Mustansiriyah Journal of Pure and Applied Sciences, Print ISSN: 2957-9910. Online ISSN: 2957-9929, Vol. 3, No. 2, 2025, Pages 135-152
DOI: 10.47831/mjpas.v3i2.324

MJPAS

MUSTANSIRIYAH JOURNAL OF PURE AND APPLIED SCIENCES

Journal homepage:
https://mjpas.uomustansiriyah.edu.iq/index.php/mjpas

RESEARCH ARTICLE - COMPUTER SCIENCE

Secure E-voting authentication system employing biometric technology, Crypto-Watermarking Approach and blockchain technology: A Review

Asia Abdullah Ahmed [1*], Nada Hussein M. Ali [2]

[1] University of Baghdad, College of Science, Department of Computer Science, Baghdad, Iraq

[2] University of Baghdad, College of Science, Department of computer science, Baghdad, Iraq

[*] Corresponding author E-mail: asia.Ahmed2201m@sc.uobaghdad.edu.iq , nada.husn@sc.uobaghdad. edu.iq

Article Info.

Article history:

Received
16 September 2024

Accepted
30 September 2024

Publishing
30 March 2025

Abstract

Moderately, advanced national election technologies have improved political systems. As electronic voting (e-voting) systems advance, security threats like impersonation, ballot tampering, and result manipulation increase. These challenges are addressed through a review covering biometric authentication, watermarking, and blockchain technologies, each of which plays a crucial role in improving the security of e-voting systems. More precisely, the biometric authentication is being examined due to its ability in identify the voters and reducing the risks of impersonation. The study also explores the blockchain technology to decentralize the elections, enhance the transparency and ensure the prevention of any unauthorized alteration or manipulation of the results. Additionally, the watermarking technology is examined for viewing the ability to store and transmit the voting result in secure manner though preserving the confidentiality ensure fair elections. this review contribution is the combination evaluating of biometric authentication, watermarking, and blockchain technologies effectiveness to develop robust e-voting framework. as a result, the key finding indicates a hybrid approach that integrates those technology offers a solution to address the security challenges.

The official journal published by the College of Education at Mustansiriyah University

Keywords: E-voting System; Biometric Authentication; Blockchain; Watermarking

1. Introduction

Elections are crucial in democratic systems for citizens to express their views and choose their representatives. There are two main voting methods: traditional and electronical. Traditional voting is costly and time-consuming, involving paper ballots and a substantial workforce. Concerns about the integrity of traditional elections include issues with ballot boxes like loss, manipulation, or destruction [1], as well as the potential for fraudulent repeated voting [2]. To address these challenges, electronic voting systems are increasingly being adopted as an alternative [3] [4]. Electronic voting assumes various forms and aims to expedite and enhance the accuracy of the voting, tallying, and counting procedures compared to conventional methodologies [5]. However, the security of electronic voting remains a persistent concern. A range of threats, such as Distributed Denial of Service (DDoS) attacks, SQL Injection, Man in the Middle (MitM) attacks, malware, spoofing, phishing, and ciphertext attacks, continue to pose ongoing risks to the dependability of electronic voting systems [6].

This review paper demonstrates three technology that will aid in addressing the challenges introduced in the e-voting system, these technologies include biometric authentication, watermarking technologies and blockchain technology. firstly, the biological characteristics are used to improve resilience in user identification and authentication, making spoofing and falsification more difficult. Since each biometric characteristic listed is almost exclusively unique to a single person, identity fraud is more difficult. There's also the added benefit that these characteristics are constantly present because they are integral to our identity[7], [8]. Hence The E-voting system incorporates biometric technology[9], which is widely acknowledged as more secure compared to traditional voting, thereby enhancing the safety of the democratic voting process[10], [11].

The second technology is the watermarking technology which is the process of adding a signal or hidden information into digital material, including audio, video, and images is known as digital watermarking. Subsequently, the encoded data is identified and retrieved to disclose the actual owner of the digital material[12]. Watermarking is a commonly employed technique for addressing security concerns, including safeguarding data from unauthorized duplication and modifications. Security, robustness, and imperceptibility are crucial factors to take into account while designing a watermarking method[13].

The last method the review paper explore is blockchain technology that become an essential alternative for addressing many of the security challenges associated with e-voting[14].blockchain technology known as A decentralized, distributed, and unchangeable ledger that is used to keep an ever-expanding list of entries, or blocks[15]Blockchain technology provides a decentralized electronic or online voting node. Electronic voting systems have recently been created using distributed ledger technologies, mostly due to its advantages in end-to-end verification. With attributes like decentralization, non-repudiation, and security protection, blockchain presents an appealing alternative for traditional electronic voting methods[16].

A thorough understanding is provided of how these integrated solutions contribute to the creation of secure, transparent, and resilient electronic voting systems in the modern electoral landscape by

1. Performing a comprehensive analysis of the biometric authentication, watermarking, and blockchain technologies and highlighting the effects in securing e-voting systems.
2. Biometric authentication is employed not just for identification of the voter in a secure way but also for impersonation prevention, which is not well addressed in the past works with multilayer security approaches.
3. The system applies watermarking to guarantee the integrity and confidentiality of the transmission of voting results' which is unique in the application in the e-voting domain.
4. This work considers blockchain technology and its potential to decentralize the voting processes in order to make them more transparent and trustworthy by ensuring impossibility to make unauthorized changes to votes as a new contribution into discussions on blockchain-based e-voting.

The rest of the paper is organized as follows. Section 2 describes an overview of the security method used in the E-voting system. Section 3 describes the literature review on e-voting system based on biometric authentication and secure watermarking systems. Section 4 represent the conclusion of the paper.

2. Preliminaries

A comprehensive understanding of the security landscape is established through an exploration of foundational methodologies.

2.1 Biometric authentication

Biometric identification has become a significant area of research in science [17]. In various applications the individual's identity is determined by their unique biological or occasionally other personal information. Individual automated identification plays a pivotal role. This is due of their precision and ease of usage in differentiating between impersonators and the user's true personality[18]. Furthermore, its non-intrusive acquisition, stability over time, and its human-perceivable differences[19] .

Biometric data is categorized into two groups: behavioral (related to knowledge) including voice, signature and keystroke. and physiological (related to physical traits) including fingerprint, face, iris, hand and finger-vein [20], [21], [22], [23]. Fig1. illustrates commonly used biometric identification features[24].

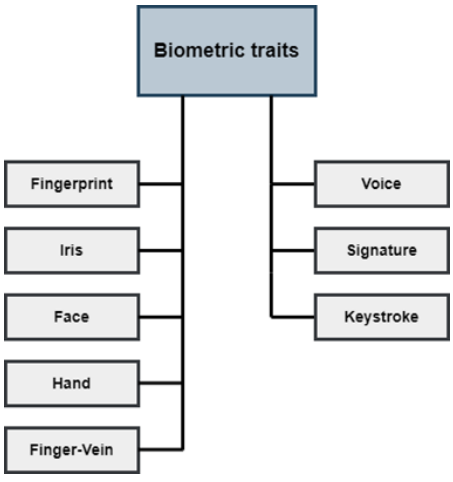

Fig. 1. Commonly used biometric features [24]

In the authentication mode, a biometric system is employed for either identification or confirmation purposes. During the confirmation phase, the system validates a user's identity by comparing the captured characteristics with a stored template. Fig. 2 illustrates how this process is executed [25]

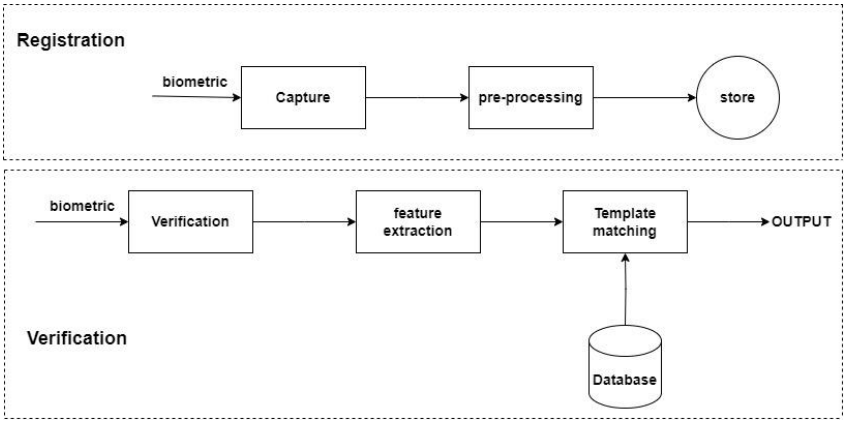

Fig. 2. Biometric registration and verification process[25]

When compared to alternative identification techniques, biometrics provide some benefits that are impervious to compromise and forget [26]. In addition, an effective biometric authentication system should not only be secure but also accurate and practical, it must be resilient against the types of attacks listed in Table 1 and safeguard user secrets. Evaluating a biometric authentication system's performance is crucial, focusing on aspects like precision, efficiency, user-friendliness, security, and privacy [27].

