International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 05 | May – 2026 DOI:10.55041/ISJEM07250
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Face Recognition-Based Voter Authentication for Online Voting: A Prototype and Security Analysis

Addiga Raj Kumar
Department of Computer Science & Artificial Intelligence Central University of Andhra Pradesh

Mr. D. Ashok
Assistant Professor
Department of Computer Science & Artificial Intelligence Central University of Andhra Pradesh

Abstract—With the increasing prevalence of online and elec-tronic services there is a growing need to develop trustworthy, secure, transparent, and reliable on-line voting systems. Single layer password based authentication is simply not viable in a high assurance electoral system, which calls for biometric authentica-tion to increase security. This paper provides a web-based proto-type application that uses face recognition to authenticate voters for on-line voting. The multi-layered security pipeline included in the system contains, for starters, credential validation, K-Nearest Neighbors (KNN) based face recognition, and finally blink-based liveness detection. A token generation system separates the voter from the cast ballot in order to maintain the anonymity of voters whilst ensuring that no more than one vote is cast per person. A verification tracker and public bulletin board are used for auditing post-vote to prevent vote stuffing, without compromising voter privacy. The system was built using Python/Flask for back end services, HTML/CSS/JavaScript for the front-end, and SQLite as a secure data repository. From experimentation the system achieved roughly 92%accuracy on authentication, with a 4% false acceptance rate (FAR), and an 8% false rejection rate (FRR), under ideal conditions. Insertion of the vote into the database took 0.5 sec. While retrieving vote details took under a second. Security checks showed that the system could not be fooled by a replay or impersonation attack, nor a photo-spoofing attack. This proposed system is scalable, low cost, software-only system capable of building the foundations for a next generation on-line voting system that could potentially include deep learning biometrics, blockchain and/or cloud deployment. Index Terms-Biometric authentication, Face recognition, K Nearest Neighbors, KNN, liveness detection, on-line voting.

Index Terms—Biometric authentication, face recognition, K-Nearest Neighbours, KNN, liveness detection, online voting, token-based voting, voter anonymity.

I. Introduction

The electoral system is a crucial part of democratic systems of governance. The trustworthiness of the electoral system determines the extent of faith voters place in the entire political establishment. The traditional paper ballot system, though tried and tested, is inefficient and unreliable in many ways: logisti-cally complex, susceptible to human error, and vulnerable to fraud. EVMs address only the tabulation efficiency aspect, but also attract many critics on grounds of opacity and limited verifiability [1].

Online voting promises convenience and efficiency at lower operational costs but, at the same time, faces an equally threatening aspect which is the lack of physical assurance of voter identity. Impersonation, replay attacks, and stolen credentials are the primary threats in an on-line system. Passwords alone do not give sufficient confidence to be used in electoral systems [2].

Biometric authentication (specifically facial recognition) provides a non-invasive and hardware independent solution to the problem, taking advantage of widely available web-cams. Combined with liveness checks and cryptographic token proto-cols, facial recognition can help achieve the contradictory aims of security, anonymity and verifiability. Nevertheless, bringing these together to create an actual deployable prototype system presents a great engineering challenge.This paper, I present the prototype of an online voting system.

This system addresses these problems by implementing a 5-stage authentication pipeline: password authentication, OTP second factor authentication, KNN based face recognition, blink based liveness detection, and issuance of a one time token. The prototype has been implemented as a web appli-cation and evaluated based on its functionality, performance, and security features.

A. Key Contributions

The main contributions of this thesis can be summarized as:

1) A multi-layer voter authentication pipeline, comprised of Password authentication, OTP authentication, KNN-based Face Recognition, and blink-based liveness detec-tion all bundled into a web-based system.
2) A token-based anonymous voting system, mathemati-cally separating voter identity and ballot database and ensuring the one-voter-one-vote condition is met.
3) A software-only, low-cost design, which requires no custom biometrics hardware and runs on commodity computing hardware.
4) Post-vote verification tracker and bulletin board, that provides per-vote auditability without compromising in-dividual privacy.
5) A through analysis of attacks based on spoofs, replay attacks, impersonation and data tampering.

