Secure Electronic Voters' Data Enrolment and Management Scheme Using Cryptography, Steganography and Blockchain Technologies: A Proof-of-Concept

Precious Bamiyo Metiboba
Department of Computer Science
Confluence University of Science and Technology
Osara, Nigeria
metibobapb@custech.edu.ng

Boniface Kayode Alese
Department of Cyber Security
Federal University of Technology
Akure, Nigeria
bkalese@futa.edu.ng

Abraham Ayegba Alfa
Department of Computer Science
Confluence University of Science and Technology
Osara, Nigeria
alfaaa@custech.edu.ng

Arome Junior Gabriel
Department of Cyber Security
Federal University of Technology
Akure, Nigeria
ajgabriel@futa.edu.ng

Lateef Caleb Umoru
Department of Computer Science
Confluence University of Science and Technology
Osara, Nigeria
umorulc@custech.edu.ng

Olayemi Mikail Olaniyi
Department of Computer Science
National Open University of Nigeria
Abuja, Nigeria
omolaniyi@noun.edu.ng

***Abstract*—Electronic voting (e-voting) systems enable the use of Internet technology for the purpose of voting and polling without the need to physically visit polling booths. Several developing countries are adopting e-voting systems during electioneering processes. E-voting systems were introduced to overcome security concerns while providing flexibility, low cost, simplicity, integrity, and security. Existing e-voting systems have been deployed using steganography, combined with cryptography, or blockchain for voting processes. But the safety of voters and polling information is generally vulnerable due to advances in media inspection and regeneration technologies. This paper proposes a secure e-voters' data enrolment scheme based on steganography, cryptography, and blockchain. The proposed hybrid scheme preprocesses voters' textual information into ASCII format before embedding it in the LSB of their grayscale images. Thereafter, the cover image is encrypted with AES-128, and SHA-256 hashes are computed for integrity prior to secure transmission with Web3.storage Interplanetary File System (IPFS). The outcomes revealed that the proposed hybrid scheme achieved an MSE of 0.06185 and a PSNR of 80.4546 dB on average for the sampled voters' information/image. The average encryption and decryption times of 0.00435 ns and 0.0030753 ns were obtained, as well as the average embedding and extraction times of the message, which were 0.00502946 ns and 0.00571 ns for the voter's information. In terms of imperceptibility and security, it offers higher integrity of voters' information when compared with related models.**

Keywords— Steganography, E-Voting, Election, Cryptography, Security, Privacy, Voter Data

I. INTRODUCTION

Online voting is a trend that is gaining momentum in modern society. It has great potential to decrease organizational costs and increase voter turnout. It removes the need to print ballot papers or open polling stations, where voters can vote from anywhere there is an internet connection. Despite these benefits, online voting solutions are viewed with a great deal of caution because they pose new threats. A single vulnerability can lead to large-scale manipulation of the votes. An electronic system must be legal, accurate, secure, and simple when used for elections [1], [2].

Electoral integrity is essential not just for democratic nations but also for the state of the voter's trust and liability. Electronic voting technologies can boost voters' participation and confidence and also reignite interest in the voting system. The weaknesses of traditional, paper-based polling have increased people's confidence in adopting e-voting [3]. A recent study shows that the traditional voting process was not entirely hygienic, raising several questions about fairness, equality, and the people's will that were not adequately quantified or understood in the context of governance. Electronic voting increases election reliability when compared to manual polling [4], [5].

In contrast to the conventional voting method, it has enhanced both the efficiency and the integrity of the process. Because of its flexibility, simplicity, and lower cost than general elections, electronic voting is widely used for various decisions. Electronic voting protocols have a single controller that oversees the whole voting process. This method leads to erroneous selections due to the dishonesty of the central authority (the election commission), which is difficult to rectify using existing methods. The decentralized network can be used as a modern electronic voting technique to avoid reliance on a central authority [6].

The voting process plays an important role in any democracy, allowing citizens to vote freely and produce an acceptable result [7]. Unfortunately, history shows that elections can be manipulated, leading to unacceptable results. In many developing nations, the compromise of electoral processes has led to the destruction of both lives and property simply because the rules of the game were not adhered to. The current electoral system's irregularities may be reduced by computer technologies such as biometrics and blockchain. Steganography [8], [9], cryptography [10], and blockchain technology [11] are top choices for everyday automation security, including e-voting systems. While some nations are still debating the effectiveness of electronic voting systems, the use of such systems has been welcomed in several

countries, including the United States and Estonia. The paper's key contributions include:

- To develop a secure e-voting enrolment model based on cryptography, steganography and Blockchain techniques.
- To determine the effectiveness of the developed secure e-voting enrolment model using encryption and decryption times, PSNR, MSE and Payload size.

The arrangement of the paper is as follows: section 2 contains the related studies. Section 3 is the research methodology. The results and explanations are presented in section 4. The conclusion is available in section 5.

II. Related Studies

Abiodun et al. [7] developed an e-voting system composed of two-stages of authentication, the national identification number, and facial identification of voters. The central server system of Mongo DB was used to store voting transactions. The outcomes showed improved performance and capable of reducing voting irregularities. But, the operations and storage infrastructure of the system are flawed and susceptible to attacks.

Kathirvelu et al. [6] proposed a secure e-voting system for voters to cast ballot securely and conveniently at remote pooling booths. It uses face identification and fingerprint authentication for verifying voter information remotely. The voters cast ballot upon accessing the e-voting system client-side. The voting transactions are safeguarded by LDAPSasl/Kerberos protocol for confidentiality and integrity. The administrative-side tracks and manages the pooling and counting of votes. The performance evaluation showed speedup of 115200 baud rate and authentication accuracy of 95%. However, security of voters' data cannot be guaranteed in centralized architecture.

Nwogu et al. [12] proposed a three-layer security architecture composed of device authentication, user authentication, and network security. The authors leveraged on Kerberos protocol for authentication and AES for user and device recognition. The interconnectivity thrives on virtual private network, demilitarized zone, and public network to ward-off cyber-attacks. The system provided more integrity and authentication for voters and voting process with the use of fingerprints and voter's card. However, security concerns of the e-voting system persist at the cloud unit.