Table 1. various forms of attacks on biological characteristics[27]

Biological Traits	Type of Attack
Face recognition attacks	Attackers get the information they want online through social networks. With the help of these images and videos, a facial recognition system would be easy to deceive.
Iris recognition attack	It is now feasible to attack an iris-based identification system and steal an image of the iris thanks to the development of high-resolution cameras. However, premium optical designs are typically costly.
Fingerprint attack, palmprint attack	A fake finger can be made from a variety of materials, including Silica gel, latex, gelatin, and others. Fingerprints can be gathered from surfaces touched by users.
Voice attack	Because sound travels in all directions in an open area, an attacker who records and duplicates a user's speech during user authentication is particularly likely to mislead the voice-based authentication system.
Keystroke and touch dynamics attack	It is difficult to imitate the acts of others. A keyboard and touch-based authentication system, on the other hand is vulnerable to statistical attacks.

The integration of the biometric traits within e-voting systems gaining a numerous benefit for securing the voting process including ensuring voter verification, prevent u authorize access and reducing the possibility of voter impersonating and fraudulent voting. The studies [28] and [29] highlights the importance of the biometric authentication in enhancing the reliability in addition to Ensuring the authentication of each vote by the legitimate individual. Furthermore, the integration of biometrics such as the fingerprint as proposed in [30] may significantly reduce the risks related to traditional authentication

techniques including passwords and identity cards which can get lost, stolen or be misused easily. Fig. 3 presents a workflow example of a biometric based e-voting system [31].

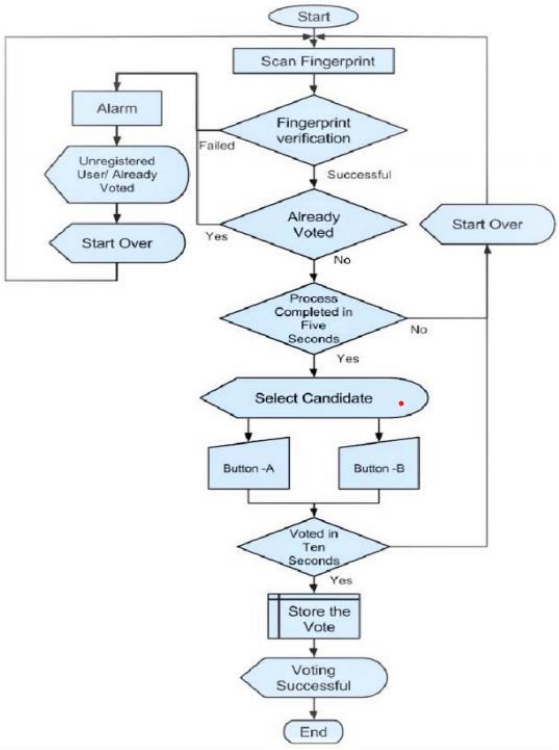

Fig. 3. E-voting system within biometric authentication [31]

2.2 Watermark technology

The proliferation of digital technology and internet usage in recent years has given birth to a new wave of complicated concerns, including the protection of intellectual property rights, the establishment of trustworthy methods of identification, and the assurance of the validity and credibility of digital material. Recently, watermarking has been shown to be a successful way to deal with these issues[32]. In addition, digital watermarking techniques are employed to enhance the security aspects of information transfers over the internet[33] .

Digital watermarking involves inserting a piece of data, known as a digital watermark, into multimedia content [34]. Watermarking entails two stages, as seen in Fig. 4 [35]:

- An embedding operation conducted on the transmitting side
- The extraction procedure used to extract the watermark at the receiving end

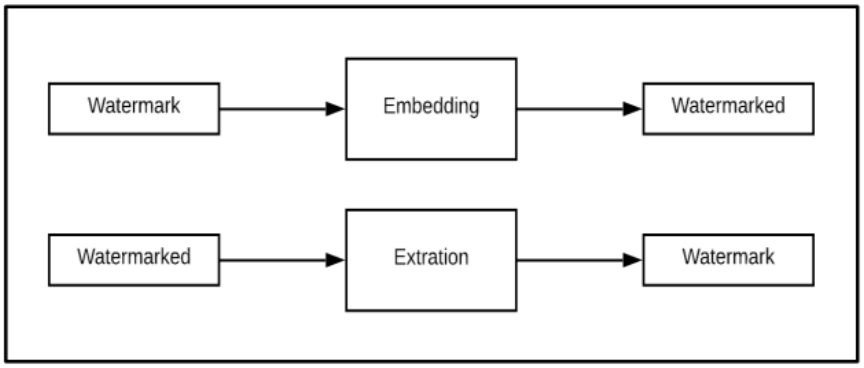

Fig. 4. The main process of watermark [35]

The categorization of watermarking images is based on several criteria, including human perception, watermark domain, accessibility, and the type of cover media[36], [37], as presented in Fig. 5.

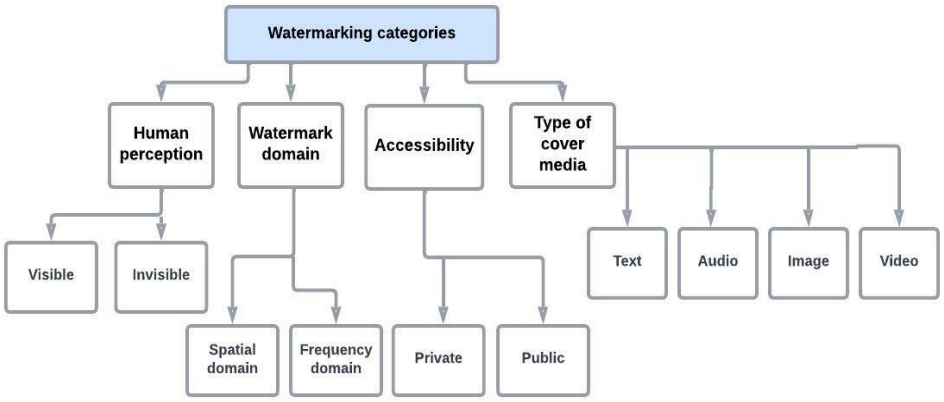

Fig. 5. Watermark categories [32], [33]

A reliable watermarking system must adhere to four key criteria [13], [34], [35], [36], [37], [38]:

- Transparency, where the watermark remains imperceptible to the human eye when added to the host image.
- Robustness, ensuring the watermark can still be accurately extracted from the image even when subjected to various attacks.
- Capacity, meaning the embedded watermark within an image should have enough capacity to store all copyright-related information.
- Security, making it challenging for an adversary to detect the embedded watermark to enhance capacity and security in watermarking, cryptographic techniques are employed.
- However, this can upset the delicate balance between execution speed, robustness, and overall complexity. Encrypting the data prior to insertion and decrypting it after extraction may introduce delays in real-world scenarios [43].

