rejection behavior under controlled conditions. This embedding-based strategy supports scalability and computational efficiency for real-time verification. The overall facial recognition pipeline illustrated in Fig.1 is used in the proposed system consists of sequential stages including face detection, facial landmark extraction for alignment, deep feature embedding generation, and storage of the resulting embedding vectors in the database for subsequent identity matching.

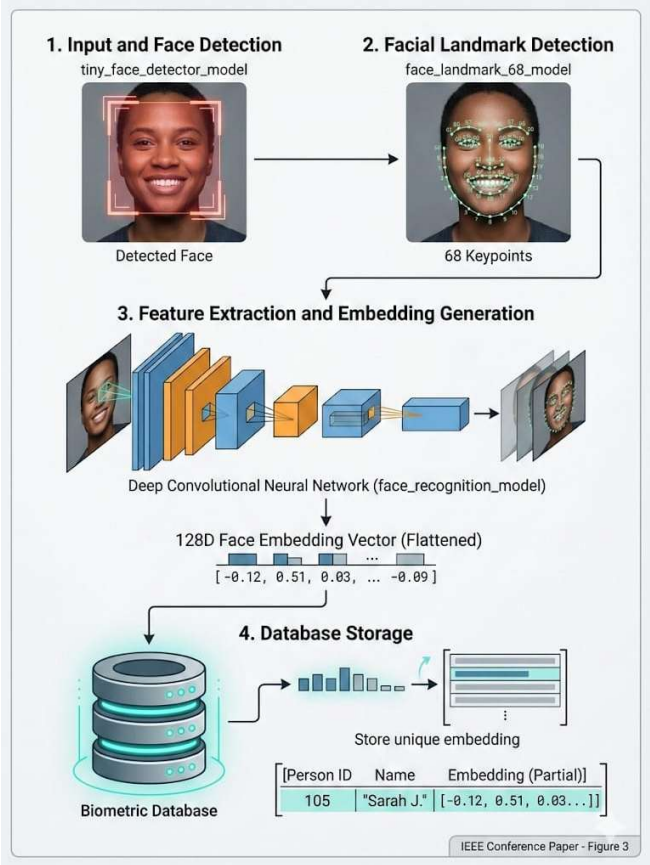

Fig. 1. Deep learning–based facial recognition pipeline.

D. Fingerprint Fallback Authentication

If facial authentication fails due to occlusion, illumination variations, or camera limitations, the fingerprint verification module is activated as a secondary authentication mechanism. The captured fingerprint image is enhanced to improve ridge clarity, and minutiae features are extracted for matching with stored templates using a pattern-matching algorithm. This fallback mechanism improves system reliability and ensures authentication continuity when facial recognition performance is affected by environmental conditions.

E. Decision-Level Fusion Strategy

The proposed framework adopts a hierarchical decision-level fusion strategy, where facial recognition acts as the primary authentication mechanism and fingerprint verification serves as a secondary confirmation method. Decision-level fusion is computationally efficient and suitable for real-time systems compared to feature-level or score-level fusion. In this workflow, successful facial verification grants immediate authentication, while fingerprint verification determines the final decision if facial recognition fails. This hierarchical structure improves operational efficiency and ensures continuous authentication in polling environments requiring rapid verification.

F. Secure Database and Privacy Protection

Biometric data protection is critical in electoral systems due to the sensitive and irreversible nature of biometric traits. In the proposed system, biometric templates are secured before storage in the *PostgreSQL database* to ensure confidentiality and integrity. Access control mechanisms restrict administrative privileges and prevent unauthorized

data manipulation. Raw biometric images are discarded after feature extraction to minimize exposure risks, and secure communication channels are used between the client interface and server to prevent interception or tampering. These measures collectively support secure biometric system design.