Metiboba et al. [13] developed a hybrid framework of cryptography, steganography and blockchain in protecting e-voting systems in Nigeria. The authors suggested AES-128 algorithm, LSB and distributed ledger technology for registering and validating voters during election process. The theoretical analysis revealed the potential of the hybrid framework known as Crystography is capable of improving the confidentiality and integrity of voters' registration in e-voting systems. However, there is the need to experiment the findings and measure the performances such as timing and security parameters.

Hassan et al. [14] identified the potential of e-voting as a service in elections especially election collation through distributed ledgers. This lowers election-related expenses and enhance security. However, the number of nodes in the blockchain network increases adding to scalability problems. There were no practical implementations of the concepts.

Verma [15] provided a framework for electronic voting with security, privacy, and dependability features. A key is produced in their system at the time of registration. following which a hash is produced. The number of votes cast in favor of each candidate block on the blockchain increases with each one. The constructed blockchain is managed by a central database that is stored on the cloud. During voter registration, the registrant's fingerprint information is hashed. At the start of every blockchain, the hash is retained. The fingerprint was not a big factor in the voting process in their method.

A Hyper Ledger Fabric blockchain-based electronic voting system for the Jordanian election was built by [16]. The front-end, and client-side system were used to cast votes. The backend interacted with voter and candidate requests through SDK server notification. Smart contracts are used to create transactions, and the blockchain stores the transactions. The operations of the various units are unified by the consensus algorithm. But, registration of voters' information was not covered.

Razu et al. [17] presented a blockchain e-voting simulation consisting mostly of two parts: block and chain. Voters can select a ballot containing a voter's ID signed with a private key. The public key must be added to the settings. Public key comes first after then, the ballot and signature are confirmed. The ballot is sealed (mined). One block contains the ballot as transaction. Voters use a private key to cast their ballots and produce a signature to sign and seal votes in the e-voting system. However, the system is unsupportive of multiple users cast their votes at the same time, which will be linked to the previous hash. Also, the longest chain rule is vulnerable because the device can be used to cast votes.

Oladotun et al. [18] implemented a hybrid security method based on a hybrid Rivest-Sharma-Adleman (RSA), and Advance Encryption Standard (AES) algorithm for securing ballot information in an e-voting system. To avoid the concerns of privacy, integrity, and verifiability that many e-voting systems have, the electronic ballots cast were encrypted using the hybrid encryption method. To improve the integrity, the encrypted ballots were buried with the LSB replacement procedure. The stego image obtained from the security scheme created and the picture quality of the cover image used Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), and Correlation were used to quantify the results.

Lai et al. [19] suggested a decentralized anonymous transparent voting system with a low level of participant confidence. The voting system was to be used for large scale electronic elections. They used the Ring Signature and PoW consensus, which is a form of cryptographic zero knowledge. It is suitable for small scale platforms. The ring signature keeps the privacy of the individual voters but it was hard to manage and coordinate several signer entities. Quite expensive, not strong enough to secure from DoS attacks because there was no third-party authority on the scheme responsible for auditing the vote.

Shahzad and Crowcroft [1] developed a process model to describe the entire system structure and proposed the BSJC proof of completion as a trustworthy electronic voting technique. It was aimed at solving anonymity, privacy and security issues in elections on a lesser scale. They utilized a process model to describe the overall structure of the system. It is suitable for smaller scale platform and also attempted to

address security problems in elections. The proof of labor is a huge and difficult mathematical task that takes a lot of time and effort to complete. The polling procedure may be delayed if the block is generated and sealed on a big scale. Another issue is involving a third party because there is a potential of data tampering, leaking and this could affect end-to-end verification.

Gao et al. [20] investigated a blockchain based anti-quantum electronic voting mechanism with audit functionality was proposed. They have also tweaked the code based Niederreiter algorithm to make it more resilient to quantum attacks. The system was designed not just to recognize the voter's anonymity but also facilitates the audit's functioning. Authors utilized the Key Generation Center, certificateless cryptosystem, that serves as a regulator. It facilitated the audit's functioning made modification to the algorithm to make it more resistant to quantum assaults. When the number is high, some of the efficiency is reduced to provide better security. However, when the number of votes is modest, the security and efficiency benefits are substantial for a small-scale election.

Lee et al. [21] developed an e-voting card voting system for Estonia election through the Internet known as the national electronic ID card built-in circuit, and a 2048-bit PIN chipset. The card generates signatures using SHA1/SHA2. The voting application must be downloaded, authenticated, and voted on by the voters. The vote data was encrypted using election-specific asymmetric cryptography and signed with a secret key only accessible to the recipient. The generated and cast ballot were sent to the central storage server. The main flaws include voting system unprotected against state-level attackers, unrestricted access to network traffic, large data storage, and low analysis capability.

Alhasnawi and Alkhalid [22] leverages on biometrics, cryptography, and steganography for developing a secure online voting system. The Particle Swarm Optimization algorithm extracts fingerprint features. And, ECC scrambles the retrieved features into a unique voter's personal identification number and candidate number. Finally, the authors used multiple chaotic logistic maps to generate a random hiding location, and the Least Significant Bit approach was used to hide the encrypted voter's information within a cover image, resulting in a stego-image that was transmitted over an insecure channel.

Lauretha et al. [23] addressed difficulties in the voting process using a novel, secure steganography scheme within an end-to-end verifiable online voting system. It uses a password hashing-based scheme and a threshold decryption procedure. The system supports the verification process with a bulletin board implementation, which is a secure append-only broadcast medium to enable encoded voters' data generation after the voting process. However, the system is susceptible to distributed denial-of-service (DDoS) attacks and server overloading in real-world situations.

Olaniyi et al. [24] implemented a stegano-cryptographic model for safe electronic voting systems in poll-site, web, and mobile voting scenarios. Elliptic Curve Cryptography and RSA encrypt the electronic ballot. Using the modified LSB-Wavelet steganographic algorithm, the encrypted voters' ballots were randomly hidden into the LSB of the cover media. The model's large-scale implementation would be beneficial in delivering high-quality e-voting by registering the unique physiological biometric fingerprint and personal data of voters prior to balloting. But, effectiveness of the model could be impacted with its decentralized operations.

III. Research Methodology

This section presents the proposed scheme, the hybrid e-voting scheme for enrolment of the voters, mathematical problem definition, system requirements and evaluation parameters.