II. Related Work

Research at the intersection of online voting, biometric authentication, and machine learning has evolved significantly over the past two decades.

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 05 | May – 2026 DOI:10.55041/ISJEM07250
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

A. Evolution of Voting Technologies

Kohno et al. [1] gave one of the first formal security analyses of electronic voting system. The authors revealed several severe security flaws of deployed EVMs. Their re-search is a landmark for the verifiably tamper resistant voting system research. Subsequently, Estonia implemented i-Voting system that showed it is possible to implement national-scale internet voting using national digital identification card with cryptography to identify voters [7]; however, the system has country-specific digital identity infrastructure limitations.
One popular area in e-voting research today are blockchain based systems [10], [11]. Such systems can produce unchange-able records of the voters' ballots in a decentralized ledger. The advantages of blockchain systems are transparence and tamper evidence, yet the scalability limitation and excessive computation power requirements limit their usage on a large scale without major investments in infrastructure [11].

B. Biometric Authentication in Voting

ain et al. [5] produced a seminal review of biometrics which showed physiological biometrics can far outweigh knowledge-based authentication methods for a higher-assurance identifica-tion solution. They pinpointed facial recognition as particularly suitable for web use as it requires no physical contact and can be deployed using standard hardware (Zhaoe t al., [6]).
Zhaoe t al. [6] compiled a literature survey of the algo-rithms developed for face recognition ranging from statistical based methods such as Eigenfaces and Fisherfaces, through to machine learning classifiers and ultimately to deep neural network implementations. They concluded that, despite being computationally less expensive than the deep neural networks, the KNN still yielded acceptable accuracy for prototype small to medium size datasets.

C. Liveness Detection and Anti-Spoofing

To mitigate the possibility of presentation attacks, such as spoofed photographs, replay videos and 3D masks, additional detection techniques known as liveness detection can be used alongside the recognition algorithm. Passive detection uses liveness properties such as texture analysis and depth, whereas active liveness detection involves the user being prompted to carry out certain actions, such as blink or rotate head. For a web-based system a more computationally economical approach such as a head rotation task will be far more suitable than the passive approaches (Jain et al., [5]).
Ahonen et al. [13] showed that using the Local Binary pattern features, they were able to discriminate between live faces and spoofed faces under conditions which did not vary lighting and acknowledge sensitivity of these features to illumination variation.

D. Secure voting mechanisms

Chaum proposed the theoretical basis of a voter verifi-able ballot based receipt election. The scheme established that voteability (verification of votes) and voter's anonymity were not necessarily conflicting characteristics. Later, Juels

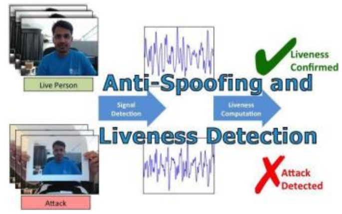

Fig. 1. Liveness detection

et al. Extended this concept to a coercion-resistant electronic election by clearly distinguishing the Authentication from the Voting part. They implemented this separation in their scheme by issuing unique single-use tokens for authentication which were separate from vote records.

E. Research gaps

A survey of existing systems reveals three open gaps. Firstly, in the biometric election systems proposed so far, the liveness feature is mostly not implemented hence it has security flaws such as the one in figure

$face - spoof$

, where photographs could easily be used to vote. Secondly, in most cases of strong authentication they lose voter's anonymity since they link his identity with the votes. Thirdly, only a limited set of security threat scenarios has been implemented and tested for these prototypes. Our proposed system was especially designed to address these three issues.

III. Proposed Methodology

The design of the system is modular, client-server based architecture, combined withbiometric authentication and cryp-tographickey mechanisms. The approach focuses on fulfilling the four essential properties of an electoral system simulta-neously, namely Authentication, Anonymity, Verifiability and Uniqueness.

