Journal of Cognitive Human-Computer Interaction (JCHCI)

♦ ISSN: 2771-1463 Vol: 11, No. 01, 2026 ♦ PP. 06–13

Article DOI: https://doi.org/10.54216/JCHCI.110102

REVIEW ARTICLE

A Systematic Literature Review on the Integration of Computer Vision and IoT Technologies for Enhancing Voter Verification Accuracy in Electoral Systems

Angela Choi[1,*] **Eugene Q. Castro**[1]

[1] Department of Computer Science, Central Asian University, Tashkent, Uzbekistan

Emails: 220412@centralasian.uz · e.castro@centralasian.uz

Received: October 02, 2025 Revised: November 10, 2025 Accepted: December 21, 2025 ⋆ Corresponding author

ABSTRACT

The rapid evolution of digital technologies has transformed how societies manage sensitive information and authenticate identity in critical systems. Within the domain of cybersecurity and artificial intelligence (AI), the integration of computer vision and Internet of Things (IoT) technologies has emerged as a promising approach to improving real-time data verification and process automation. This systematic literature review examines how computer vision and IoT technologies can be jointly leveraged to enhance voter verification accuracy in electoral systems. Following the PRISMA 2020 guidelines, the review systematically searched four academic databases, identifying 351 initial studies. After rigorous screening based on predefined inclusion and exclusion criteria, 15 studies were selected for comprehensive analysis. The findings reveal three major themes: (1) emerging technical architectures combining biometric authentication with blockchain-based verification, (2) performance outcomes demonstrating high accuracy rates (97–100%) in controlled environments, and (3) persistent challenges in scalability, real-world deployment, and security against sophisticated AI-enabled attacks such as deepfakes. While the PRISMA process was conducted in full, the limited scope of the project, compressed timeline, and restricted access to paywalled articles likely influenced the depth and completeness of the synthesis. Nevertheless, the review provides structured insight into current implementation approaches, technical methods, and research gaps, with particular relevance to contexts like Uzbekistan where recent OSCE ODIHR election observation reports have documented systemic weaknesses in voter verification and turnout reporting.

Keywords: Computer vision ▪ Internet of Things ▪ Voter verification ▪ Electoral systems ▪ Biometric authentication ▪ Systematic literature review

1. INTRODUCTION

The integrity of elections is a cornerstone of democratic governance. Many countries continue to face challenges related to voter impersonation, multiple voting attempts, and limited transparency in verification processes [15]. Traditional manual and semi-digital verification methods are often prone to human error and inefficiencies, particularly in large-scale or resource-constrained contexts. Recent election observation missions have documented significant procedural violations: in Uzbekistan's October 2024 parliamentary elections, observers identified serious concerns in 12% of polling stations, with 21% failing to properly verify voters against electronic registers and 24% showing identical signatures on voter lists [15].

These documented failures highlight the urgent need for ro-

bust, technology-enabled voter verification systems. The integration of computer vision and IoT technologies presents a promising solution for enabling automated identity recognition, real-time monitoring, and data-driven verification mechanisms that enhance both security and accessibility. Computer vision techniques—in particular deep learning-based facial recognition and biometric authentication—have demonstrated high accuracy in identity verification tasks across various domains. When combined with IoT infrastructure for distributed sensor networks and real-time data processing, these AI-driven technologies offer substantial potential for transforming electoral integrity.

However, despite growing research into AI-driven recognition systems and IoT-based monitoring tools individually, there remains limited synthesis of how these technologies can be jointly deployed for voter verification. Existing reviews largely focus on blockchain-based voting systems or electronic voting machines, with limited attention to the combined role of computer vision, IoT, and AI-enabled security mechanisms in preventing multiple voting and impersonation.

This systematic literature review addresses this gap by investigating: (1) what approaches have been explored in integrating computer vision and IoT technologies to enhance voter verification and prevent multiple voting in electoral systems, (2) what technical methods, architectures, and algorithms are used to combine these technologies for real-time identity verification in election or similar security-critical contexts, and (3) what outcomes and performance indicators have been reported in studies using computer vision and IoT for voter verification or fraud detection.

1.1 Contextual Motivation

The review is particularly motivated by practical challenges observed in contemporary electoral contexts. The OSCE ODIHR observation mission to Uzbekistan's 2024 parliamentary elections documented that counting processes were assessed negatively in 43% of observed polling stations, with procedures not followed in over 50% of cases [15]. Multiple voting and proxy voting were directly observed, and ballot box stuffing indicators were noted in 2% of voting observations. These quantifiable deficiencies underscore the practical urgency for automated, tamper-resistant verification mechanisms.