A. Description of the Proposed Scheme

This paper proposes a hybrid scheme for a secured electronic voting system in developing economies where less-emphasis is placed on conducting transparent, fair and trusted elections. The keys assumptions guiding the research include:

- Point of data generation during registration of voter is susceptible to threats.
- Point of data storage on cloud for voters is highly susceptible to threats.

Therefore, the paper provides proof-of-work for an end-to-end hybrid security scheme for voter data registration and warehousing first conceived by [13]. At the registration point, the method to be used cryptography and steganography to secure voter's data from passive attacks. At the storage point, the method to be used is blockchain, the voter's data are packed into blocks and signed cryptographically as illustrated in Fig. 1.

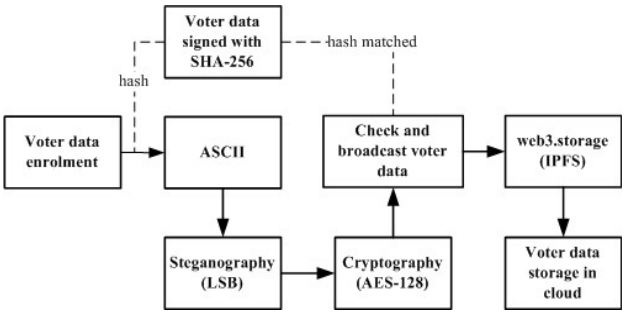

Fig. 1. Conceptual layout of the proposed scheme.

In Fig. 1, the description of the distinct blocks and operations in the proposed hybrid voter's enrolment scheme are stated as follows:

Voter Enrolment: The voters' attributes are collected securely, including: voter's polling unit, state of origin, blood group, age, marital status, sex, residential address. The Voter's Identification Number (VIN) is generated and linked to successfully enrolled persons. Thereafter, the voter data is scrambled before being concealed in the LSB portion of the passport photograph using cryptography and steganography. This unit is essentially composed of cryptography and steganography. It is the frontend that is used for capturing of data related to voters before onward transmission to the cloud.

Voter Authentication: It is the backend unit composed mainly of the blockchain that provides security for voters' information in storage. The voter information is accessed through appropriate authorization and authentication methods as shown in Fig. 2.

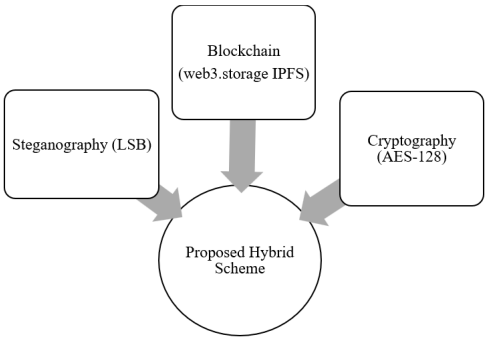

Fig. 2. Proposed voter data enrolment scheme.

The complete physical design of the proposed e-voting enrolment system is composed of voter terminal, wireless links, electoral official, DLT servers as shown in Fig. 3.

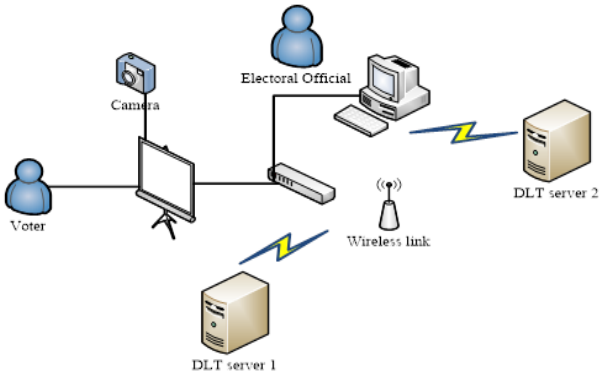

Fig. 3. The physical design of the proposed e-voting enrolment system.

B. *Problem Definition*

The proposed secure e-voting system is composed of the first component, which is the input that receive the various information concerning as represented by Algorithm 1.

Algorithm 1. Secure hybrid scheme for voter's data enrolment.

Input: **Output**:	Voter's data Voter's data packed into block on blockchain
1.	**Collect** voter's information is composed of different unique characteristics including names, date of birth, address, phone number and photograph.
2.	**Convert** the voter's data including detailed and spatial information.
3.	**Apply hashing algorithm** to sign and increase voter data integrity during broadcast and temporary storage points.
4.	**Encrypt** and **conceal** voter data into the vertexes of cover image (passport photography of voter). Voter information **scrambled** with ASCII algorithm are the LSB locations on the cover image vertices and obtain the stego image.
5.	**Broadcast** the voter information by verifying the associated message digest or fingerprint is given by **step 3.**
6.	**Store and authenticate access** to voter data encoded within stego image is retransmitted to the DLT for warehousing and further security.
7.	**Return** Content identity number of voter enrolment data.

The system flowchart for conducting the proof-of-work of the proposed e-voting registration system is illustrated in Fig. 4.

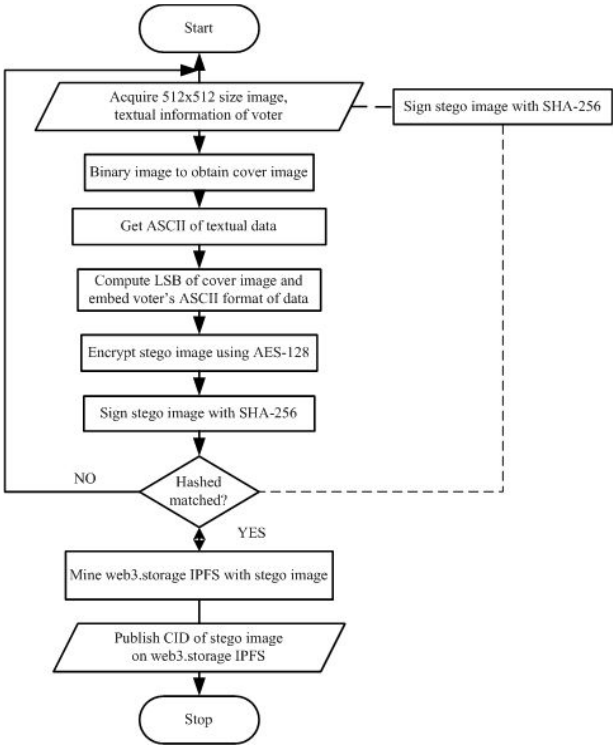

Fig. 4. The flowchart of the proposed hybrid scheme implementation.