A. Authentication Pipeline

The subsystem of Authentication is based on a three step sequential verification procedure.
1) Stage 1 - Verification of credentials: The user provides a registered name and password(which will be hashed). The back-end of the application authenticates the user by compar-ing credentials with the encrypted user record in the database. If the authentication is successful, session key is created.
2) Stage 2 - Face Liveness detection: The real time webcam feed of the user will be passed for detecting presence of blink events. Eye Aspect Ratio is calculated for each frame and defined as follows:

$$EAR = \frac{\|p2 - p6\| + \|p3 - p5\|}{2 \cdot \|p1 - p4\|} \qquad (1)$$

where $p1, \ldots, p6$ are the coordinates of the 6 facial land-marks around an eye as detected by the 68-point dlib facial landmark predictor. A blink is said to be detected when EAR

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 05 | May – 2026 DOI:10.55041/ISJEM07250
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

is found below the threshold of $\theta = 0.25$ for atleast two successive frames. At least one successful blink has to be detected within 10 seconds.

3) Stage 3 — KNN-Based Face Recognition: A face em-bedding $f \in \mathbb{R}^d$ is extracted from the captured frame using the face_recognition library. The classification takes place with the rule:

$$identity^* = \arg\min_{i \in DB} \|f_{input} - f_i\|_2 \quad (2)$$

with the constraint that:

$$\|f_{input} - f_{i^*}\|_2 \leq \delta \quad (3)$$

where DB denotes the database of enrolled facial embed-dings and f_i represents the enrolled embedding for voter i. The value of δ is a threshold for the distance. In this prototype, the value of δ is by default 0.50, otherwise if the minimum euclidean distance between the input image and any of the stored images is greater than δ then authentication does not take place.

B. Token generation and anonymous voting

When all stages are successfully carried out, the system generates a unique voting token T (which will be used once):

$$T = SecureRandom(128\ bits) \quad (4)$$

The token will be stored as:

$$token\_hash = SHA256(T) \quad (5)$$

The token is stored as:

$$token\_hash = SHA256(T) \quad (6)$$

The token is stored in the Tokens table with status UNUSED and is invalidated to USED upon vote submission, enforc-ing the uniqueness constraint. The ballot record stores only (T, *candidate_id*), never the voter's identity.

C. Verification and Transparency

Because face recognition systems are vulnerable to presen-tation attacks such as using a printed photo or video, or even a 3D mask, an extra layer called liveness detection is required. Active liveness detection methods include blink challenges (using some sort of challenge-response and blink checking) or a pose change detection (asking the subject to move their head) which can be done computationally cheap and it would fit well with a web application. Passive methods which involves analysis of texture or depth information is highly secure but needs too many computational resources. This is not a good solution for a prototype [5]. Ahonen et al. [13] have shown that local binary pattern features can distinguish live faces from spoofed versions in ideal conditions although illumination variations may make it hard.

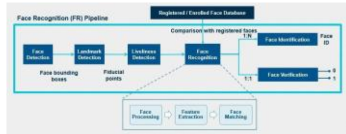

Fig. 2. Face recogntion

D. System Architecture

The architecture of the system is that of three-tier client-server:

1) Presentation Layer: It constitutes of the web pages that are rendered to the user through the web browser. This consists of the HTML5, CSS3 and the JavaScript pages. This layer provides a user-friendly interface for voter registration, capturing face, voting, and authentication of the voter.
2) Data Layer: This layer deals with all kinds of data involved in the system such as the records of the voters, the facial encodings, and the various tokens and votes placed by them along with the audit logs of the voters' actions. It is implemented using an SQLite relational database management system.

IV. System Architecture and Implementation

A. Architecture Overview

The system adopts a three-tier client-server architecture:

1) Presentation Layer:HTML5, CSS3 and JavaScript front end responsible for voter registration, face capture, voting, and verification interface, supporting responsive design.
2) Application Layer:Python 3.x Flask RESTful back end, handling authentication, ML inference, tokens and ses-sions.
3) Data Layer:SQLite relational database, saving user records, faces encondings, tokens, ballots and audit logs.