Although the use of watermarking in e-voting systems is not widespread, it has proven to be effective in addressing the challenges of current electoral systems. The watermarking technology contributes in enhancing the authenticity and the integrity of the voting process. The study [44] highlighted the importance of the watermarking in Guaranteeing that every vote remains secure and immune to tampering throughout the whole process, from when it is cast to when it is counted. This capacity is essential for safeguarding against the manipulation of vote values, a prevalent concern in electronic voting, particularly when votes are transmitted across potentially insecure networks. In addition to ensuring the robustness against the cyberattacks [45]. The fig. 6 shows the voting process employing the watermarking technology.

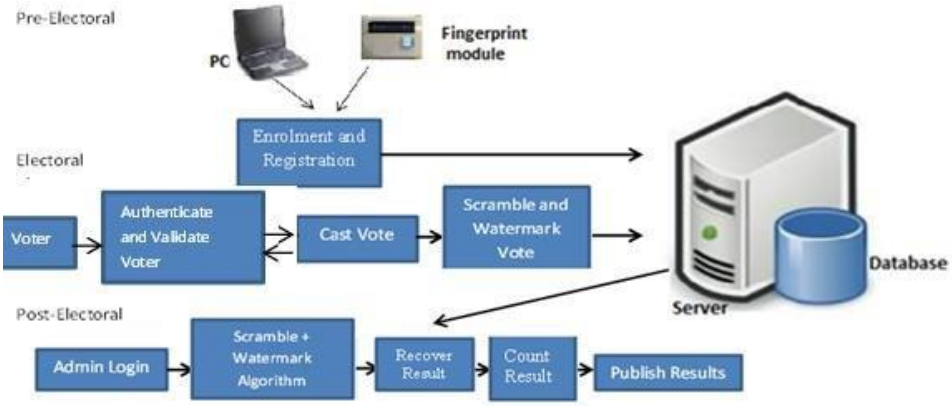

Fig. 6. E-voting system employing the watermarking technology

2.3 Blockchain technology

Blockchain, functioning as a distributed and immutable ledger of transactions, is most useful in untrustworthy decentralized situations. This is accomplished by documenting transactions and building decentralized consensus on the legitimacy of the transaction record. Furthermore, the operational code encoded in transactions simplifies the execution of software services, allowing users to communicate in an untrusted environment [46].

Blockchain is classified into three types: public, private, and consortium. The blockchain is public because it is shared by many nodes, but it is also private since only a small number of nodes can access it. A consortium blockchain is one in which certain nodes are in charge of establishing consensus while others can participate in transactions[47].

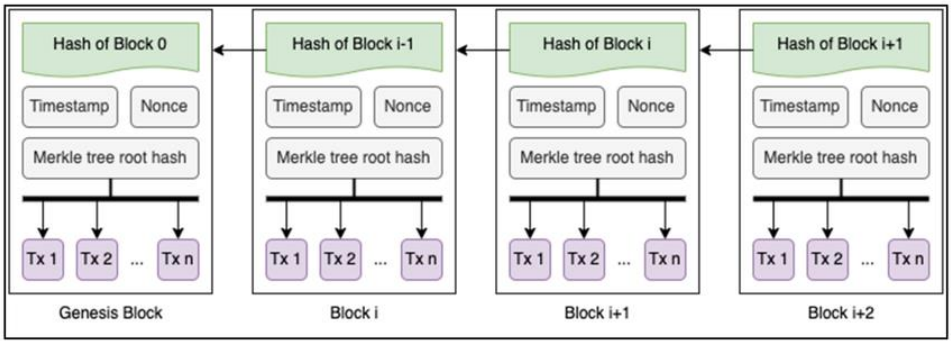

Fig 7. Blockchain structure [48]

The Blockchain consists of interconnected blocks storing transactional data, linked by reference hashes to their parent blocks, excluding the genesis block. Each block comprises a header and body as shown in fig. 7 and table 2, with metadata in the header. The block body contains recorded transactions and a counter for additional transactions, with the block's capacity determined by size constraints. Blockchain ensures authenticity through digital signatures and asymmetric cryptography, with participants using private-public key pairs for transaction security. Distributed public keys enhance transparency and trust among network users[48].

Table 2. Block header attributes [48]

Header Attributes	**Definition**
Block Version	Indicates which set of block validation rules to follow.
Previous Block	Hash A 256-bit hash value that points to the previous block.
Merkle tree root	The hash value of all the transactions in the block.
Timestamps	Current timestamp as seconds since 1970-01-01T00:00 UTC.
nBits	Current hashing target in a compact format.
Nonce	A 4-byte field that usually starts with 0 and increases with each hash calculation.

The blockchain has following key characteristics[49]:

- Decentralization: In contrast to centralized transaction systems, blockchain enables peer-to-peer transactions, reducing server costs and mitigating performance bottlenecks at central servers.
- Persistency: Transactions in blockchain are confirmed and recorded in distributed blocks, making tampering nearly impossible. Validation by other nodes and transaction checks enhance security, allowing easy detection of falsification.
- Anonymity: Users interact with blockchain through generated addresses, and the option to create multiple addresses protects identities. The decentralized nature eliminates the need for a central entity to store private information, preserving privacy within acknowledged constraints
- Auditability: Transactions in blockchain are validated, timestamped, and recorded, enabling users to verify and trace records through any distributed network node. In Bitcoin blockchain, transactions can be iteratively traced, improving traceability and transparency.

The blockchain plays a vital role in the context of e-voting, which can be demonstrated through the following:

- Security and Transparency: the blockchain grants the immutable ledger and the decentralization that ensuring one vote is recorded and ensuring that every alteration is detectable. While the transparency means recording all the votes in the blockchain in accessible manner to the network participants [50].
- Decentralization: the blockchain technology enables beer to beer transaction in order to reducing the single point failure [51].

- Persistency and Auditability: recording the votes within the blockchain make the votes tamperproof due to the vote stored in distributed blocks furthermore enhance the voting process security by making the process trackable and auditable [52].
- Anonymity: The blockchain employing the cryptographic technique to protect the voter privacy by ensuring the voters identity not linked to their votes [53]. Fig. 8 shows an example of the e-voting system based on blockchain technology.

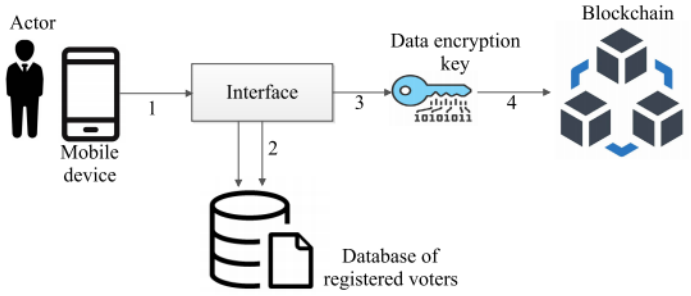

Fig. 8. The e-voting system based on the blockchain technology [54]

3. Literature review

3.1 Electronic voting system based on biometrics authentication

The integration of biometric authentication has gained significant attention as a potential solution to enhance security and accuracy. This literature review explores the method, objective and limitation of biometric authentication in the context of voting systems.

In [55] The researchers have designed a preliminary model of an electronic voting device that employs fingerprint biometric technology to authenticate voters. The suggested system entails the incorporation of this technology with the database administered by the Unique Identification Authority. The limitation of This system is performed on small scall election in addition, the system may be vulnerable to spoofing attack. The reliance on a central database may rase a concern in facing a centralized attack, data breaches and single point failure.

The study[56] introduces a secure online e-voting crypto-biometric technique, incorporating Gabor filtering, palmprint, and palm-vein features. The method encrypts data with a randomly generated key, integrated into a biometric feature vector using a fuzzy commitment mechanism. The study aims to reduce voting violations and secure voter information against potential fraud. Limitations include evaluation on limited datasets (300 voters), the lack of real-world sensor-based testing in the research in addition to the Gabor filtering and Fuzzy schemes may not be implemented in a fully optimized manner for real-time processing during large-scale elections. In the PLP modality, the Genuine Acceptance Rate (GAR) achieved a value of 99.984%, and in the PLV modality, it was 99.981% for open identification.