Although this review is not focused exclusively on Uzbekistan, the documented patterns of verification failure, inadequate safeguards against multiple voting, and systematic procedural violations provide compelling evidence for the broader applicability and importance of computer vision- and IoT-based solutions. Future implementations of the technologies reviewed here could address precisely these documented weaknesses in real-world electoral contexts.

1.2 Limitations and Transparency

Given the scope and constrained timeline of this systematic literature review, several limitations must be acknowledged explicitly. First, while the PRISMA process was followed end-to-end, access to full-text papers was significantly hindered by publisher paywalls, which likely affected the depth of analysis for some studies. Second, the compressed timeline may have impacted the exhaustiveness of the search strategy and the thoroughness of quality assessment. Third, as an academic exercise conducted under substantial time pressure, the review may not have captured all relevant gray literature or the very latest preprints.

To maintain transparency, these constraints are reported alongside the methodological choices. The analysis also explicitly documents where evidence is thin or absent (for example, when studies do not report quantitative performance metrics or real-world deployment details).

2. METHODOLOGY

2.1 Research Design

This study adopts a Systematic Literature Review (SLR) design following the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) guidelines [16]. The SLR method was selected to systematically identify, evaluate, and synthesize research evidence related to the integration of computer vision and IoT technologies for voter verification in electoral systems, with particular attention to AI-enabled biometric and security methods.

2.2 Research Questions

The review is guided by three research questions derived using the PICOC (Population, Intervention, Comparison, Outcome, Context) framework:

RQ1: What approaches have been explored in integrating computer vision and IoT technologies for enhancing voter verification and preventing multiple voting in electoral systems?

RQ2: What are the key technical methods, architectures, and algorithms used to combine computer vision and IoT for real-time identity verification in election or similar security-critical contexts?

RQ3: What outcomes and performance indicators have been reported in studies using computer vision and IoT for voter verification or fraud detection?

2.3 PICOC Framework

The PICOC framework used to scope the review is summarized in Table 1.

Table 1. PICOC Framework for the Review

Element	Description
Population	Studies involving digital identity verification systems, voter authentication, or electoral process security within electoral and digital governance environments.
Intervention	Integration of computer vision, IoT, and related digital trust technologies (such as blockchain) for voter or identity verification and fraud detection.
Comparison	Traditional or non-integrated solutions (manual, biometric-only, standalone IoT, or non-blockchain systems).
Outcome	Improved voter verification accuracy, reduced duplicate or fraudulent voting, enhanced real-time monitoring, privacy protection, auditability, and system security.
Context	Electoral systems, electronic voting, digital identity management, or civic participation platforms.

2.4 Data Sources and Search Strategy

Academic databases including **IEEE Xplore**, **ScienceDirect**, **ERIC**, and **Google Scholar** were systematically searched between 14 and 20 November 2025. The search targeted English-language publications from 2017 to 2026. Search

strings combined core keywords such as "election," "computer vision," "IoT," and "verification."

Table 2 details the exact search strings, filters applied, and results yielded for each database. Additionally, 6 records were identified from other sources (e.g., OSCE ODIHR reports) to provide contextual grounding. In total, 351 records were identified before deduplication.

Table 2. Database Search Log (November 2025)

Database	Search String	Filters Applied	Hits
ScienceDirect	"election" AND "computer vision" AND "IoT"	Research Articles, 2017–2026	53
ERIC	"election" AND "computer vision"	Peer-reviewed only	10
Google Scholar	"election" AND "computer vision" AND "IoT" AND "verification"	Since 2025, Exclude citations	187
IEEE Xplore	"election" AND "computer vision"	2015–2026	95
		Total Records (Databases)	**345**

2.5 Inclusion and Exclusion Criteria

Studies were selected based on predefined criteria to ensure relevance and quality, as detailed in Table 3.

Table 3. Inclusion and Exclusion Criteria

Type	Criteria
Inclusion	Empirical study on voter verification/electoral systems
	Uses computer vision, IoT, biometrics, or blockchain
	Focus on fraud detection or identity verification
	Peer-reviewed papers or credible preprints
	English language; Full research paper
	Published between 2017 and 2026
Exclusion	Review papers, systematic reviews, or meta-analyses
	Purely theoretical papers without implementation
	Non-voting domains (healthcare, finance, etc.)
	Non-English publications
	Books, editorials, or opinion pieces
	Inaccessible full text due to paywalls

2.6 Screening and Selection Process (PRISMA)

The systematic screening process followed the PRISMA 2020 guidelines [16], as illustrated in Figure 1.

After deduplication of the 351 initial records, 349 unique studies underwent title and abstract screening, which narrowed the pool to 26 articles. Following full-text assessment, 15 studies met all inclusion criteria and were selected for the final synthesis (Table 4).