G. System Workflow

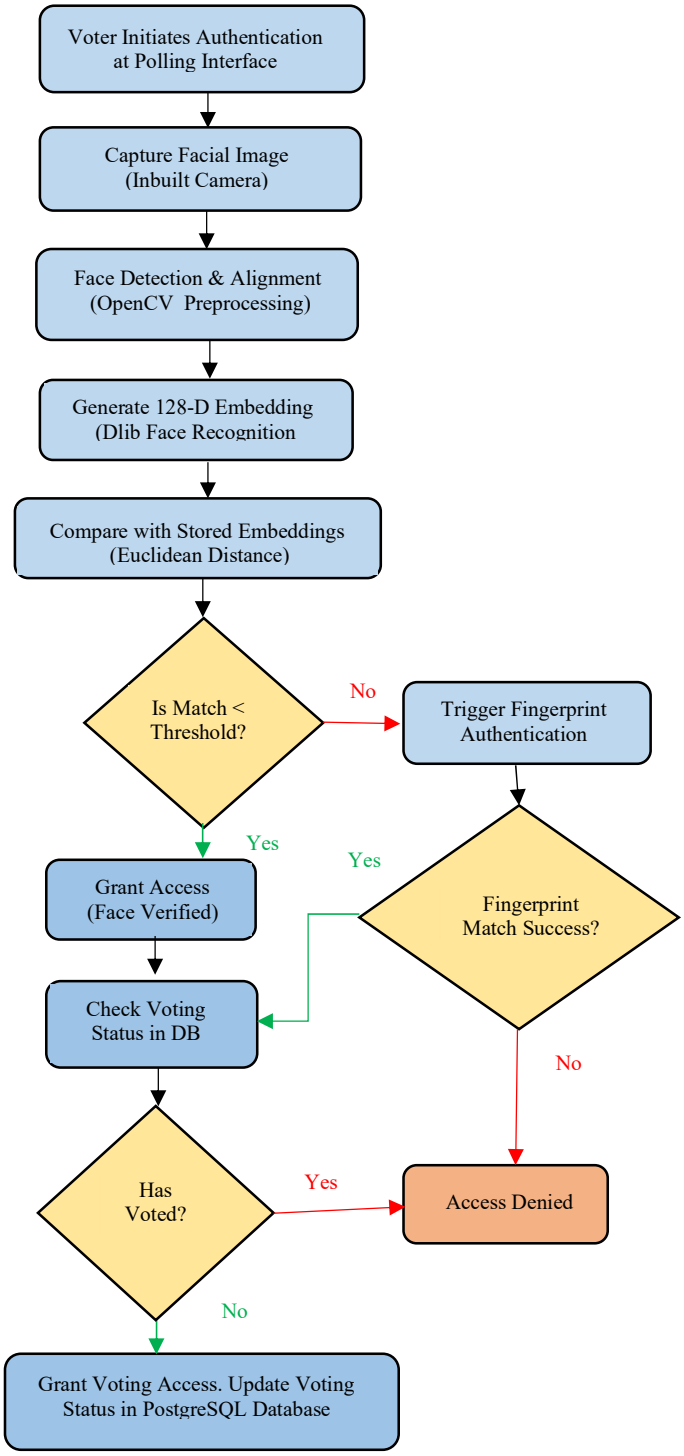

Fig. 2. Operational Workflow

The operational workflow of the proposed system begins when a voter initiates authentication through the web-based polling interface. The system captures a live facial image, performs face detection and alignment, and converts the processed image into a *128-dimensional embedding vector* using a pretrained *deep learning–based model*. This embedding is compared with stored templates in the database using Euclidean distance to determine identity similarity. If the similarity threshold is satisfied, authentication is granted and the voter is allowed to proceed.

If facial verification fails due to mismatch or poor image conditions, the system activates *fingerprint authentication* as a secondary verification mechanism. After successful authentication through either modality, the final decision is recorded, and the voter's status is updated in the database to prevent duplicate voting. By integrating facial recognition and fingerprint verification within a secure web-based architecture, the proposed approach enhances reliability and overcomes limitations associated with unimodal biometric systems while maintaining real-time functionality.

IV. Prototype Implementation and Functional Validation

The proposed Secured Biometric Voter Verification System was implemented as a web-based prototype to validate the feasibility of multimodal biometric authentication in electronic voting. The system uses real-time facial recognition as the primary method, supported by fingerprint verification as a fallback, along with secure database management and duplicate vote prevention.

The facial recognition module employs a pretrained deep learning–based embedding model to generate compact 128-dimensional feature vectors, eliminating the need for extensive training while ensuring reliable performance. During enrollment, facial images are captured via a webcam and preprocessed through detection, alignment, resizing, and normalization before embedding generation.

The generated embeddings are stored in a PostgreSQL database as numerical templates instead of raw images, enhancing privacy and security. Each voter record includes a unique ID, facial embedding, fingerprint reference, and a *Has_Voted* flag to prevent duplicate voting.