The [57]propose a system with three-tiered security strategy that includes an individual identity code, a time-expiring token password that is refreshed every five minutes, and the use of biometrics, which includes iris and fingerprint data and the time taken for the enrollment is 5 seconds. The principal goals of this study is eliminate fraud and the possibility of voting multiple times while the possible limitation is lacks the safeguards implemented to uphold the data's integrity in order to thwart any unauthorized access or malicious alterations furthermore, the system's dependency on a token password that expires in time, especially in regions of low connectivity where refreshes of the token can cause disenfranchisement of the voter due to delayed or missed authentication attempts..

The research [58] put forward an electoral system with dual-factor biometric authentication, combining fingerprint and iris recognition, to address identified challenges. The use of MySQL for managing machine tables and creating a user-friendly graphical interface aims to improve voter identification and deter electoral fraud. However, a limitation exists as the study discusses MySQL's role in data management but lacks exploration of data security, storage capacity, and redundancy measures in addition to employing dual- factor for the authenticity may lead to Expensive hardware expenses and the need for sophisticated maintenance of systems. The electoral system yielded 94 percent accuracy. While Iris response time for voter enrollment and verification is 15s and 20s, Fingerprint response time is 3s and 9s.

The study [59]introduces an electronic voting system with facial recognition using advanced deep learning techniques, integrating blockchain technology and a blind signature mechanism for enhanced security and trustworthiness. While Convolutional Neural Networks (CNN) are employed for facial recognition with achieved accuracy is 99% , the research lacks thorough examination of protective measures against counterfeit representations like photographs, videos, and masks. Moreover, latency and scalability issues may raise due to the incorporation of the blockchain technology and the blind signature.

The study[60]proposes an Electronic Voting Machine to address tampering, fraudulent voting, and security concerns. The design incorporates biometric data, specifically fingerprints, for voter authentication. The envisioned prototype includes an LCD display, a ballot unit, and a control unit. The time taken between successive vote is 60 seconds . However, limitations exist due to a lack of real-world testing, and there is a gap in specifying critical security measures, including secure data transmission and encryption techniques.

In the research [61]] introduces an AI-driven facial detection and identification system for online voting, employing machine learning and deep learning techniques to evaluate facial features. The key goals encompass improving online voting security, ensuring eligibility, preventing multiple voting instances, preserving voter confidentiality, and accurately tallying valid votes. The face recognition accuracy up to 98%. However, the research lacks a comprehensive examination of safeguards against counterfeit facial representations, furthermore it predominantly focuses on elucidating MySQL's role in data management, important factors like data security are not taken into account and the AI-powered facial recognition system may exhibit algorithmic bias, resulting in a greater likelihood of misidentifying or falsely authenticating individuals.

Table 3 shows various research in biometric authentication in the context of voting system.

Table 3. biometric authentication in voting system

Ref / Year	Method	Objective	Limitation	Evaluation Metric
[56] 2018	An integrated crypto-biometric method utilizes palmprint and palm-vein features with Gabor filtering	- minimize the risk of voting violations. - Protect voter information from potential fraud.	- small datasets - The lack of real-world sensor-based testing - concerns in facing a centralized attack, data breach and single point of failure	-
[55] 2020	fingerprint biometric technology	authenticate voters	- Performed on small scall election. - The system may be vulnerable to spoofing attack. - the Gabor filtering and Fuzzy schemes not be implemented in a manner for real-time processing.	PLP the GAR is 99.984% and PLV was 99.981%
[57] 2021	- individual identity code. - Time-expiring token. - The use of biometrics including iris and fingerprint data	Eliminate fraud and the possibility of voting more than once	- The lack of protective measures to maintain the integrity of the data. - Lose the taken in low connectivity regions.	Enrolment time is 5 seconds
[58] 2022	combining fingerprint and iris recognition	- enhance the efficiency of voter identification and verification. - simultaneously serving as a deterrent to electoral fraud and the potential disenfranchisement of voters	- insufficient exploration of data security, storage capacity, and redundancy measures associated with the use of MySQL - dual-factor authentication leads to High hardware costs and complex maintenance of systems	Iris response time for voter enrollment and verification is 15s and 20s, Fingerprint response time is 3s and 9s.
[59] 2022	- Convolutional Neural Networks (CNN) are employed for facial	enhancing the security and trustworthiness of online voting systems	- limited coverage of safeguards against fraudulent faces, such	accuracy is 99 %

	recognition - Blockchain technology - Blind signature mechanism		as photos, videos, and masks. - The corporation of the block chain and blind signature may leads to scalability and latency issues.	
[60] 2022	- Electronic voting machine - Fingerprint biometric - Envisioned prototype includes an LCD display, a ballot unit, and a control unit.	Address tampering, fraudulent voting, and security concerns	- Lack of real-world testing. - Gap in specifying critical security measures, including secure data transmission and encryption techniques.	time taken between successive vote is 60 seconds
[61] 2023	Machine learning and deep learning techniques to evaluate facial features	- Improving online voting security. - Ensuring eligibility, preventing multiple voting instances. - Preserving voter confidentiality. - Accurately tallying valid votes.	- Lacks a comprehensive examination of safeguards against counterfeit facial representations. - Data security is not taken into account - AI-powered facial recognition system may exhibit. algorithmic bias.	- accuracy up to 98%

Upon reviewing the study related to the biometric traits within voting system. Significant gabs should be taken with consideration including the lack of large-scale testing for making sure about the efficiency in the real-world election, depending on centralizes database for managing and storing the biometric data, constraints in preserving the voter's information integrity, high cost of dual biometric factors integration.

Based on the mentioned gabs the direction of the future studies could focus on depending on replace the centralized database with decentralized by employing the blockchain technology for avoiding the system vulnerability to attacks with take into the consideration the scalability issues. Furthermore, for the making the proposed system reliable and authentic the biometrical authentication procedure should be tested in large-scale elections as well as enhancing the robustness of biometric systems for more effective management so the issue like poor quality or aging not affecting the voter verification performance. Also securing the vote transmission and storing through integrating the encryption technique.

3.2 Electronic voting system based on Watermarking technology

In the context of exploring watermarking technology in voting system, this section highlighting various application of watermarking as a valuable tool to address the evolving challenges in ensuring trust and reliability in electronic voting processes.

The study[44] employs a biometric and wavelet-based image watermarking strategy, integrating a highly secure mechanism for embedding a voter's fingerprint into their YCgCb color picture. The approach yields a PSNR of up to 54.26 and a Normalized Correlation (NC) of 1, demonstrating exact fingerprint recovery. The study intends to offer a multilayer protected, internet-based voting system; nevertheless, a significant disadvantage is the absence of administrative considerations in the e-voting system, the fingerprint identification technique is not adaptable for deployment on mobile platforms and lack in the discussion of the processing power needed to work with high-resolution biometric data in real time.

The method introduced in [62] extending the principles of the Juels, Catalano, and Jakobsson (JCJ) scheme to maintain ballot integrity and specifically fortify the attribute of coercion resistance. Additionally, electronic watermarking is proposed to save computing processes and improve validity verification. The stated issue is the awareness of the mixnet used in the JCJ scheme struggles with the processing of ballots containing forged credentials, posing a threat to the system's overall integrity. Furthermore, the computing demands are intensified due to the reliance on mixnet technology.

In [63] The researchers improved the crypto-watermarking concept for protecting electronic voting by using Advanced

Encryption Standard (AES) cryptosystems. In this study, the Mean Square Error (MSE) is calculated to be 70.64. The major aim is to build a multi-layer security approach that protects votes during network transfers from unauthorized access and electronic surveillance. However, the highlighted constraint is the need for the development of measures to strengthen protection against Denial of Service (DoS) assaults and discussing the possible latency problems that may result from the use of AES cryptosystems in a real-time voting environment.