C. *System Requirements*

The technical details, specifications and functional requirements of the hardware and software used are stated as follows:

The hardware components used in the development of the system include: A Computer System, 4.0GHz processor, Intel CORE i7, 16.00 GB RAM, and 1 Terabyte hard disk size.

The software tools required for the implementation of the proposed hybrid scheme include: MATLAB R2023a, Microsoft Window 11 home single language, 64-bit operating system, web3.storag, IPFS, Node.JS, and JavaScript.

The components, technique and security parameters of the proposed e-voting registration system are presented in Table 1.

TABLE I. THE TECHNIQUES AND SECURITY PARAMETERS

Component	Technique	Security parameters
Cryptography	Advanced Encryption Standard (AES-128)/ Secure Hashing Algorithm (SHA-256)	Encryption time, payload size, decryption time/ integrity of data (signing).
Steganography	Least Significant Bits (LSB) in the spatial domain.	Payload size, Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR).
Blockchain	Web3.storage based Interplanetary File System (IPFS) Distributed Storage	Token key size, content identification number, image size.

D. *Evaluation Parameters*

Cryptography: This uses AES-128 for encrypting data in a single block instead of individual bits of data. SHA-256 generate hash for signing data into a fixed length and one-way

encryption mode which is difficult to reverse and support secure the communication. Encryption is faster thereby making it ideal for applications, firmware and hardware that requires low latency and high throughput. It also supports the largest bit size and is practically unbreakable by brute force based on current computing power. The following parameters were adopted for measure the effectiveness:

Encryption Time: This is the duration it takes to convert plaintext (unencrypted data) into ciphertext (encrypted data). This process typically involves applying a cryptographic algorithm such as AES-128. The encryption time depends on factors such as the size of the plaintext, the encryption algorithm, the key size and the computational capabilities of the system or device performing the encryption. Low encryption time is expected in this study.

Throughput: This measure the throughput of any process of encryption in which the total encrypted plaintext (in bytes) is divided by the encryption time. In this study, the voter's details hidden in images were encrypted prior their embedding into the blockchain technology, higher throughput is expected.

Decryption Time: This is the time needed to convert ciphertext back into plain text, effectively reversing the encryption process. This involves applying corresponding decryption algorithms and key(s) to the ciphertext. The decryption time is influenced by factors similar to those affecting encryption time, such as ciphertext size, the decryption algorithm used, the key size and the computational resources available.

Ciphertext size: Longer key sizes may increase the time required for both encryption and decryption due to the increased complexity of the algorithms.

Steganography: The LSB steganography technique hides information within other data in a way that is not easily detectable. In this way, each pixel or byte in an image or file is modified to encode the hidden data, which is image steganography. It is expected such a pixel or byte does not introduce changes to the visual appearance of the image. The security parameters were tested as follows:

MSE: It stands for Mean Squared Error, and commonly used metric to measure the quality of a steganographic algorithm. The MSE is calculated by taking the average of the squared differences between the original cover image and the stego-image. If MSE value gotten is lower, the quality of the image will be better, so the image looks like the original image as given by Equation 1.

$$MSE = \sum_{M,N} \frac{[I_1(m,n) - I_2(m,n)]^2}{M * N} \qquad 1$$

where, $M * N$ are the dimension of the images, I_1 is the stego image of dimension, m, n, and I_2 is the original image of dimension, m, n.

PSNR: It is Peak Signal-to-Noise Ratio, and commonly used metric in image processing and steganography to assess the quality of a stego image compared to the original cover image. It is measured in decibels (dB) and provides a numerical value that indicates the quality of the stego image.

Ideal PSNR values tend to be around 30 dB or higher for good-quality grayscale and RGB images, with RGB often showing slightly higher PSNR due to colour channel averaging effects (Bharti et al., 2024; Abed & Al-Khafaji, 2024; Cao & Liu, 2024; Astawa et al., 2018) [26], [27], [28], [29]. However, the exact ideal value depends on the specific task and noise conditions.

Higher PSNR values imply a higher fidelity and similarity between the cover and stego images, meaning that the steganography algorithm preserved the cover image with minimal distortion or noise as given by Equation 2.

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right) \qquad 2$$

IV. Results And Discussion

This section describes the implementation of the proposed hybrid e-voting enrolment scheme, the evaluation and discussion of results obtained from the experimentation, and comparisons with existing studies.

A. Steganography Procedure Outcomes

The effectiveness of the voters' information embedding to the different cover images in terms of image size, MSE and PSNR are presented in Table 2.

TABLE II. Voter's Data Hidden in 512x512 Cover Image

Secret Message (Text)	Message size (byte)	Image Size (kb)	MSE	PSNR (dB)
Precious Metiboba,Female,18-26,205168166,54968461,Student	57	51340	0.00082397	78.9717
Metiboba Victor,male,27-35,7031297740,Employed	46	51340	0.00075912	79.3277
Saviour,male,27-35,07064335750,Entrepreneur	43	51340	0.00072479	79.5287
Adebayo Ayoola,male,27-35,08102376992,Entrepreneur	51	51340	0.00079346	79.1356
Michael Richard,male,27-35,09138317990,Employed	47	51340	0.00070953	79.6211
Adeyemi Deborah,Female,27-35,08138624318,,Student	49	51340	0.00075531	79.3496
Marvellous,Female,27-35,08102928160,Entrepreneur	48	51340	0.00072098	79.5516
Blessing Onoja,Female,27-35,08125171521,Student	47	51340	0.00074768	79.3936
Victor Moses,male,27-35,7039334219,Employed	43	51340	0.00065994	79.9357
Lawal Paul,male,18-26,08136704128,Student	41	51340	0.00059509	80.385

From Table 2, the cover images were converted into grayscale to increase the imperceptibility of hidden voters' information. Prior to the embedding of the voters'

information, the textual make up were converted into ASCII binary codes to facilitate the LSB substitution method selected for the image steganography. The graphical representation of the various performances for the voters' information and cover image embedding capacity is presented in Fig. 5.