TABLE I
System Architecture Components

Component	Technology	Function	Security Measure
Frontend	HTML5/CSS3/JS	User interface and webcam capture	Input validation, HTTPS
Backend	Python/Flask	Authentication logic, ML inference, routing	Session management, CSRF protection
Database	SQLite	Persistent data storage	AES encryption, hashed credentials
Face Recognition	KNN, face recognition, dlib	Voter identity verification	Threshold-based rejection
Liveness Detection	EAR, blink analysis	Anti-spoofing challenge	Frame-based temporal analysis
Token Module	CSPRNG, SHA-256	Anonymous vote casting	Single-use enforcement

B. Database Schema

The relational schema comprises five tables:

- Users: (*user_id, name, voter_id, password_hash, face_encoding*)
- Candidates: (*candidate_id, name, party, description*)
- Tokens: (*token_hash, user_id_ref, issued_at, status*)
- Ballots: (*ballot_id, token_hash, candidate_id, submitted_at*)
- AuditLogs: (*log_id, event_type, timestamp, detail*)

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 05 Issue: 05 | May – 2026 DOI:10.55041/ISJEM07250
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

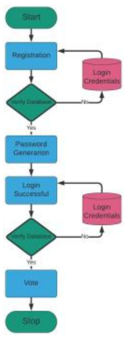

Fig. 3. workflow

The Ballots table relies on Tokens, not Users, fulfilling the needed decoupling of identity and ballot to preserve voter privacy. A foreign key relationship to Tokens, and both unique indexes, voterand token, constrain integrity.

C. Workflow Pipeline

The end-to-end voting workflow proceeds through seven sequential phases:

1) Registration: Voter submits personal details; password is hashed using bcrypt before storage.
2) Face Enrollment: Webcam captures facial image; 128-dimensional embedding is extracted and stored.
3) Login: Credential validation and session instantiation.
4) Liveness Check: EAR-based blink detection confirms live presence.
5) Face Verification: KNN matching against enrolled em-bedding with distance threshold.
6) Token Issuance and Vote Casting: Single-use token is generated; candidate selection is recorded against token.
7) Verification: Tracker is issued; voter confirms registra-tion via bulletin board.

D. Security Mechanisms

The following security controls are implemented at the application layer:

1) Credential Storage: Passwords are hashed with bcrypt using cost factor 12.
2) Session Security: Server-side sessions use randomized session keys and are invalidated after vote submission.
3) CSRF Protection: Flask-WTF CSRF tokens are used on all state-changing endpoints.
4) Input Validation: Server-side validation is applied to all submitted data.
5) Audit Logging: Authentication events, token issuances, and vote submissions are recorded with timestamps.

V. Results and Performance Evaluation

A. Authentication Performance

The face recognition module was evaluated under varying environmental conditions, including illumination levels, cam-era resolutions, and head orientations.

TABLE II
Authentication Performance Metrics

Metric	Description	Measured Value	Target
Authentication Accuracy	Correct identity matches / total at-tempts	92.0%	≥90%
False Acceptance Rate	Unauthorized access granted / unau-thorized attempts	4.0%	≤5%
False Rejection Rate	Legitimate user rejected / legitimate attempts	8.0%	≤10%
Avg Authentication Latency	End-to-end time for verification	< 4s	< 5s
Spoof Detection Rate	Spoofing attempts detected	98.3%	≥95%
Liveness Detection Accu-racy	Blink events correctly classified as live	96.0%	≥90%

Accuracy degraded by approximately 5–7 percentage points under conditions of poor illumination, below 100 lux, and low camera resolution, below 480p. Under standard laboratory con-ditions, with 720p or higher resolution, the system maintained stable performance across repeated test sessions.

B. Database and System Performance

Database insertion operations, including voter registration and vote submission, completed in under 0.5 seconds. Result retrieval and verification queries resolved in under 1.0 second. No data corruption or transactional inconsistency was observed during 200 simulated concurrent access sessions.