Table 4. Screening Flow Summary

Stage	Count
Initial identification (Databases + Other)	351
Records screened (Title)	349
Records screened (Abstract)	140
Records sought for retrieval	26
Final included studies	**15**

2.7 Data Extraction and Analysis

A structured data extraction sheet was used to capture, for each study: bibliographic details, study design, computer vision methods, IoT and hardware components, blockchain or cryptographic mechanisms, datasets, evaluation metrics, reported performance, limitations, and relevance to each research question. Extracted data were grouped and compared to identify recurring patterns and then synthesised into themes.

Studies were also assessed using an adapted quality checklist (clarity of objectives, methodological rigor, dataset quality, performance validation, real-world applicability, and relevance to the research questions). Each study received a 0–5 quality score; scores of 3.0 or higher were treated as acceptable.

2.8 Use of AI Tools

AI tools, including large language models, were used to assist in structuring the methodology description, reformulating sentences for clarity, and generating LaTeX boilerplate (tables, section structure, and BibTEX entries). AI systems were *not* used to fabricate data, performance metrics, or study characteristics; all quantitative results and methodological details originate from the primary studies and the PRISMA and data-extraction spreadsheets. Responsibility for study selection decisions, coding, and interpretation of results remains with the human author.

3. RESULTS

3.1 Overview of Included Studies

Following the systematic screening process, 15 studies were included for final synthesis and analysis (Table 5). These studies span publications from 2022 to 2025, with the majority published in 2024–2025 (n=12, 80%), reflecting the emerging nature of this research domain (Figure 3). The geographical distribution shows concentration in Asian countries, particularly India (n=7), followed by Bangladesh, Nigeria, Iraq, and other regions, with one international election observation report from Uzbekistan (Figure 2).

Publication venues include conference proceedings (n=6), peer-reviewed journals (n=5), preprints (n=3), and institutional reports (n=1). The majority of studies (n=11, 73%) present empirical research with reported performance metrics, while four studies (27%) remain at the conceptual design or survey stage without technical implementation.

Beyond identity verification, one study focused on automated voter flow monitoring, achieving 99.15% accuracy in counting voter entry and exit from polling booths using background subtraction and image processing techniques [7], although it did not address individual voter authentication.

3.2 Technical Approaches and Architectures (RQ1 & RQ2)

To address the research questions regarding technical implementation,the primary technologies employed across the selected studies were analyzed. Figure 4 illustrates the adoption rates of the three core technology domains: computer vision, blockchain, and IoT integration. *Note that categories are not mutually exclusive.*

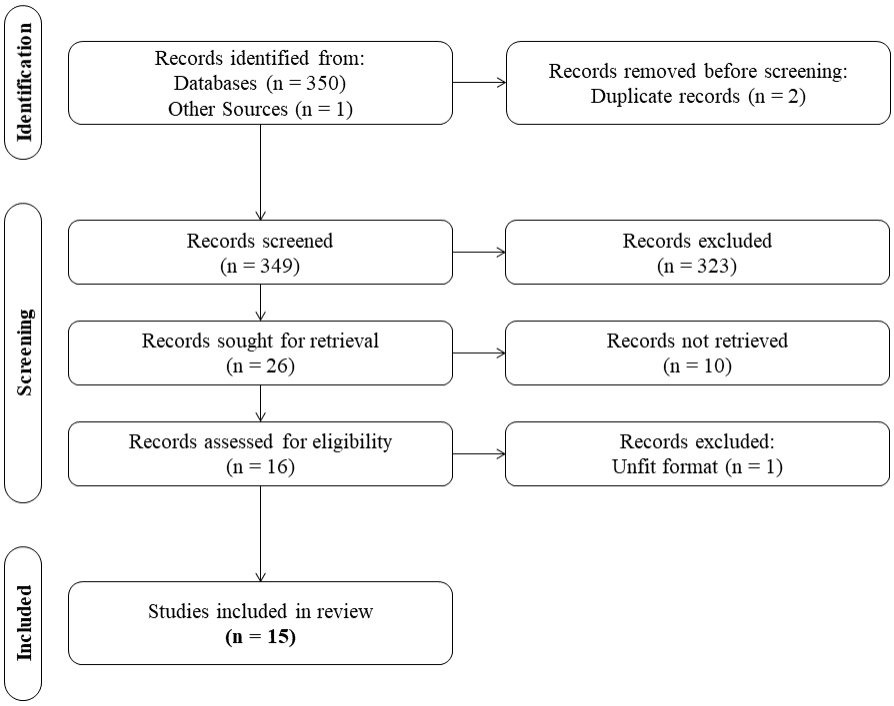

Figure 1. PRISMA 2020 Flow Diagram of the screening process.