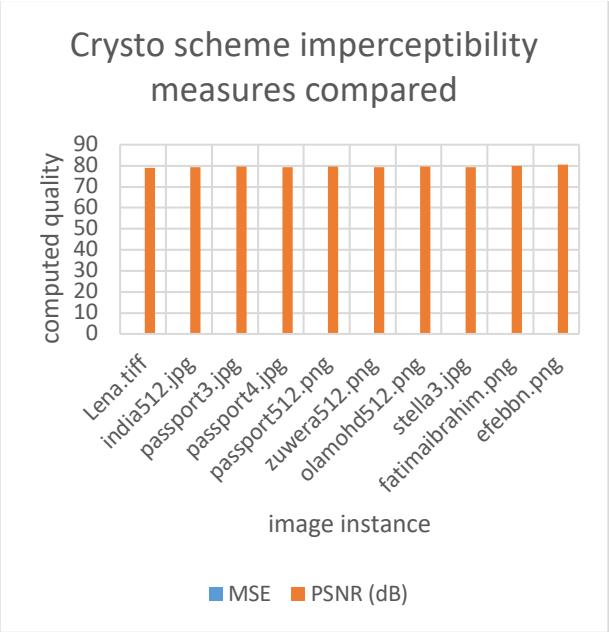

Fig. 5. The performance of the image steganography for voters' details compared

From Fig. 1, the MSE computed as 0.000595 for the grayscale version of the efebbn.png was the least and best performing, which is indicative of minimal distortions to the cover image after hiding the message (voter information) at the LSB positions. Similarly, the PSNR computed at 80.385 dB for the grayscale version of the efebbn.png was best against comparable cover images, which reveals that majority cover images after hiding voter information retain their quality and appearance to HVS. Notably, the performances of the different cover images used to embed voters' information showed considerably satisfactory MSE and PSNR because of little distortion, and high quality of the stego images generated.

B. Cryptography Procedure Outcomes

The relative effectiveness of applying cryptography, which is AES-128, on the various Stego images realized from embedding secret messages (voters' information) using measures such as encryption time, decryption time, MSE and PSNR are presented in Table 3.

TABLE III. OUTCOMES OF AES-128 ENCRYPTION/DECRYPTION PROCEDURES OF STEGO IMAGES COMPARED

Encryption Time (ns)	**Decryption Time (ns)**	**Embedding time (ns)**	**Extracting time (ns)**
0.0065087	0.005566	0.0044189	0.007826
0.0048879	0.0037919	0.0058548	0.0064652
0.0032728	0.002359	0.0038074	0.0067144
0.0043703	0.0038034	0.0066554	0.0040408
0.0022302	0.0016286	0.0042372	0.0051048
0.0060324	0.0025947	0.0043462	0.0083091
0.0043083	0.0027008	0.0050412	0.0049028
0.0048187	0.0026184	0.0057699	0.001031
0.003726	0.0031972	0.0061519	0.0057128
0.0033094	0.002493	0.0040117	0.0069808

From Table 3, the process of applying block cryptography increases the noise and rate of bits displacements in the stego image, which improve the security of the hidden media (voters' information). As expected, the values of the MSE are more than the values of the PSNR, which reveal scrambling stego image contents, and meaningless to the HVS. The best performing stego image: encryption time (13.59s) is sample 8; decryption time (13.01s) is sample 5; MSE (45.68) is sample 1; and PSNR (11.53 dB) is Sample 1 respectively. The graphical representation of the different performances of the stego images after applying AES-256 algorithm is depicted in Fig. 6.

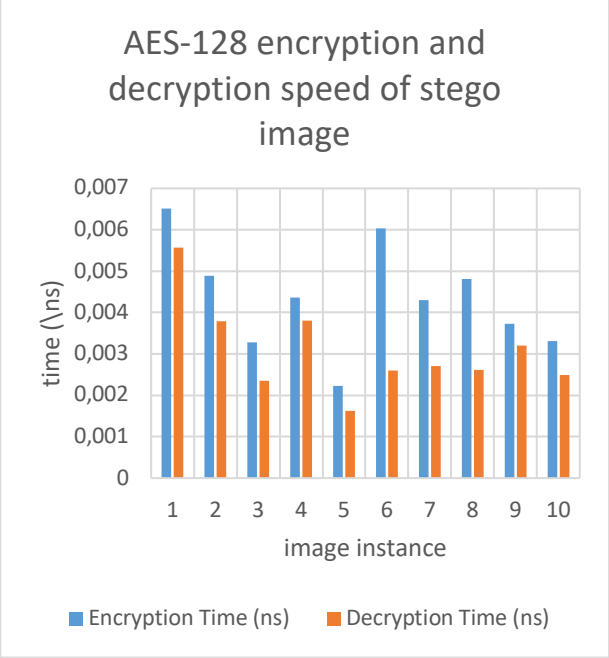

Fig. 6. The AES-128 encryption/decryption time based on stego images compared.

From Fig. 6, the graph shows considerable differences between the MSE values due to dissimilarities in the stego image contents. But there are relatively minimal differences between the encryption time, and decryption time as computed speedup of proposed Crystochain scheme across the various images experimented.

C. Proposed Hybrid Scheme Procedure Outcomes

This paper utilizes distributed blockchain storage (web3-storage IPFS) for integrity, confidentiality, distributed, secure, and immutability, which an improvement over the centralized storage. These are achieved with the following steps:

Step 1: Generate the web3.storage API token by signing up to https://web3.storage/tokens/ as shown in Fig. 7.

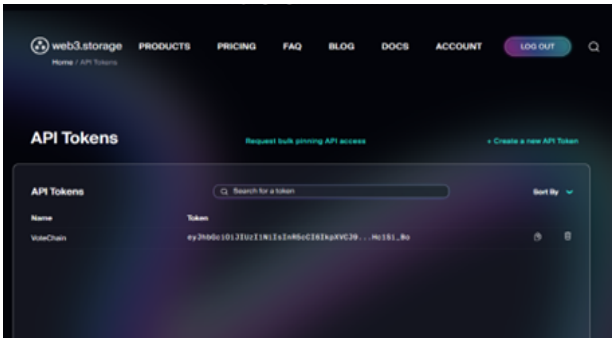

Fig. 7. The web3.storage API token generation interface.