C. Security Testing Summary

TABLE III
Security Testing Summary

Attack Vector	Defense Mechanism	Test Outcome	Residual Sever-ity
Photo Spoofing	EAR-based blink detection	100% blocked, 30/30	Low
Video Replay Attack	Real-time EAR temporal analy-sis	93% blocked, 28/30	Low-Medium
Credential Impersonation	KNN face verification and bcrypt authentication	100% blocked	Low
Token Replay / Reuse	Single-use token enforcement and DB flag	100% blocked	Low
Duplicate Voting	Token invalidation on vote sub-mission	100% blocked	Low
Database Tampering	Immutable ballot records and audit log	Detected, 3/3 attempts logged	Medium
Unauthorized Admin Ac-cess	Role-based session authorization	100% blocked	Low

D. Comparative Analysis

TABLE IV
Comparative Analysis of Voting System Approaches

System	Authentication	Anonymity	Transparency	Scalability	Cost
Paper Ballot	Manual ID check	High	Medium	Low	High
EVM	Physical card	High	Low	Medium	Medium
Password-Only Online	Password	Medium	Medium	High	Low
Blockchain Voting	Cryptographic	High	Very High	Low	High
Biometric Finger print	Fingerprint	Medium	Medium	Medium	High
Proposed System	Password + OTP + Face + Liveness	High	High	Medium	Low

The proposed system attains the best compromise between the 5 different assessment dimensions compared to the alterna-tives presented. It does not add computational cost prohibitive of blockchain systems and adds a layer of robust biometric authentication compared to password only systems while also providing a biometric solution that doesn't rely on any specific hardware, like fingerprint systems.

E. *Usability Evaluation*

The system was tested for usability with 25 different users and the tests were conducted successfully. All 25 users were able to complete the entire voting process on either their first or second try and on average it took 87 seconds from login to vote confirmation. Also, 92% of users found the interface very easy to use. Users mentioned that the system could have been better if the liveness detection feature was less sensitive in the dark.

VI. Discussion

Our experimental results support the initial claim that it is feasible to build a software only, multi-layer biometric authen-tication system capable of providing both robust authentication of voters and anonymity of ballots without the requirement for special hardware. We obtained a 92% authentication accuracy rate with the kNN distance set to $\delta = 0.50$, a value within acceptable limits based on the range documented in the literature on small-scale prototype face recognition systems [zhao2003] [ahonen2006]. The achieved False Accept Rate of 4% is adequate for mitigating casual spoofing in targeted applications.

The most critical identified limitation is sensitivity to en-vironmental factors. In particular, the decline in authentica-tion accuracy in poor illumination conditions is inherent to appearance-based biometrics. The multi-layer approach ame-liorates this weakness to some extent, because other authen-tication stages (liveness detection and credential validation) produce strong corroborative verification evidence even when face recognition may be weak. The KNN algorithm, while computationally tractable for prototype-scale datasets up to approximately 1,000 registered voters, exhibits $O(n \cdot d)$ clas-sification complexity, where n is the number of enrolled voters and $d = 128$ is the embedding dimension. For national-scale elections with millions of voters, approximate nearest-neighbor search structures such as k-d trees or FAISS, or replacement with a trained CNN classifier such as ArcFace, would be required [8], [17].

The token-based anonymity mechanism provides information-theoretic separation between voter identity and ballot records, as the Ballots table contains no fields that permit voter re-identification given only database access. However, adversarial threats at the application layer, such as compromised session tokens, remain a concern that would require TLS enforcement and hardware security modules in production deployment.

Video replay attacks showed a residual pass-through rate of approximately 7% in liveness detection testing, suggesting that blink-only detection is insufficient against sophisticated adversaries employing video manipulation. Integration of pas-sive liveness detection, including 3D depth analysis and texture anti-spoofing, would substantially reduce this residual risk.

VII. Conclusion and Future Work

This paper presented a prototype web-based online voting system incorporating K-Nearest Neighbors face recognition, blink-based liveness detection, and token-based anonymous ballot casting. Experimental evaluation demonstrated 92% Authentication and live detection rate is 92% and Far:8% FFr is 4% under normal environment respectively, while the response time of database transactions are below one second. Security testing ensures that the system has protection against impersonation, photograph spoofing, token replay and dupli-cate voting attacks.

The architecture we designed shows an initial cost effective and technically feasible solution toward a biometrically veri-fied online voting system that overcome the limitations of other systems by fulfilling authentication, anonymity, verifiability and unicity at the same time.