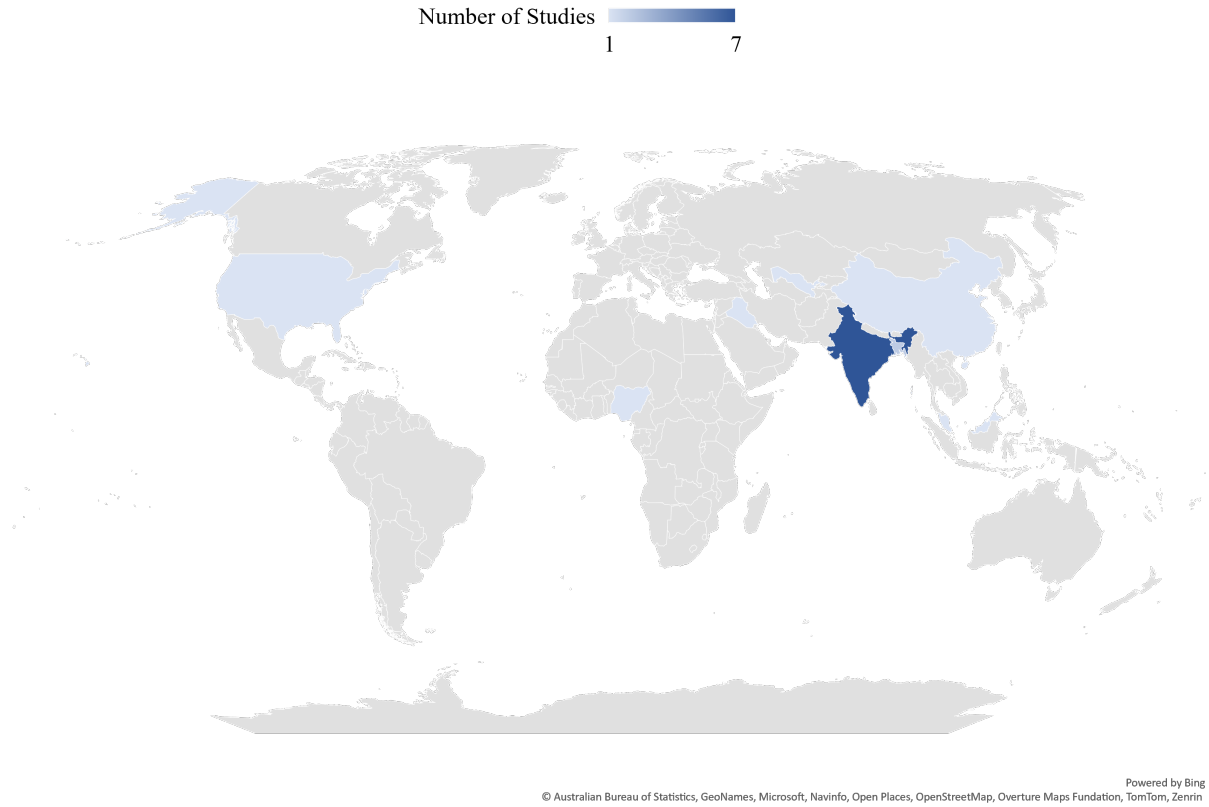

Figure 2. Geographical Distribution of Studies

3.2.1 Computer Vision Methods

Facial recognition emerged as the predominant computer vision technique (n=10 studies), implemented using various deep learning architectures: Convolutional Neural Networks (CNNs) with architectures including VGG16, VGG19, ResNet18, MobileNetV2; custom CNN models optimized for biometric verification; hybrid architectures combining ResNet and VGG features; OpenCV with Haar Cascade classifiers for face detection; and Dlib for facial landmark detection and encoding [1, 3, 10, 12, 14].

Fingerprint recognition was employed in four studies, utilizing Gabor filters, Hough transforms, and specialized fingerprint sensors (e.g., FPM10A modules). One notable implementation achieved 97% authentication accuracy with fingerprint scanning in a university election context [2].