The research [45] employs a unimodal fingerprint biometrics approach and utilizes the Advanced Encryption Standard in conjunction with Wavelet-based Crypto-watermarking. This system addresses the issue of potential errors in authenticating voters and ensures the integrity and confidentiality of the votes stored on the server. While the paper touches on the concept of confidentiality, it does not extensively explore the associated data privacy concerns. It is of utmost importance to safeguard voter information and guarantee that the system maintains the anonymity of voters. Furthermore, The lack of discussion regarding the system's management of simultaneous user requests and delays in verifying voters' identities may impact its viability in situations of heavy demand.

The research [64] investigated cryptographic techniques and security measures, such as a distributed ElGamal cryptosystem, Decisional Diffie-Hellman-based pseudorandom function, keyed-hash message authentication code, non-interactive zero-knowledge proof, verifiable mixnet, digital signature, multifactor authentication, and zero-watermarking. The outcome, a secure and verifiable polling system (SeVEP), guarantees vote confidentiality, election integrity, and voter authentication with multifactor security, allowing multiple votes while preventing duplicates. Despite thorough evaluations for security and performance, SeVEP is limited by its complexity and resource demands, making it more suitable for smaller to medium-sized online polling scenarios rather than universally applicable as well as causing slower processing time due to the system complication.

In[65] The authors propose a blockchain-based electronic voting system utilizing watermarked QR codes for biometric voter identification integrity. Visual cryptography ensures secure score voting through homomorphic encryption, with non-interactive range proofs to verify data integrity and prevent repudiation. Despite addressing security needs for large-scale governance, the integrated approach may introduce complexity, posing implementation and maintenance challenges, particularly in regions with limited technical resources and the need for substantial computational power foe process the encryption and decryption techniques. Additionally, concerns about biometric data privacy, especially in terms of security and transmission, are not adequately addressed.

Table 4 provides a concise summary of studies on watermark technology in e-voting systems.

Table 4. watermark technology in e voting system

Ref/ Year	Method	Objective	Limitation	PSNR
[44] 2012	- Biometric fingerprint - Wavelet-based image watermarking strategy.	intends to offer a multilayer protected, internet-based voting system	- Absence of administrative considerations. - The fingerprint identification technique is not adaptable for deployment on mobile platforms. - lack in the discussion of the processing power needed to work with high-resolution biometric data in real time.	54.26
[62] 2015	- JCJ scheme. - Electronic watermarking.	- Maintain ballot integrity and specifically fortify the attribute of coercion	- The mixnet used in the JCJ scheme struggles with the processing of ballots containing forged	-

			resistance. - Save computing processes and improve validity verification.	credentials, posing a threat to the system's overall integrity. - computing demands.	
[63]	2015	crypto-watermarking concept by using AES cryptosystems	Build a multi-layer security approach that protects votes during network transfers from unauthorized access and electronic surveillance.	- The need for the development of measures to strengthen protection against DOS. - Possible latency results from the use of AES. -	70.64
[45] 2016		- unimodal fingerprint biometrics - Advanced Encryption Standard in conjunction with Wavelet-based Crypto-watermarking.	addresses the issue of potential errors in authenticating voters and ensures the integrity and confidentiality.	- The study does not extensively explore the associated data privacy concerns. - lack of discussion regarding the system's management of simultaneous user requests and delays in verifying voters' identities.	45.32
[64] 2019		- Distributed ElGamal cryptosystem. - a pseudorandom function relying on Decisional Diffie-Hellman - Keyed-hash message authentication code - Non-interactive zero-knowledge proof. - Verifiable mixnet, a digital signature method. - Multifactor authentication. - Zero-watermarking from a scientific standpoint	- Confidentiality - Maintain the integrity of elections. - Authenticate voters. - Allows for multiple voting while preventing duplicates.	- Suitable for small to medium-sized online polling scenarios. - slower processing time due to the complexity.	-
[65] 2023		- Watermarked QR codes - Homomorphic encryption	- Data integrity - Prevent repudiation. - Safeguard	- Not addressing the concerns about biometric data privacy.	-

	voter privacy while ensuring verifiability. - Addresses the security requirements for large-scale governance, - Emphasizing source authentication.	-	the need for substantial computational power foe process the encryption and decryption techniques.

While the watermarking techniques provides substantial progress in securing the voting process, several gaps need to be analyzed. Starting with the scalability issues within large-scale election needed for more optimization in addition to the need for advanced infrastructure technology for handling the watermarking process efficiently. Moreover, the lack of watermarking resilience against attacks in order to preserve the embedded data. As a result, the future work direction Heading to achieving high processing power for the watermark process in real time to overcome the scalability issues and preserving the accuracy as possible. preserving the voter privacy and ensuring the election integrity and make the watermarking technology robust against several types of attack for preserving the embedded data by incorporation robust encryption technique. Focusing on developing light weight watermarking to be implemented in the mobile platform consider as a direction with significant objective due to high reliance on the mobiles nowadays.

3.3 Electronic voting system based on Blockchain technology

The incorporation of blockchain technology into voting systems has sparked considerable interest due to its potential to improve transparency and security. This study of the literature investigates the influence of blockchain in the election processes.

In[50] the Voter data is securely stored on the proposed blockchain system by utilizing distributed ledger technology to assist in bringing security and transparency to the poll. Voter identification is verified and double-spending is avoided by using UID numbers like Aadhaar. The structure improves the system's validation and prevents unauthorized updates by using Proof of Work and Merkle Tree hashing. A drawback is that the system's dependency on multicore CPUs and high-speed networks about 1Gbps may compromise the system's usability for certain voters and depending on UID numbers like Aadhaar potentially compromise voter privacy. 90 second is the tame taken for per vote in a small network with four nodes.

This paper[51] presents an electronic voting system based on the Ethereum Blockchain. Through the implementation of a smart contract-powered decentralized voting application, the study showcases the effectiveness of blockchain technology. The solution guarantees dependability, security, adaptability, and real-time support for voting account, vote, and candidate information storage by leveraging Ethereum's network and decentralized database. But there's a catch: delay throughput problems might make large-scale adoption difficult and slow down Ethereum's ability to be widely used in electronic voting systems and not take in the consideration the improving the speed of the Ethereum network.

In[67] the research discusses reducing direct contact in elections by employing blockchain-based electronic voting to lessen the effects of COVID-19. The system makes use of multi-chain functions for data storage and integrity, robust cryptographic protocols, and a ballot for vote confirmation. however, the research does not fully outline the procedures used to confirm voters' identities in addition to a number of drawbacks associated with internet-based electronic voting. Furthermore, lack in discussion the integration of the multi-chain system within the system database. The system usability score (SUS) is 90 and the reliability score of 0.820.

In[52] The authors provide a secure and transparent E-voting system relying on Blockchain technology through IOT devices to identify and mitigate any risks posed by attackers at different stages. The suggested technique is tested against several security metrics, including message tampering, Denial of Service (DoS), Distributed Denial of Service (DDoS), and authentication latency. Notably, drawbacks of the system are the observed increase in authentication delay with an increased number of nodes also the system was not implemented using real-time data furthermore, the depending on IOT devices leads to Insufficient authentication and vulnerability to physical tampering.

In[68] The suggested method describes an online voting system that uses the Ethereum Blockchain and Voter ID connected to their Aadhar cards with face and fingerprint recognition to identify voters. With double verification and remote voting, it aims to replace conventional shortcomings with blockchain for security, accuracy, and transparency. The primary objectives are to reduce the possibility of vote manipulation, improve transparency, and mitigate physical presence difficulties. Increased biometric verification latency, longer processing times with more participants, and longer authentication delays are potential

challenges requiring for adjustment. In addition to the sensitive biometric data vulnerable to misuse due to the lack of security measure.