Table I presents the database schema and sample records used during prototype validation.

TABLE I. Voter Database Schema and Records

ID	Voter-_ID	Face_Embedding	Fingerprint	Has_ Voted
1	V01	[0.124, -0.982, 0.451, … , 0.773]	TEMP	FALSE
2	V02	[-0.334, 0.672, -0.118, … , -0.552]	TEMP	TRUE
3	V03	[0.887, -0.221, 0.004, … , -0.129]	TEMP	FALSE
4	V04	[-0.556, 0.341, -0.778, … , 0.990]	TEMP	TRUE
5	V05	[0.112, 0.445, -0.993, … , 0.214]	TEMP	FALSE

The Face_Embedding field stores a 128-dimensional numerical feature vector generated by the pretrained deep learning–based facial recognition model. This vector represents the unique facial characteristics of each voter in a compact form, enabling efficient similarity-based matching during authentication. For representation purposes, only partial values of the embedding vector are shown in Table I.

The *Fingerprint* field contains a reference value ("TEMP") corresponding to the stored fingerprint template used for fallback authentication. This indicates that the actual fingerprint data is securely maintained in the system without exposing raw biometric information, thereby ensuring privacy and security.

The *Has_Voted* attribute is implemented as a Boolean flag that indicates whether a voter has already cast a vote. A value of TRUE denotes that the vote has been recorded, while FALSE indicates that the voter is yet to vote. This field plays a critical role in enforcing the one-person-one-vote policy by preventing duplicate voting attempts.

During the authentication phase, the system follows a real-time verification workflow. When a voter initiates the process, a live facial image is captured through the webcam interface. The system performs face detection and alignment to normalize the facial region and reduce variations due to pose or orientation. The processed image is then passed through the pretrained model to generate a 128-dimensional embedding vector.

Authentication is performed by computing the Euclidean distance between the live embedding and the stored embedding corresponding to the voter ID. If the similarity score satisfies the predefined threshold, the voter is successfully authenticated and allowed to proceed.

After a successful vote, the ***Has_Voted*** field is updated to *TRUE* in the database. Any subsequent attempt by the same voter is automatically rejected based on this flag, thereby preventing duplicate voting. In cases where facial authentication fails, the system activates the fingerprint module as a fallback mechanism, ensuring robustness and continuity in the authentication process.

Functional testing of the prototype was conducted with multiple users under controlled indoor conditions with consistent lighting. The objective of this phase was to validate end-to-end system functionality rather than compute large-scale biometric performance metrics such as *False Acceptance Rate (FAR)* or *Equal Error Rate (EER)*. The prototype successfully demonstrated accurate facial detection and alignment, reliable embedding generation and storage, correct similarity-based authentication decisions, effective duplicate vote prevention, and proper activation of the fingerprint fallback mechanism when required.

The system response was observed to be suitable for real-time applications, with minimal perceptible delay between image capture and authentication decision. Although precise timing measurements were not formally recorded, practical testing confirmed that the authentication process is sufficiently fast for polling station deployment scenarios.

Large-scale quantitative evaluation involving extensive subject populations and systematic impostor testing was not conducted at this stage. However, functional testing verified that repeated voting attempts by the same registered user are correctly detected and denied. Therefore, detailed biometric performance indicators such as *False Acceptance Rate (FAR), False Rejection Rate (FRR), and Receiver Operating Characteristic (ROC)-based analysis* are reserved for future work. FAR represents the probability that the system incorrectly accepts an unauthorized individual, whereas FRR denotes the probability that the system incorrectly rejects a legitimate user. The ROC curve further evaluates classifier performance by illustrating the relationship between the True Positive Rate and False Positive Rate across different thresholds.

The current implementation primarily validates system feasibility, architectural correctness, and operational reliability. Future work will focus on large-scale dataset collection, statistical performance benchmarking, threshold optimization, and robustness evaluation under diverse environmental conditions. Overall, the prototype confirms that the proposed multimodal biometric voter verification framework is technically feasible and capable of enforcing secure voter authentication with duplicate vote prevention in electronic voting environments.