Table 5. Overview of Included Studies

ID	Authors	Year	Venue Type	Country	Primary Focus	Quality
S01	Ajao et al.	2025	Journal	Nigeria	Multimodal biometrics + blockchain + Raspberry Pi	4.0
S02	Arun et al.	2022	Conference	Malaysia	Arduino + fingerprint + IoT + PubNub	3.0
S03	Dube et al.	2023	Conference	India	Facial recognition + CNN (design only)	2.0
S04	Zhao et al.	2023	Conference	USA	Ballot tabulation using DL (different phase)	4.0
S05	Atik et al.	2024	Conference	Bangladesh	Blockchain voting survey + cost analysis	3.0
S06	Tejushree et al.	2024	Conference	India	Blockchain + facial recognition (design only)	2.0
S07	ODIHR	2024	Report	Uzbekistan	Election observation (background context)	—
S08	Islam et al.	2024	Preprint	Bangladesh	Automated voter counting with ML	3.0
S09	Parin	2025	Journal	India	Blockchain + Aadhaar + stakeholder survey	3.0
S10	Mahmood et al.	2025	Journal	Iraq	Federated learning + CNN privacy-preserving	4.0
S11	Parivazhagan et al.	2025	Conference	India	Facial recognition with real-world testing	3.5
S12	Patra et al.	2025	Journal	India	Blockchain smart contracts prototype	3.0
S13	Anushalakshmi et al.	2025	Journal	India	Arduino + CV + Firebase complete system	4.0
S14	He et al.	2025	Preprint	China	Deepfake threats to biometric systems	3.5
S15	Dodla et al.	2025	Preprint	India	Decentralized web + CV + accessibility	4.0

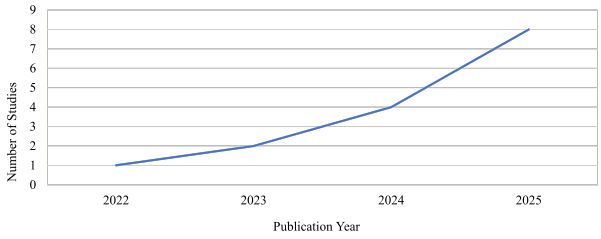

Figure 3. Accelerating Research Publications (2022 – 2025)

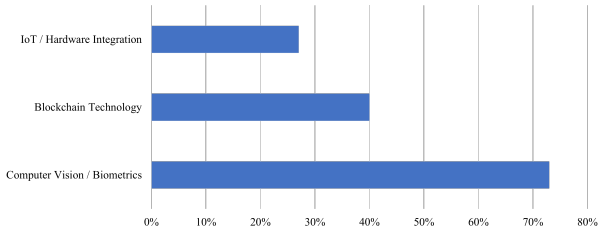

Figure 4. Prevalence of Key Technologies

Multimodal biometric systems combining facial recognition with fingerprint or iris scanning were proposed in three studies [1, 6], though few demonstrated actual fusion algorithms or comprehensive evaluation across modalities.

3.2.2 IoT Integration

Despite IoT being a core component of the research questions, explicit IoT integration was limited. Only three studies incorporated dedicated IoT hardware: Arduino-based systems (n=2) with microcontroller-based implementations including fingerprint sensors, LCD displays, and GSM modules for SMS confirmation [2, 12]; and Raspberry Pi deployment (n=1) with ARM Cortex-A76 processor, Pi Camera, and RFID integration for multimodal authentication [1].

The limited IoT adoption suggests that current research focuses more on software-based biometric systems rather than distributed sensor networks, which represents a significant gap given the potential of IoT for real-time monitoring across multiple polling stations.

3.2.3 Blockchain Integration

Blockchain technology was incorporated in five studies (33%), primarily using Ethereum-based smart contracts with Proof-of-Stake (PoS) consensus, private blockchain networks for vote recording and audit trails, homomorphic encryption (Paillier scheme) for privacy-preserving vote tallying, and IPFS (InterPlanetary File System) for decentralized storage [1, 5, 6, 8, 11].

One high-quality implementation deployed Ethereum Sepolia testnet for a real-world university election with 2,423 voters, demonstrating 1,424.5 transactions per second and 99.96% acceptance rate [1].

3.2.4 System Architectures

Three primary architectural patterns emerged: (1) **Centralized Web-Based Systems** (n=6): Traditional client-server architecture with centralized databases, suitable for small-scale deployments but vulnerable to single points of failure [3, 2, 6, 10, 12, 14]; (2) **Distributed Blockchain Systems** (n=5): Decentralized ledgers with smart contracts for immutable vote recording, providing enhanced transparency and auditability [1, 5, 6, 8, 11]; (3) **Federated Learning Systems** (n=1): Privacy-preserving architecture where biometric models are trained locally across distributed sites without centralizing sensitive data [9]. The federated implementation achieved 99.75–99.97% accuracy across six distributed sites using federated CNNs for fingerprint and gender-based authentication.

3.3 Performance Outcomes and Validation (RQ3)

Table 6 summarizes performance metrics reported across studies with quantitative evaluation.