In[53] smart Contract-enabled Blockchain-Enhanced Electronic Voting improves efficiency and security. By using smart contracts and transparent transactions, blockchain-based e-voting ensures confidence while reducing costs and resource consumption. For increased security, the suggested MongoDB, ExpressJS, ReactJS, NodeJS (MERN) based web application incorporates enhanced authentication, such as face verification and One-Time Passcode Verification (OTP). The voting information is securely stored in a Blockchain ledger that is based on smart contracts. Nevertheless, scalability concerns restrict its usage to local elections, hence requiring meticulous planning of infrastructure and stability for bigger implementations. A research gab consider in the omission of the potential enhancements to the MERN stack in the context of large-scale elections and the vulnerability of OTPs to spoofing or interception.

Table 5 Summarizes previous studies on the utilization of blockchain technology in e-voting systems.

Table 5. blockchain technology in e voting system

Ref/ Year	Method	Objective	Limitation
[50] 2019	blockchain system utilizing distributed ledger technology	- Security - Transparency - Voter identification - system's validation and prevents unauthorized updates	- Not every voter has access to 1 Gbps networks. - Depending on UID numbers like Aadhaar potentially compromise voter privacy.
[51] 2020	- the Ethereum Blockchain - smart contract-powered decentralized voting application	- Dependability - Security - Adaptability - real-time support	- The speed of LaEthereum prevents it from being widely used. - Not take in the consideration the improving the speed of the Ethereum network.
[67] 2020	- Blockchain - Multi-chain functions - Cryptographic protocols	- Reducing direct contact in elections - Data storage - Integrity	- No authentication for the user identity - drawbacks associated with internet-based electronic voting - lack in discussion the integration of the multi-chain system within the system database.
[52] 2021	- Blockchain technology through IoT devices.	- evaluated against message tampering, DoS, DDoS, and authentication delay.	- Increase authentication delay with an increased number of nodes. - the system was not implemented using real-time data. - The depending on IOT devices leads to Insufficient authentication and vulnerability to physical tampering
[68] 2022	- Ethereum Blockchain - Voter ID linked with Aadhar card - Face and fingerprint recognition	- Security - Accuracy - Transparency - Reduce the possibility of vote manipulation - mitigate physical presence difficulties	- Increased biometric verification latency - Longer processing times with more participants - Longer authentication delays. - the sensitive biometric data vulnerable to misuse due to the lack of security measure.
[53] 2023	- Blockchain - Smart Contracts - MERN - OTP - face verification	- Efficiency - Security - Confidence - Reducing costs and resource consumption.	- limit its application to local elections - the omission of the potential enhancements to the MERN stack in the context of large-scale elections - The vulnerability of OTPs to spoofing or interception

The adoption of blockchain technologies has inherent limitations, which can be summarized in networks issues due to the increasing of the transaction numbers. Furthermore, the region with limited infrastructure considers the adoption of the blockchain as a complex endeavor. In addition to integrating the biometric verification within the blockchain may slowdown the voting process as reason of increasing the number of nodes. As a future work direction, the e-voting systems may focus on enhancing the scalability issues for managing the large-scale election. Maintaining the transparency through interacting the different blockchain interoperability. Furthermore, adopting advanced encryption method act ad promising direction in protecting the voter privacy and ensuring transparency and verifiability of the voting process.

Conclusion

In conclusion, this research delves into the intricate realms of biometric authentication, watermarking, and blockchain technologies, aiming to proactively address the multifaceted challenges inherent in the current electronic voting paradigm. The integration of biometric authentication serves as a pivotal component, amplifying the efficacy of user identity verification processes while concurrently acting as a formidable deterrent against unauthorized access. The overarching objective of watermarking technologies is to fortify data integrity, offering a multifaceted defense mechanism against unauthorized duplication and illicit modifications. The methodological design of watermarking is underscored by a meticulous consideration of critical factors such as security, robustness, and imperceptibility.

Furthermore, the incorporation of blockchain technology emerges as a transformative force, contributing substantively to the establishment of decentralized electronic voting nodes. the combination of each technology findings highlights the key challenges, including the data integrity, voter impersonation, vote tampering in addition to the issues related with the centralized systems. the outcomes of theses finding are important for guiding the development of secure, scalable and user-friendly e-voting systems. However, there are some notable gaps that would need to be taken up as future research like the scalability of these technologies or the security of biometric data or even the integration process with existing electoral processes. Although the review providing valuable insights, technically focused reviews may overlook recent developments or take into account socio-political challenges typical in this area. New research must be undertaken to fine-tune and adapt these technologies to current electoral demands.

Reference

[1] Y. Liu and Q. Zhao, ‘E-voting scheme using secret sharing and K-anonymity’, *World Wide Web*, vol. 22, no. 4, pp. 1657–1667, Jul. 2019, doi: 10.1007/s11280-018-0575-0.

[2] A. Olumide S., B. Olutayo K., and S. E. Adekunle, ‘A Review of Electronic Voting Systems: Strategy for a Novel’, *International Journal of Information Engineering and Electronic Business*, vol. 12, no. 1, pp. 19–29, Feb. 2020, doi: 10.5815/ijieeb.2020.01.03.

[3] A. Olumide S., B. Olutayo K., and S. E. Adekunle, ‘An Innovative Approach in Electronic Voting System Based on Fingerprint and Visual Semagram’, *International Journal of Information Engineering and Electronic Business*, vol. 13, no. 5, pp. 24–37, Oct. 2021, doi: 10.5815/ijieeb.2021.05.03.

[4] SCAD College of Engineering and Technology and Institute of Electrical and Electronics Engineers, *Proceedings of the International Conference on Trends in Electronics and Informatics (ICOEI 2019) : 23-25, April 2019*.

[5] S. S. Chaeikar, A. Jolfaei, N. Mohammad, and P. Ostovari, ‘Security Principles and Challenges in Electronic Voting’, in *Proceedings - IEEE International Enterprise Distributed Object Computing Workshop, EDOCW*, Institute of Electrical and Electronics Engineers Inc., 2021, pp. 38–45. doi: 10.1109/EDOCW52865.2021.00030.

[6] Institute of Electrical and Electronics Engineers, *Proceeding of 15th International Conference on Telecommunication Systems, Services, and Applications (TSSA) : 18-19 November 2021, Bandung, Indonesia.*

[7] S. Alwahaishi and J. Zdralek, ‘Biometric Authentication Security: An Overview’, in *Proceedings - 2020 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2020*, Institute of Electrical and Electronics Engineers Inc., Nov. 2020, pp. 87–91. doi: 10.1109/CCEM50674.2020.00027.

[8] Y. K. Lee and J. Jeong, ‘Securing biometric authentication system using blockchain’, *ICT Express*, vol. 7, no. 3, pp. 322–326, Sep. 2021, doi: 10.1016/j.icte.2021.08.003.

[9] R. Rezwan, H. Ahmed, M. R. N. Biplob, S. M. Shuvo, and Md. A. Rahman, 'Biometrically secured electronic voting machine', in *2017 IEEE Region 10 Humanitarian Technology Conference (R10-HTC)*, IEEE, Dec. 2017, pp. 510–512. doi: 10.1109/R10-HTC.2017.8289010.

[10] S. Dinesh Kumar, P. Vamsikrishna, A. Tyagi, D. Bommisetty, and H. B. Kandala, 'Theoretical analysis of voting systems', in *2016 International Conference on Communication and Electronics Systems (ICCES)*, IEEE, Oct. 2016, pp. 1–5. doi: 10.1109/CESYS.2016.7889932.

[11] B. M. Mouad H Ali and A. T. Gaikwad Babasaheb, 'Multimodal Biometrics Enhancement Recognition System based on Fusion of Fingerprint and PalmPrint: A Review', 2016.