V. Experimental Validation and Results

The proposed system was evaluated under controlled conditions to verify authentication accuracy, system reliability, and duplicate vote prevention. Facial images were successfully converted into 128-dimensional embeddings and securely stored in the PostgreSQL database, demonstrating consistent and stable feature extraction across multiple captures.

During authentication, Euclidean distance-based matching effectively distinguished legitimate users from invalid attempts. As shown in Fig. 3, the system displays a green "Verified Successfully" interface for authenticated users and a red rejection interface for unauthorized or repeated attempts, confirming correct system response.

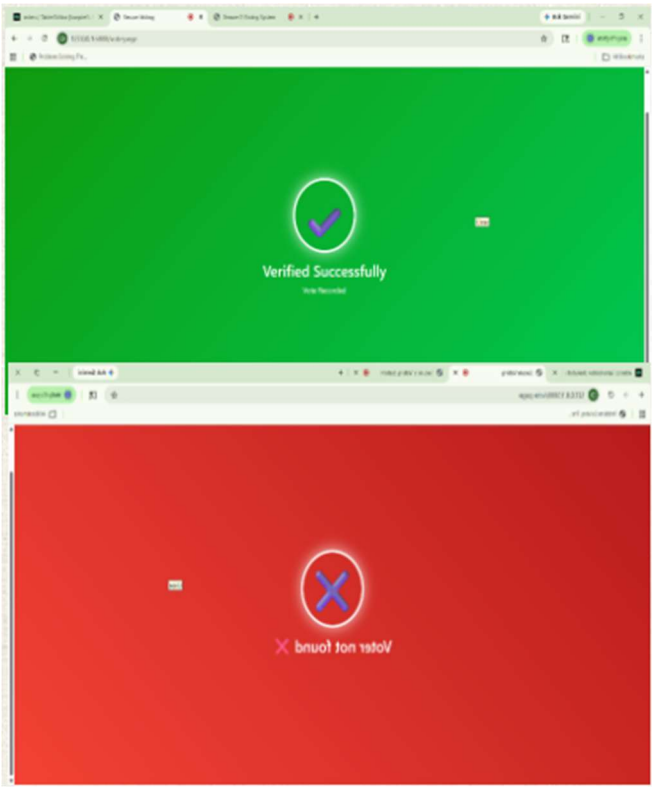

Fig. 3. System output showing successful authentication (green) and rejection case (red).

The duplicate voting prevention mechanism was validated using the *Has_Voted* flag, which is updated immediately after

a successful vote and prevents further voting attempts by the same individual. In cases where facial authentication did not meet the similarity threshold, the fingerprint fallback mechanism was activated, ensuring continuous and reliable authentication.

The system exhibited near real-time performance with minimal delay during verification, making it suitable for practical deployment in polling environments. Overall, the results confirm the feasibility, reliability, and effectiveness of the proposed biometric voter verification system.

VI. Conclusion and Future Work

This paper presented a Secured Multimodal Biometric Voter Verification System that integrates facial recognition as the primary authentication mechanism with fingerprint verification as a fallback modality. A pretrained embedding-based facial recognition model generates 128-dimensional feature vectors for efficient identity matching.

The developed web-based prototype demonstrated secure voter enrollment, real-time authentication, biometric template storage, and effective duplicate vote prevention through database management. Experimental validation confirmed the system's ability to enforce the one-person–one-vote policy while maintaining reliable authentication performance.

Large-scale biometric evaluation was beyond the scope of this work. Future research will focus on testing with larger datasets, computing performance metrics such as FAR, FRR, and EER, and integrating liveness detection and enhanced template protection mechanisms. Overall, the proposed framework demonstrates the feasibility of multimodal biometric authentication for secure electronic voting systems.

References

[1] O. N. Kadhim and M. H. Abdulameer, "Biometric Identification Advances: Unimodal to Multimodal Fusion of Face, Palm, and Iris Features," *Journal of Engineering and Applied Science*, vol. 72, no. 4, pp. 1–18, 2025.

[2] T. Keerthi et al., "Real Time Implementation of Biometric-based EVM System for Distinct Verification," *Procedia Computer Science*, vol. 230, pp. 407–416, 2023, doi: 10.1016/j.procs.2023.12.096.

[3] G. Chetty, T. P. P. Arunodayam and C. P. Maheswaran, "Biometric Authentication Voting System," in *Proc. 2024 9th Int. Conf. on Science Technology Engineering and Mathematics (ICONSTEM)*, Chennai, India, 2024, pp. 1–4, doi: 10.1109/ICONSTEM60960.2024.10568700.