From Fig. 7, the token name (VoteChain) from web3.storage to enable client side to communicate with the cloud storage provided by IPFS services as follows:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJkaWQ6ZXRocjoweDZDRTA2NDlhMDUzOTZBODMxOTkwMTQ5N0EwQWJFZDdhNTFGNmM4NzYiLCJpc3MiOiJ3ZWIzLXN0b3JhZ2UiLCJpYXQiOjE2ODY0MDQ4MTg0MTIsIm5hbWUiOiJWb3RlQ2hhaW4ifQ.U97ieNok23AEmikQ_8pfbk85JDd4yBfz1LCHc1Si_Bo

Step 2: The file upload interface is started at GITCMD command prompt by typing to start the server application, npm run dev. The interface for the GITCMD command prompt is shown in Fig 8.

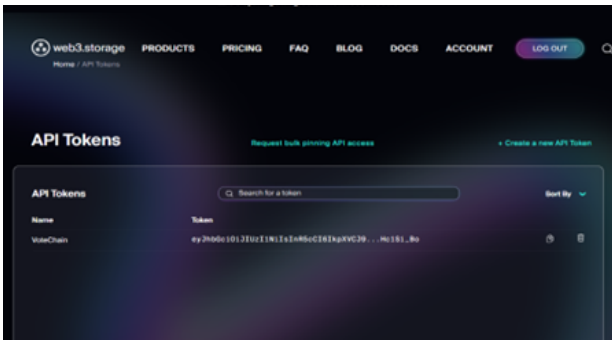

Fig. 8. The server application startup interface

From Fig. 8, the server connection address is displayed as when successful at http://localhost:3000/, which enables client to upload Stego image files generated from previous steganographic and cryptographic procedures.

Step 3: The web browser is open and the (http://localhost:3000/) is entered to open the file upload to the client node on the web3.storage using the API token for the Vote Chain as shown in Fig. 9.

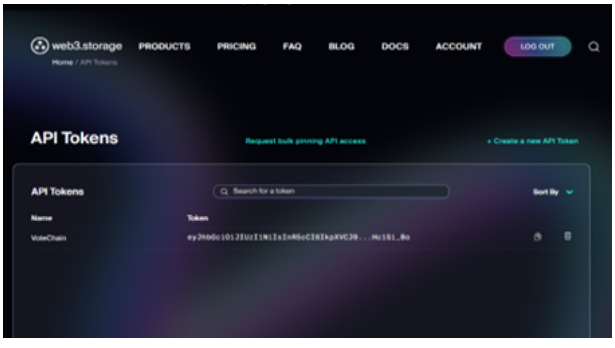

Fig. 9. The voters' data upload to web3.storage DLT node

In Fig. 9, the stego image files are uploaded to the storage node on the web3.storage based IPFS by clicking on the "choose a file to upload" text area. This enables the stego images to be broadcast to the distributed ledger technology for cloud storage and protection against manipulations, deletion, and modification. The access to the voters' data is achieved through the API token and the CID. The different stego images saved to the distributed cloud can be accessed through their CID shared by the client to third parties as follows:

https://dweb.link/ipfs/bafybeifh44tbo5wivq2xc4bu4lnicy5rlflztrqjjgdmpzhjl7fbq7dqye

The client node on web3.storage containing the various uploads for permanent storage is displayed in Fig. 10.

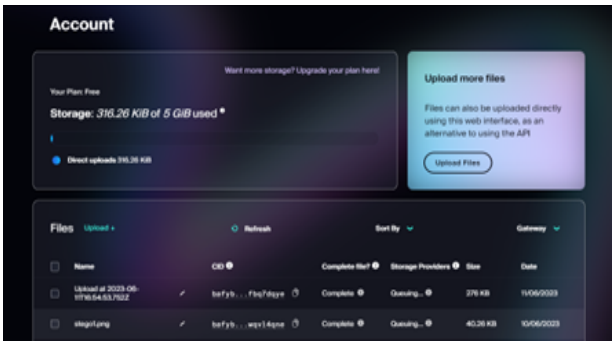

Fig. 10. The web3.storage DLT of voters' data upload to IPFS.

The results of embedding voters' data in photo of a 3-dimensional 512 x 512 colour image, which is converted to grayscale image format suitable for concealment. The original voters' image and stego image are illustrated Fig.11.

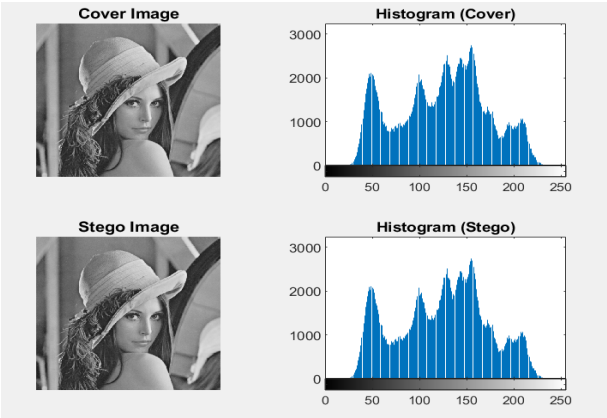

Fig. 11. Comparison of cover and stego images

From Fig. 11, the outlooks of both images are relatively the same to an onlooker's HVS, which the protects the secret messages embedded in the medium. The bits distributions of various images within the histogram spaces are used to explain the distortions and disparities in the images. The histograms of stego- and encrypted-stego images transmitted to the web3.storage IPFS platform are illustrated in Fig. 12.

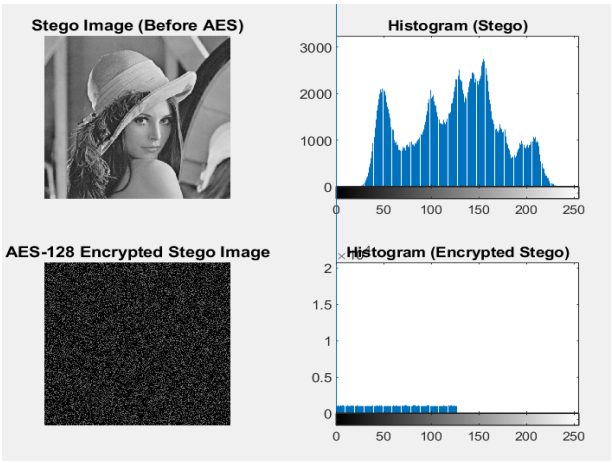

Fig. 12. The original voter's image and stego-image transmitted to web3.storage IPFS.