[12] P. Singh, 'A Survey of Digital Watermarking Techniques, Applications and Attacks', *Certified International Journal of Engineering and Innovative Technology (IJEIT*, vol. 9001, no. 9, 2008, [Online]. Available: https://www.researchgate.net/publication/342344131

[13] S. Ajili, M. A. Hajjaji, and A. Mtibaa, 'Crypto-Watermarking Algorithm Using Weber's Law and AES: A View to Transfer Safe Medical Image', *Sci Program*, vol. 2021, pp. 1–22, Aug. 2021, doi: 10.1155/2021/5559191.

[14] S. A.-B. Salman, S. Al-Janabi, and A. M. Sagheer, 'A Review on E-Voting Based on Blockchain Models', *Iraqi Journal of Science*, pp. 1362–1375, Mar. 2022, doi: 10.24996/ijs.2022.63.3.38.

[15] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, 'E-Voting System Based on Blockchain Technology: A Survey', in *2021 International Conference on Information Technology, ICIT 2021 - Proceedings*, Institute of Electrical and Electronics Engineers Inc., Jul. 2021, pp. 200–205. doi: 10.1109/ICIT52682.2021.9491734.

[16] U. Jafar, M. J. A. Aziz, and Z. Shukur, 'Blockchain for Electronic Voting System—Review and Open Research Challenges', *Sensors*, vol. 21, no. 17, p. 5874, Aug. 2021, doi: 10.3390/s21175874.

[17] H. I. Abdulrazzaq and R. D. Al-Dabbagh, 'Biometric Identification System Based on Contactless Palm-Vein Using Residual Attention Network', *Iraqi Journal of Science*, pp. 1802–1810, Apr. 2022, doi: 10.24996/ijs.2022.63.4.37.

[18] M. Mudhafer Taher Al Mossawy and L. E. George, 'A digital signature system based on hand geometry - Survey', *Wasit Journal of Computer and Mathematics Science*, vol. 1, no. 1, pp. 1–14, Apr. 2022, doi: 10.31185/wjcm.Vol1.Iss1.18.

[19] Muntasser S. Falih, Fatima B. Ibrahim, and Mahmood K. Ibrahem, 'Network Authentication Protocol Based on Secure Biometric NIDN', *Iraqi Journal of Science*, pp. 232–239, Jan. 2021, doi: 10.24996/ijs.2021.SI.1.33.

[20] R. Ryu, S. Yeom, S.-H. Kim, and D. Herbert, 'Continuous Multimodal Biometric Authentication Schemes: A Systematic Review', *IEEE Access*, vol. 9, pp. 34541–34557, 2021, doi: 10.1109/ACCESS.2021.3061589.

[21] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, and C. Reich, 'Continuous and transparent multimodal authentication: reviewing the state of the art', *Cluster Comput*, vol. 19, no. 1, pp. 455–474, Mar. 2016, doi: 10.1007/s10586-015-0510-4.

[22] S. Hemalatha, 'A systematic review on Fingerprint based Biometric Authentication System', in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*, IEEE, Feb. 2020, pp. 1–4. doi: 10.1109/ic-ETITE47903.2020.342.

[23] M. M. Hoobi, 'Keystroke Dynamics Authentication based on Naïve Bayes Classifier باستخدام مصنف نيف بايز ميس محمد هوبي على ديناميكية ضغطة المفتاح استنادا مصادقة المستخدم', *Hoobi Iraqi Journal of Science*, vol. 56, no. 2A, pp. 1176–1184, 2015.

[24] S. Arora and M. P. S. Bhatia, 'Challenges and opportunities in biometric security: A survey', 2022, *Taylor and Francis Ltd.* doi: 10.1080/19393555.2021.1873464.

[25] S. A. Abdulrahman and B. Alhayani, 'A comprehensive survey on the biometric systems based on physiological and behavioural characteristics', *Mater Today Proc*, vol. 80, pp. 2642–2646, Jan. 2023, doi: 10.1016/j.matpr.2021.07.005.

[26] S. M. H. Osama A. Salman, 'User Authentication via Mouse Dynamics', *IRAQI JOURNAL OF SCIENCE*, vol. 59, no. 2B, May 2018, doi: 10.24996/ijs.2018.59.2B.18.

[27] Z. Rui and Z. Yan, 'A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification', 2019, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2018.2889996.

[28] K. Okokpujie, J. Abubakar, S. John, E. Noma-Osaghae, C. Ndujiuba, and I. Princess Okokpujie, 'A secured automated bimodal biometric electronic voting system', *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 10, no. 1, p. 1, Mar. 2021, doi: 10.11591/ijai.v10.i1.pp1-8.

[29] G. Revathy, K. Bhavana Raj, A. Kumar, S. Adibatti, P. Dahiya, and T. M. Latha, 'Investigation of E-voting system using face recognition using convolutional neural network (CNN)', *Theor Comput Sci*, vol. 925, pp. 61–67, Aug. 2022, doi: 10.1016/j.tcs.2022.05.005.

[30] M. Ahmad *et al.*, 'Security, usability, and biometric authentication scheme for electronic voting using multiple keys', *Int J Distrib Sens Netw*, vol. 16, no. 7, p. 155014772094402, Jul. 2020, doi: 10.1177/1550147720944025.

[31] S. Agarwal, A. Haider, A. Jamwal, P. Dev, and R. Chandel, 'Biometric Based Secured Remote Electronic Voting System', in *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, IEEE, Jul. 2020, pp. 1–5. doi: 10.1109/ICSSS49621.2020.9202212.

[32] L. E. G. Zainab J. Ahmed, 'Robust Watermarking for Video Using Mean Modulation Technique', *IRAQI JOURNAL OF SCIENCE*, vol. 58, no. 4C, Dec. 2017, doi: 10.24996/ijs.2017.58.4C.17.

[33] S. A. S. Hussien, T. A. S. Hussien, and M. A. Noori, 'A Proposed Algorithm for Encrypted Data Hiding in Video Stream Based on Frame Random Distribution', *Iraqi Journal of Science*, pp. 3243–3254, Sep. 2021, doi: 10.24996/ijs.2021.62.9.37.

[34] A. Fatahbeygi and F. Akhlaghian Tab, 'A highly robust and secure image watermarking based on classification and visual cryptography', *Journal of Information Security and Applications*, vol. 45, pp. 71–78, Apr. 2019, doi: 10.1016/j.jisa.2019.01.005.

[35] F. TareqAbdulateef, 'BLIND ROBUST WATERMARK BASED ON CHAOTIC MAP AND FREQUENCY TRANSFORM IN A COLORED IMAGE', *JOURNAL OF MECHANICS OF CONTINUA AND MATHEMATICAL SCIENCES*, vol. 15, no. 8, Aug. 2020, doi: 10.26782/jmcms.2020.08.00060.

[36] P. Garg and R. R. Kishore, 'Performance comparison of various watermarking techniques', *Multimed Tools Appl*, vol. 79, no. 35–36, pp. 25921–25967, Sep. 2020, doi: 10.1007/s11042-020-09262-1.

[37] Y. A. Hassan and A. M. S. Rahmah, 'An Overview of Robust Video Watermarking Techniques', *Iraqi Journal of Science*, pp. 4513–4524, Jul. 2023, doi: 10.24996/ijs.2023.64.7.38.

[38] X. Yu, C. Wang, and X. Zhou, 'A Survey on Robust Video Watermarking Algorithms for Copyright Protection', *Applied Sciences*, vol. 8, no. 10, p. 1891, Oct. 2018, doi: 10.3390/app8101891.

[39] L.-Y. Hsu and H.-T. Hu, 'Blind watermarking for color images using EMMQ based on QDFT', *Expert Syst Appl*, vol. 149, p. 113225, Jul. 2020, doi: 10.1016/j.eswa.2020.113225.

[40] Md. Asikuzzaman and M. R. Pickering, 'An Overview of Digital Video Watermarking', *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 28, no. 9, pp. 2131–2153, Sep. 2018, doi: 10.1109/TCSVT.2017.2712162.