[4] S. Gunasekaran et al., "Secure Online Voting with Enhanced Biometric Verification Using Cryptography Approach," in *Proc. 2024 4th Int. Conf. on Advancement in Electronics & Communication Engineering (AECE)*, Ghaziabad, India, 2024, pp. 616–620, doi: 10.1109/AECE62803.2024.10911295.

[5] S. P. Kodati et al., "An effective E-voting enhancement system through multi secret image sharing security system," *Knowledge-Based Systems*, vol. 315, Art. no. 113239, 2025, doi: 10.1016/j.knosys.2025.113239.

[6] M. Barelli, M. D'Onghia and S. Longari, "Toward Secure Electronic Voting: A Survey on E-Voting Systems and Attacks," *IEEE Access*, vol. 13, pp. 89600–89626, 2025, doi: 10.1109/ACCESS.2025.3569334.

[7] W. Liu, Y. Wen, Z. Yu, and M. Yang, "Deep face recognition: A survey," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 44, no. 1, pp. 1–35, Jan. 2022, doi: 10.1109/TPAMI.2021.3066160.

[8] Z. Zhang, S. Liu, and A. K. Jain, "Face anti-spoofing: A survey," *IEEE Access*, vol. 9, pp. 3770–3790, 2021, doi: 10.1109/ACCESS.2020.3047568.

[9] M. Wang and W. Deng, "Deep face recognition: A survey," *Neurocomputing*, vol. 429, pp. 215–244, 2021.

[10] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, "VGGFace2: A dataset for recognising faces across pose and age," in *Proc. IEEE Int. Conf. Automatic Face & Gesture Recognition*, 2018, pp. 67–74, doi: 10.1109/FG.2018.00017.

[11] F. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in *Proc. IEEE Conf. Computer Vision and Pattern Recognition (CVPR)*, 2015, pp. 815–823, doi: 10.1109/CVPR.2015.7298682.

[12] I. Masi, Y. Wu, T. Hassner, and P. Natarajan, "Deep face recognition: A survey," in *Proc. 31st SIBGRAPI Conf. Graphics, Patterns and Images*, 2018, pp. 471–478.

[13] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, "ArcFace: Additive angular margin loss for deep face recognition," in *Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 4690–4699, doi: 10.1109/CVPR.2019.00482.

[14] K. Nandakumar and A. K. Jain, "Biometric template protection: Bridging the performance gap between theory and practice," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 88–100, Sep. 2015, doi: 10.1109/MSP.2015.2427191.

[15] R. Cappelli, D. Maio, D. Maltoni, J. L. Wayman, and A. K. Jain, "Performance evaluation of fingerprint verification systems," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 1, pp. 3–18, Jan. 2006, doi: 10.1109/TPAMI.2005.128.

[16] K. Nandakumar, Y. Chen, S. C. Dass, and A. K. Jain, "Likelihood ratio-based biometric score fusion," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, no. 2, pp. 342–347, Feb. 2008, doi: 10.1109/TPAMI.2007.1176.

[17] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004, doi: 10.1109/TCSVT.2003.818642.

[18] A. K. Jain and A. Ross, "Multibiometric systems," *Commun. ACM*, vol. 47, no. 1, pp. 34–40, Jan. 2004, doi: 10.1145/966712.966725.

[19] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics*. New York, NY, USA: Springer, 2006.

[20] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. London, U.K.: Springer, 2009.

[21] S. Z. Li and A. K. Jain, *Handbook of Face Recognition*, 2nd ed. London, U.K.: Springer, 2011.

[22] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security & Privacy*, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003, doi: 10.1109/MSECP.2003.1193209.

[23] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Syst. J.*, vol. 40, no. 3, pp. 614–634, 2001.

[24] S. Galbally, J. Fierrez, and J. Ortega-Garcia, "Vulnerabilities in biometric systems and countermeasures," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 24, no. 6, pp. 13–21, Jun. 2009.

[25] I. Masi, Y. Wu, T. Hassner, and P. Natarajan, "Evaluation of local descriptors for face verification," *IEEE Trans. Image Process.*, vol. 26, no. 4, pp. 1704–1716, Apr. 2017.