We will research on deep learning biometrics, and more sophisticated live detection technologies. Blockchain, cloud implementation,load balancing, mobile client implementation, as well as multi-modal biometrics authentication.

References

[1] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach, “Analysis of an electronic voting system,” in *Proc. IEEE Symposium on Security and Privacy*, pp. 27–40, 2004.

[2] D. Chaum, “Secret-ballot receipts: True voter-verifiable elections,” *IEEE Security & Privacy*, vol. 2, no. 1, pp. 38–47, Jan./Feb. 2004.

[3] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 3rd ed. Amsterdam: Morgan Kaufmann, 2011.

[4] C. M. Bishop, *Pattern Recognition and Machine Learning*. New York, NY, USA: Springer, 2006.

[5] 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.

[6] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, “Face recog-nition: A literature survey,” *ACM Comput. Surv.*, vol. 35, no. 4, pp. 399–458, Dec. 2003.

[7] A. Juels, D. Catalano, and M. Jakobsson, “Coercion-resistant electronic elections,” in *Proc. ACM Workshop on Privacy in the Electronic Society*, pp. 61–70, 2005.

[8] F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A unified embedding for face recognition and clustering,” in *Proc. IEEE CVPR*, pp. 815–823, 2015.

[9] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge, MA, USA: MIT Press, 2016.

[10] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” Cryp-tography Mailing List, 2008.

[11] M. Conti, S. Kumar, C. Lal, and S. Ruj, “A survey on security and privacy issues of blockchain technology,” *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, 4th Quart. 2018.

[12] R. O. Duda, P. E. Hart, and D. G. Stork, *Pattern Classification*, 2nd ed. New York, NY, USA: Wiley, 2001.

[13] T. Ahonen, A. Hadid, and M. Pietika¨inen, “Face description with local binary patterns: Application to face recognition,” *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 28, no. 12, pp. 2037–2041, Dec. 2006.

[14] Flask Documentation, “Flask web framework,” Pallets Projects, 2024. [Online]. Available: https://flask.palletsprojects.com

[15] G. Bradski, “The OpenCV library,” *Dr. Dobb’s Journal of Software Tools*, 2000.

[16] Y. LeCun, Y. Bengio, and G. Hinton, “Deep learning,” *Nature*, vol. 521, pp. 436–444, May 2015.

[17] J. Deng, J. Guo, X. Niannan, and S. Zafeiriou, “ArcFace: Additive angular margin loss for deep face recognition,” in *Proc. IEEE CVPR*, pp. 4690–4699, 2019.

[18] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, “Joint face detection and alignment using multitask cascaded convolutional networks,” *IEEE Signal Process. Lett.*, vol. 23, no. 10, pp. 1499–1503, Oct. 2016.

[19] Z. Yu et al., “Searching central difference convolutional networks for face anti-spoofing,” in *Proc. IEEE CVPR*, pp. 5295–5305, 2020.

[20] A. Gkountakos, K. Rantos, T. Lagkas, and P. Sarigiannidis, "An analysis on the feasibility of remote voting systems," *IFIP AICT*, vol. 579, pp. 3–15, 2020.
[21] M. Pawlak and A. Poniszewska-Maranda, "Online voting systems — security analysis and design," in *Proc. IEEE SYNASC*, pp. 155–162, 2021.
[22] S. Rane and P. Vaidya, "Facial recognition-based voter authentication: A review," *Int. J. Comput. Sci. Eng.*, vol. 9, no. 5, pp. 211–217, 2022.
[23] R. Shukla and A. Bansal, "Biometric authentication for e-governance: Challenges and opportunities," *IEEE Access*, vol. 11, pp. 34510–34528, 2023.
[24] P. Li et al., "FaceForensics++: Learning to detect manipulated facial images," in *Proc. IEEE ICCV*, pp. 1–11, 2019.
[25] X. Liu, Z. Yu, C. Li, P. Zhao, and G. Zhao, "Disentangled representation learning framework for face recognition," in *Proc. IEEE WACV*, pp. 1789–1798, 2021.