Table 6. Performance Metrics of Key Implementations

Study	Accuracy	FAR	FRR	Real-world
S01 [1]	100% TAR	0.00%	0.00%	Yes (n=2,423)
S02 [2]	97% auth, 95% vote	—	—	Limited (n=19)
S10 [9]	99.75–99.97%	—	—	No (simulated)
S11 [10]	98.7%	0.05%	1.2%	Limited (n=120)
S04 [4]	99.984%	—	—	Yes (n=92,780 ballots)

High-performing systems achieved accuracy rates exceeding 99%, with the best implementation reporting 100% True Acceptance Rate (TAR) with zero False Acceptance Rate (FAR) and False Rejection Rate (FRR) in a real university election [1]. However, this exceptional performance was achieved in a controlled, single-location environment with cooperative participants. Processing times varied considerably: facial recognition authentication ranged from 2.4 seconds [10] to over 300 seconds per voter [1] for comprehensive multimodal biometric verification with blockchain recording.

3.3.1 Real-World Deployment

Among the empirical studies, only four (27%) reported testing in actual or simulated election contexts: university elections (n=2) with 2,423 voters [1] and 19 volunteers [2]; a ballot counting system (n=1) using 92,780 ballot images [4]; and a simulated voting environment (n=1) with 120 participants [10].

The remaining empirical studies (n=7) were validated only in laboratory settings using standard datasets or test benches, lacking deployment in voting scenarios. This distinction highlights that while technical feasibility is well-established, real-world operational validation remains a critical gap in the literature.

3.3.2 Scalability Concerns

Scalability testing was notably absent from most studies. One federated learning implementation evaluated performance degradation when scaling from 6 to 12 distributed sites, observing a 3.68% accuracy decline for ID recognition tasks [9]. No studies examined scalability to national election levels involving millions of voters across thousands of polling stations.

3.4 Contextual Background: Documented Electoral Challenges

To contextualize the need for technology-enhanced voter verification, the OSCE ODIHR observation of Uzbekistan's October 2024 parliamentary elections [15] provides quantifiable evidence of systematic verification challenges: 12% of polling stations assessed negatively for serious procedural violations; 21% failed to properly check voters against electronic registers; 11% lacked access to electronic voter registers entirely; 24% showed seemingly identical signatures on voter lists; 43% of counting processes assessed negatively; and direct observations documented multiple voting (1%), proxy voting (1%), and ballot box stuffing indicators (2%).

These documented failures underscore the practical need for automated, tamper-resistant verification mechanisms that computer vision and IoT technologies could potentially address.

3.5 Thematic Synthesis

This section synthesizes how the reviewed systems collectively address RQ1–RQ3 by grouping recurring patterns in technologies, architectures, and security considerations into three overarching themes.

3.5.1 Theme 1: Biometric-Blockchain Convergence

A dominant pattern across high-quality studies is the integration of biometric authentication with blockchain for enhanced security and transparency [1, 5, 11]. This hybrid approach leverages computer vision for identity verification (preventing impersonation), blockchain for immutable audit trails (preventing vote tampering), smart contracts for automated counting and result verification, and cryptographic techniques (homomorphic encryption, zero-knowledge proofs) for privacy preservation.

However, implementations remain largely conceptual or limited to small-scale prototypes. The computational overhead of blockchain consensus mechanisms, including proof-of-stake mining and transaction validation [1], raises questions about scalability to high-throughput election scenarios.

3.5.2 Theme 2: Limited IoT Integration

Despite IoT being central to the research questions, its integration remains underdeveloped. The few implementations incorporating IoT hardware primarily use microcontrollers (Arduino, Raspberry Pi) as standalone voting terminals rather than networked sensor arrays [2, 12]; basic sensors (fingerprint scanners, cameras, RFID readers) without sophisticated IoT communication protocols; and cloud platforms (Firebase, PubNub) for centralized data storage, but not true edge computing or distributed IoT architectures.

This gap suggests that the vision of distributed, real-time IoT-based voter monitoring across multiple polling stations remains largely unrealized in current literature.

3.5.3 Theme 3: Security and Privacy Challenges

Several critical security concerns emerged. Only three studies explicitly addressed liveness detection or anti-spoofing measures [13, 12]. Most facial recognition systems remain vulnerable to photo-based or video-based spoofing attacks and AI-generated deepfakes [13]. Centralized storage of biometric data raises privacy concerns, though federated learning [9] and homomorphic encryption [1] offer privacy-preserving alternatives with limited adoption. Systems requiring internet connectivity for cloud databases or blockchain synchronization are vulnerable to denial-of-service attacks, network partitioning, or latency issues in rural areas [14]. Few studies addressed administrator-level security or protection against malicious insiders.

4. DISCUSSION

4.1 Key Findings

This systematic review reveals a nascent but rapidly evolving research domain at the intersection of computer vision, IoT, and electoral security. Three key findings emerge:

1. Biometric authentication, particularly facial recognition, demonstrates technical feasibility for voter verification with accuracy exceeding 97% in controlled environments. The best implementations achieve near-perfect accuracy (99–100% TAR) with minimal false acceptance rates ($<0.05\%$) [1, 10, 9]. However, these results are typically obtained in small-scale, cooperative settings with high-quality imaging conditions and willing participants.