From Fig. 12, the histogram representations of the stego image, and encrypted-stego image transmitted to the blockchain, and cryptographically scramble to avoid attacks because of random arrangements and compositions of bits, which implies large noise properties. The encrypted stego image histogram distribution converted the varying pixels distributions to a marginal space of 1000 bits to scramble and deceive HVS attackers. This generates meaningless and totally senseless image representation of the stego media for high security of embedded voter's information. The encrypted-stego images are stored on the decentralized blockchain technology (that is, web3-storage IPFS) to protect the sensitive voters' data in cloud whose integrity and data access analysis are computed in Table 4.

TABLE IV. STEGO IMAGES DATA ACCESS AND INTEGRITY CHECK OF THE PROPOSED HYBRID SCHEME COMPARED

Recovered Image Sample	Embedding time (ns)	Extracting time (ns)	Integrity Check
1	0.0044189	0.007826	TRUE
2	0.0058548	0.0064652	TRUE
3	0.0038074	0.0067144	TRUE
4	0.0066554	0.0040408	TRUE
5	0.0042372	0.0051048	TRUE
6	0.0043462	0.0083091	TRUE
7	0.0050412	0.0049028	TRUE
8	0.0057699	0.001031	TRUE
9	0.0061519	0.0057128	TRUE
10	0.0040117	0.0069808	TRUE

From Table 4, the recovered image samples from the hybrid scheme procedure showed remarkable quality and low distortion rate. Image sample 2 obtained the best message embedding time of 0.0038074 ns. While image sample 8 achieved the finest message extracting time of 0.001031 ns. In particular, the embedding time, extracting time, and integrity check of the 10 stego-image samples experimented are illustrated in Fig. 13.

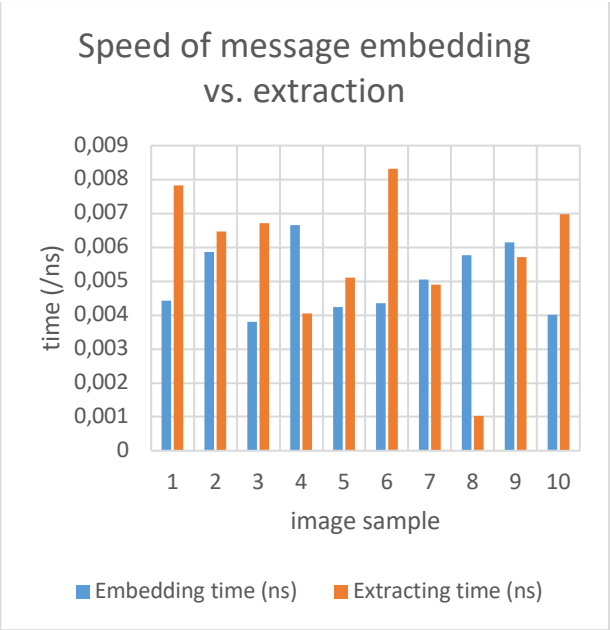

Fig. 13. The recovered voters' images bits distortion rate and quality measured.

From Fig. 13, the integrity of voter's information recovered from the AES-128 stego covers for the image samples stable because the SHA-256 digest of voter's data before and after recovery matched. Again, the voters' information embedding time outperformed the extracting time for samples 4, 7, 8 and 9. While the extraction time vs. embedding time was best image samples 1, 2, 3, 6, and 10. These are attributed to dissimilar message sizes (or voters' information sizes), and cover image characteristics of the experimented samples.

D. Performance Evaluation Outcomes Compared

The performance of the proposed scheme outcomes and comparable studies using security goal and countermeasure against confidentiality problems of voters' data are presented in Table 6.

TABLE V. QUALITATIVE COMPARISONS OF VOTER'S DATA HIDDEN IN 512Z512 COVER IMAGES

Criteria	[24]	[18]	[17]	[25]	This Paper
Security goal	Authentication, Confidentiality, integrity & vote auditing	Privacy, Integrity and Verifiability	Anonymity, Authentication, Accuracy and Verifiability	Transparency, Authentication	Confidentiality & integrity privacy
Confidentiality Counter measure	Steganographic approach: lifting wavelength Transform	RSA and AES	SHA-256	Visual cryptography	LSB, AES-128, SHA-256, and web3.storage IPFS

From Table 6, the performance of the proposed scheme offers high imperceptibility and security when compared to the existing schemes due to encryption of the voters' data embedded into photograph prior Web3.storage cloud storage.

V. CONCLUSION

The emergence of e-voting attempted to overcome the obvious challenges with the manual or paper-based polling approach. E-voting methods hold high potentials in minimizing organizational costs, raise turnout of voters, reduce use of ballot papers, and open polling booths where voters cast vote from anywhere using the Internet connectivity. E-voting have flaws, and vulnerable to new threats, a large scale of manipulations of the votes, less secure, and technological shortfalls. To deal with these challenges, this paper proposes a scheme that transforms voters' data into unreadable format then concealed into image prior transmission across vulnerable public channels. Thereafter, voters' data are stored and accessed using the web3.storage IPFS. This paper combined steganography, cryptography and blockchain to secure the most important component of the e-voting systems, voter enrolment, that seek to protect voter textual information through image LSB steganography. The stego images are encrypted using AES-128 and SHA-256 signed prior to their transmission to web3.storage-IPFS.

The outcomes revealed the average MSE and PSNR values were 0.000729 and 79.520 dB as obtained from the Crystochain scheme, which indicates high quality of stego images caused by low noise. Similarly, the average encryption time and decryption of 0.00435 ns and 0.0030753 ns were obtained. The average embedding time of message was 0.00502946 ns, and average extracting time of 0.00571 ns for mining the voter's information from the blockchain platform, which indicates the proposed scheme's speedup. The hashes of the voter's messages matched before and after transmission to the blockchain platform.

Hence, the voters' data enrolment, transmission, and storage across vulnerable public channels are more secure using the proposed Crystochain when compared to present-day voter registration procedure by the Electoral Umpires. The voter information is free from detection from central storage, tampering, manipulation, unauthorized access and view, low integrity, low confidentiality, and insecurity. Therefore, the voting process can be highly reliable and supportive of better electioneering process through online voting systems in developing nations. In the future work, the actual setup of the proposed scheme can be carried out to determine its effectiveness especially with higher payloads and real-time application constraints.