[41] J. Wang, D. Wu, L. Li, J. Zhao, H. Wu, and Y. Tang, 'Robust periodic blind watermarking based on sub-block mapping and block encryption', *Expert Syst Appl*, vol. 224, p. 119981, Aug. 2023, doi: 10.1016/j.eswa.2023.119981.

[42] S. Ajili, M. A. Hajjaji, and A. Mtibaa, 'Combining watermarking and encryption algorithm for medical image safe transfer: method based on DCT', *International Journal of Signal and Imaging Systems Engineering*, vol. 9, no. 4/5, p. 242, 2016, doi: 10.1504/IJSISE.2016.078269.

[43] A. Ray and S. Roy, 'Recent trends in image watermarking techniques for copyright protection: a survey', Dec. 01, 2020, *Springer Science and Business Media Deutschland GmbH*. doi: 10.1007/s13735-020-00197-9.

[44] B. L. Gunjal and S. N. Mali, 'Secure E-voting system with biometric and wavelet based watermarking technique in YCgCb color space', in *IET International Conference on Information Science and Control Engineering 2012 (ICISCE 2012)*, Institution of Engineering and Technology, 2012, pp. 1.27-1.27. doi: 10.1049/cp.2012.2284.

[45] O. M. Olaniyi, T. A. Folorunso, A. Ahmed, and O. Joseph, 'Design of Secure Electronic Voting System Using Fingerprint Biometrics and CryptoWatermarking Approach', *International Journal of Information Engineering and Electronic Business*, vol. 8, no. 5, pp. 9–17, Sep. 2016, doi: 10.5815/ijieeb.2016.05.02.

[46] W. Gao, W. G. Hatcher, and W. Yu, 'A Survey of Blockchain: Techniques, Applications, and Challenges', in *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, IEEE, Jul. 2018, pp. 1–11. doi: 10.1109/ICCCN.2018.8487348.

[47] M. H. Madhi, A. M. Al-Bakry, and A. K. Farhan, 'Blockchain in Realistic Areas of Application and Difficulties Encountered: A Survey Study', *Iraqi Journal of Science*, pp. 5301–5321, Oct. 2023, doi: 10.24996/ijs.2023.64.10.36.

[48] A. A. Monrat, O. Schelén, and K. Andersson, 'A survey of blockchain from the perspectives of applications, challenges, and opportunities', 2019, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2019.2936094.

[49] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, 'Blockchain challenges and opportunities: a survey', *International Journal of Web and Grid Services*, vol. 14, no. 4, p. 352, 2018, doi: 10.1504/IJWGS.2018.095647.

[50] A. Pandey, M. Bhasi, and K. Chandrasekaran, 'VoteChain: A Blockchain Based E-Voting System', in *2019 Global Conference for Advancement in Technology (GCAT)*, IEEE, Oct. 2019, pp. 1–4. doi: 10.1109/GCAT47503.2019.8978295.

[51] A. M. Al-madani, A. T. Gaikwad, V. Mahale, and Z. A. T. Ahmed, 'Decentralized E-voting system based on Smart Contract by using Blockchain Technology', in *2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC)*, IEEE, Oct. 2020, pp. 176–180. doi: 10.1109/ICSIDEMPC49020.2020.9299581.

[52] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, 'On the Design and Implementation of a Blockchain Enabled E-Voting Application Within IoT-Oriented Smart Cities', *IEEE Access*, vol. 9, pp. 34165–34176, 2021, doi: 10.1109/ACCESS.2021.3061411.

[53] R. Kumar, L. Badwal, S. Avasthi, and A. Prakash, 'A Secure Decentralized E-Voting with Blockchain & Smart Contracts', in *2023 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, IEEE, Jan. 2023, pp. 419–424. doi: 10.1109/Confluence56041.2023.10048871.

[54] S. Chaudhary *et al.*, 'Blockchain-Based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach', *IEEE Access*, vol. 11, pp. 76537–76550, 2023, doi: 10.1109/ACCESS.2023.3297492.

[55] S. Agarwal, A. Haider, A. Jamwal, P. Dev, and R. Chandel, 'Biometric Based Secured Remote Electronic Voting System', in *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, IEEE, Jul. 2020, pp. 1–5. doi: 10.1109/ICSSS49621.2020.9202212.

[56] A. Meraoumia, H. Bendjenna, M. Amroune, and Y. Dris, 'Towards a Secure Online E-voting Protocol Based on Palmprint Features', in *2018 3rd International Conference on Pattern Analysis and Intelligent Systems (PAIS)*, IEEE, Oct. 2018, pp. 1–6. doi: 10.1109/PAIS.2018.8598520.

[57] K. Okokpujie, J. Abubakar, S. John, E. Noma-Osaghae, C. Ndujiuba, and I. Princess Okokpujie, 'A secured automated bimodal biometric electronic voting system', *IAES International Journal of Artificial Intelligence (IJ-AI)*, vol. 10, no. 1, p. 1, Mar. 2021, doi: 10.11591/ijai.v10.i1.pp1-8.

[58] B. U. Umar, O. M. Olaniyi, A. B. Olatunde, A. A. Isah, A. K. Haq, and I. T. Ajayi, 'A Bi-Factor Biometric Authentication System for Secure Electronic Voting System', in *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, IEEE, Apr. 2022, pp. 1–5. doi: 10.1109/NIGERCON54645.2022.9803174.

[59] G. Revathy, K. Bhavana Raj, A. Kumar, S. Adibatti, P. Dahiya, and T. M. Latha, 'Investigation of E-voting system using face recognition using convolutional neural network (CNN)', *Theor Comput Sci*, vol. 925, pp. 61–67, Aug. 2022, doi: 10.1016/j.tcs.2022.05.005.

[60] M. A. Zamir, D. A. Khan, and M. S. Umar, 'Secure Electronic Voting Machine using Biometric Authentication', in *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*, IEEE, Mar. 2022, pp. 511–516. doi: 10.23919/INDIACom54597.2022.9763202.

[61] M. Tamilselvi, B. Manimaran, and S. C. Inunganbi, 'Empirical Assessment of Artificial Intelligence Enabled Electronic Voting System Using Face Biometric Verification Strategy', in *2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, IEEE, Apr. 2023, pp. 1–7. doi: 10.1109/ICONSTEM56934.2023.10142923.

[62] Y. Souheib, D. Stephane, and R. Riadh, 'Watermarking in e-voting for large scale election', in *2012 International Conference on Multimedia Computing and Systems*, IEEE, May 2012, pp. 130–133. doi: 10.1109/ICMCS.2012.6320237.

[63] O. Mikail Olaniyi, O. Joseph, O. Mikail, T. Abiodun, I. Mohammed, and J. Oluwagbemiga, 'Performance Evaluation of an Enhanced Crypto-Watermarking Model for Secure Electronic Voting'. [Online]. Available: https://www.researchgate.net/publication/278205836

[64] A. Qureshi, D. Megías, and H. Rifa-Pous, 'SeVEP: Secure and Verifiable Electronic Polling System', *IEEE Access*, vol. 7, pp. 19266–19290, 2019, doi: 10.1109/ACCESS.2019.2897252.

[65] A. Agrawal, K. Sethi, and P. Bera, 'Blockchain-Based Cardinal E-Voting System Using Biometrics, Watermarked QR Code and Partial Homomorphic Encryption', 2023, pp. 411–436. doi: 10.1007/978-981-19-6414-5_23.

[67] M. Kamil, A. S. Bist, U. Rahardja, N. P. L. Santoso, and M. Iqbal, 'Covid-19: Implementation e-voting Blockchain Concept', *International Journal of Artificial Intelligence Research*, vol. 5, no. 1, Jan. 2021, doi: 10.29099/ijair.v5i1.173.

[68] T. M. Roopak and R. Sumathi, 'Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology', in *2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA)*, IEEE, Mar. 2020, pp. 71–75. doi: 10.1109/ICIMIA48430.2020.9074942.