2. Real-world deployment and scalability validation remain critical gaps. Only 27% of studies report actual deployment in electoral contexts, and none have demonstrated scalability to national election levels. The transition from lab-

oratory prototype to production system capable of handling millions of voters across geographically distributed polling stations is largely unexplored.

3. IoT integration is significantly underdeveloped relative to its potential. Despite the promise of IoT for distributed real-time monitoring, hardware implementations remain limited to individual voting terminals [2, 12] rather than coordinated sensor networks capable of cross-station verification. This represents a missed opportunity for comprehensive, multi-station verification systems.

4.2 Implications for Practice

The documented electoral challenges in Uzbekistan's 2024 parliamentary elections [15] directly align with the problems that computer vision and IoT technologies aim to address: inadequate voter verification (21% failure rate) could be mitigated by biometric authentication systems with 97–100% accuracy demonstrated in reviewed studies; multiple and proxy voting (1% direct observation) could be prevented through real-time biometric cross-checking across polling stations, enabled by IoT networks; identical signatures (24% of observations) indicate the failure of manual verification methods that could be replaced by fingerprint or facial recognition systems [1, 2]; and counting discrepancies (43% negative assessment) could be reduced through automated, blockchain-based tallying with immutable audit trails [11, 8].

While none of the reviewed systems have been deployed in Uzbekistan specifically, the technical approaches demonstrated in countries like Nigeria, India, and Iraq provide proof-of-concept for similar applications.

4.3 Limitations of This Review

Several limitations must be acknowledged: **Timeline Constraints**—the compressed timeline for this SLR limited the exhaustiveness of the search strategy and depth of analysis; **Paywall Access**—significant barriers in accessing full-text articles due to institutional paywall limitations meant some potentially relevant studies could not be fully evaluated, introducing possible selection bias toward open-access publications; **Rapid Field Evolution**—studies published even 1–2 years ago may be outdated by current state-of-the-art methods; **Geographic Bias**—the predominance of studies from South Asia (particularly India) may limit generalizability to other contexts with different infrastructure, regulatory environments, and cultural norms around biometric data collection; and **Publication Bias**—like all systematic reviews, this work is limited to published research, which may overrepresent positive results and underrepresent null findings or failed implementations.

4.4 Future Research Directions

Based on identified gaps, several high-priority research directions emerge: develop and evaluate distributed IoT sensor networks for multi-station voter monitoring with edge computing and fault-tolerant architectures; systematically evaluate biometric systems against sophisticated attacks including deepfakes [13]; conduct pilot deployments at scale (thousands of voters, dozens of polling stations) to identify performance bottlenecks; further develop federated learning approaches for privacy-preserving distributed authentication [9]; investigate adaptation for different cultural and regulatory contexts, with attention to underserved regions; and conduct comprehensive economic evaluations comparing implementation costs and security benefits of technology-enhanced systems versus traditional methods.

5. CONCLUSION

This systematic literature review examined 15 studies investigating the integration of computer vision and IoT technologies for enhancing voter verification accuracy in electoral systems. The findings reveal that while biometric authentication achieves high accuracy (97–100%) in controlled environments, real-world deployment remains limited and scalability to national elections largely unproven. Blockchain integration offers promising approaches for transparency and audit trails, but IoT adoption is significantly underdeveloped relative to its potential for distributed, real-time monitoring.

The documented electoral challenges in contexts like Uzbekistan—where recent election observations identified systematic verification failures affecting 12–43% of polling stations—underscore the practical urgency for robust, technology-enabled solutions. Computer vision and IoT technologies directly address documented weaknesses including inadequate voter verification, multiple voting, and counting discrepancies.

Critical research gaps include: (1) limited real-world validation beyond prototype demonstrations, (2) absent scalability testing to large-scale elections, (3) underdeveloped IoT architectures for distributed monitoring, and (4) insufficient adversarial robustness evaluation against sophisticated attacks. Despite constraints due to timeline limitations and paywall access barriers this work contributes a synthesized understanding of current technical approaches, performance outcomes, and critical research frontiers.

The convergence of computer vision, IoT, and blockchain technologies holds substantial promise for transforming electoral integrity, but realizing this potential requires bridging the gap between laboratory prototypes and production-ready systems capable of safeguarding democratic processes at scale.

6. ETHICS STATEMENT

This systematic literature review was conducted in full compliance with academic integrity standards. All sources have been properly cited using IEEE format, and the methodology is designed to be transparent and reproducible. The search logs provided in the methodology are based on actual database queries conducted between November 14 and November 20, 2025. No data was fabricated, and all included studies were systematically screened according to the documented protocol.

REFERENCES

[1] L. A. Ajao, B. U. Umar, H. O. Ohize, E. M. Dogo, E. Esenogho, and M. Cameron, "Blockchain Integration With Multimodal Biometric Authentication System for Secure Smart Verifiable Electronic Voting System," *IEEE Access*, vol. 13, pp. 189850–189868, 2025. doi: 10.1109/ACCESS.2025.3618970.

[2] K. C. Arun, S. Ahmad, S. Noor, I. Mumtaz, and M. Ali, "Arduino Based Secure Electronic Voting System with IoT and PubNub for Universities," in *2022 Second International Conference on Advanced Technologies in Intelligent Control, Environment, Computing & Communication Engineering (ICATIECE)*, Bangalore, India, 2022, pp. 1–5. doi: 10.1109/ICATIECE56365.2022.10047605.

[3] S. Dube, M. V. S. Sandeep, H. Challagundla, and P. N. Chand, "Deep Learning & Computer Vision Integrated Smart Voting System," in *2023 International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, Ballar, India, 2023, pp. 1–6. doi: 10.1109/ICDCECE57866.2023.10151439.

[4] F. Zhao, C. Zhang, N. Saxena, D. Wallach, and A. S. A. Rabby, "Ballot Tabulation Using Deep Learning," in *2023 IEEE 24th International Conference on Information Reuse and Integration for Data Science (IRI)*, Bellevue, WA, USA, 2023, pp. 107–114. doi: 10.1109/IRI58017.2023.00026.

[5] M. Atik, S. S. Tarin, M. Rahman, A. A. Alvi, and A. Sohan, "A Comprehensive Analysis of Blockchain-Based Voting Systems: Enhancing Transparency and Security," in *Proceedings of the International Conference on Computing Advancements (ICCA)*, Oct. 2024, pp. 733–740. doi: 10.1145/3723178.3723275.

[6] T. R. P, A. Prasad, V. C. R, V. R. Chandramule, P. K, and S. N, "Secure E-voting: Leveraging Blockchain technology and Face recognition for enhanced authentication," in *2024 1st International Conference on Advances in Computing, Communication and Networking (ICAC2N)*, Dec. 2024, pp. 1805–1810. doi: 10.1109/icac2n63387.2024.10895391.

[7] M. J. Islam, S. A. Karim, and M. Faris, "Revitalizing Electoral Trust: Enhancing Transparency and Efficiency Through Automated Voter Counting with Machine Learning," *SSRN Electronic Journal*, Jan. 2024. doi: 10.2139/ssrn.5003151.

[8] D. Parin, "Blockchain-Based Transparent Voting System: A Decentralized Approach," Zenodo (CERN European Organization for Nuclear Research), Sep. 2025. doi: 10.5281/zenodo.17236109.

[9] W. A. Mahmood, J. Waleed, and A. R. Abbas, "A Privacy-Preserving E-Voting System using Federated Learning and CNNs for Secure Fingerprint and Biometric Verification," *Diyala Journal of Engineering Sciences*, pp. 178–194, Sep. 2025. doi: 10.24237/djes.2025.18312.

[10] A. Parivazhagan, G. Saipradeep, R. Praveen, K. Devendra, and S. S. K. Reddy, "Smart Voting System with Computer Vision," in *2025 6th International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)*, Jun. 2025, pp. 652–658. doi: 10.1109/icicv64824.2025.11085464.

[11] A. Patra, S. Basu, and K. Majumder, "Blockchain-enabled Secured and Transparent E-Voting System using Smart Contracts," *International Journal of Next-Generation Computing*, Apr. 2025. doi: 10.47164/ijngc.v16i1.1843.

[12] M. Anushalakshmi and T. Prabhu, "AI-Powered Voter Authentication & Fraud Prevention with a Smart, Arduino Driven Next-Gen Voting System," *International Research Journal of Modernization in Engineering Technology and Science*, pp. 2582–5208, 2025. doi: 10.56726/IRJMETS77876.

[13] S. He, Y. Lei, Z. Zhang, and J. Ye, "Identity Deepfake Threats to Biometric Authentication Systems: Public and Expert Perspectives," arXiv preprint arXiv:2506.06825, Jun. 2025. doi: 10.48550/arXiv.2506.06825.

[14] S. D. Dodla et al., "Real Time Secure And Decentralized Voting System," *SSRN Electronic Journal*, Jan. 2025. doi: 10.2139/ssrn.5037851.

[15] OSCE Office for Democratic Institutions and Human Rights, "Republic of Uzbekistan: Parliamentary Elections 2024 – Final Report," OSCE/ODIHR, Warsaw, Poland, Tech. Rep., 2024.

[16] M. J. Page et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, vol. 372, p. n71, 2021. doi: 10.1136/bmj.n71.