REFERENCES

[1] B. Shahzad, and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology." *IEEE Access*, vol., 7, no. 1, pp. 24477-24488, 2019.

[2] S. El-Kafhali, "Blockchain-based electronic voting system: significance and requirements." *Mathematical Problems in Engineering,* vol. 2024, no. 1, pp. 5591147, 2024.

[3] H. U. Khan, A. A. Christopher, and M. K. Alomari, "Role of e-voting system for void of errors in the electoral manipulations: a case study of Nigeria." *International Journal of Business Information Systems*, vol. 42, no. 2-3, pp. 478-502, 2023.

[4] Y. Liu, and Q. Wang, "An e-voting protocol based on blockchain." *Cryptology ePrint Archive*, 2017.

[5] B. Jayakumari, S. L. Sheeba, M. Eapen, J. Anbarasi, V. Ravi, A. Suganya, and J. Malathy, "E-voting system using cloud-based hybrid blockchain technology." *Journal of Safety Science and Resilience*, vol. 5, no. 1, pp. 102-109, 2024.

[6] M. Kathirvelu, S. Brintha, B. Darwin, K. Balaji, V. G. Dhivya, and S. M. Gnana, "Design and implementation of secured e-voting system." *2024 International Conference on Cognitive Robotics and Intelligent Systems*, IEEE, 2024.

[7] M. K. Abiodun, J. K. Adeniyi, A. E. Adeniyi, J. B. Awotunde, D. R. Aremu, O. Samuel, A. A. Adebiyi, and O. G. Atanda, "A web based biometric system for e-voting." In *2024 International Conference on Science, Engineering, and Business for Driving Sustainable Development Goals*, IEEE, 2024.

[8] A. A. Alfa, K. B. Ahmed, S. Misra, A. Adewumi, R. Ahuja, F. Ayeni, and R. Damasevicius, "A comparative study of methods for hiding large size audio file in smaller image carriers." In *Emerging Technologies in Computer Engineering: Microservices in Big Data Analytics: 2nd International Conf.*, 2019. Springer Singapore.

[9] A. A. Alfa, K. B. Ahmed, S. Misra, C. Dhawale, and R. Ahuja, "A CRT-LZW-based compression of multiple and large size images for clustered embedding in image cover. In *Proceedings of Soft Computing for Problem Solving*, 2021. Springer Singapore.

[10] A. A. Alfa, J. K. Alhassan, O. M. Olaniyi, and M. Olalere, "Enhanced hash value and public key infrastructure generations for blockchains using sooner lightweight cryptography." In S. Misra and T. A. Kumar. (eds) Blockchain Applications in the Smart Era. *EAI/Springer Innovations in Communication and Computing*, 2022. Cham, Springer International Publishing.

[11] O. M. Olaniyi, A. A. Alfa, and B. U. Umar, "Artificial intelligence for demystifying Blockchain technology challenges: a survey of recent advances." *Frontiers in Blockchain,* vol. 5*,* p. 927006, 2022.

[12] E. R. Nwogu, W. C. Ahiara, and P. M. Aondohemba, "Enhancing the robustness of a three-layer security electronic voting using Kerberos authentication." ABUAD Journal of Engineering Research and Development, vol. 6, no. 2, pp. 73-84, 2023.

[13] P. B. Metiboba, A. J. Gabriel, B. K. Alese, "Crystochain: towards securing electronic voting systems in Nigeria." *International Conference for Internet Technology and Secured Transactions*, 2022. London, UK.

[14] C. A. Hassan, M. Hammad, J. Iqbal, S. Hussain, S. S. Ullah, H. AlSalman, M. A. A. Mosleh, and M. Arif, "A liquid democracy enabled blockchain-based electronic voting system." *Scientific Programming*, vol. 2022, no. 1, p. 1383007, 2022.

[15] G. Verma "Secure framework for e-voting using blockchain." In *2022 2nd International Conf. on Computer Science, Engineering and Applications*, 2022. IEEE.

[16] S. Al-Maaitah, Q. Abdullah, and Q. Mohammed, "Blockchain-based E-Voting System for Election in Jordan." *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 5, pp. 1584–93, 2022.

[17] A. Razu, M. S. Javed, A. Asraf, M. Rajib, and K. Arifa, "The future of electronic voting using blockchain." *International Journal of Scientific and Technology Research,* vol. 9, no. 2, pp. 2277-8616, 2020.

[18] O. Oladotun, A. Okediran, A. Adeyemi, A. Sijuade, and B. W. Wajeed, "Secure electronic voting using a hybrid cryptosystem and steganography." *Journal of Advances in Mathematics and Computer Science*, vol. 34, no. 1, pp. 1-26, 2019.

[19] W. J. Lai, Y. C. Hsieh, C. W. Hsueh, and J. L. Wu, "Date: a decentralized, anonymous and transparent e-voting system." In *2018 1st IEEE International conference on Hot Information Centric Networking*, 2018. IEEE.

[20] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum e-voting protocol in blockchain with audit function." *IEEE Access*, vol. 7, pp. 115304-115316, 2019.

[21] J. Lee, J. Choi, J. Kim, and H. Oh, "SAVER: SNARK-friendly, additively-homomorphic, and verifiable encryption and decryption with rerandomization." *Cryptology ePrint Archive*, 2019.

[22] M. K. Alhasnawi, and A. S. Alkhalid, "Secure online voting using steganography and biometrics." *International Journal of Current Engineering and Technology*, vol. 7, no. 3, pp.1097-1104, 2017.

[23] R. Lauretha, I. Biju, and K. H. Mana, "Online voting system based on image steganography and visual cryptography." *Journal of Computing and Information Technology,* vol. 25, no. 1, pp. 47-61, 2017.

[24] O. M. Olaniyi, T. O. Arulogun, E. O. Omidiora, and O. O. Okediran, "Enhanced stegano-cryptographic model for secure electronic voting." *Journal of Information Engineering and Applications,* vol. 5, no. 4, pp. 1-15, 2015.

[25] S. Ashwini, and J. Santosh, "Secure e-voting system using visual cryptography and blockchain ledger." *Turkish Journal of Computer and Mathematics Education*, vol. 12, no. 1, 7-12, 2021.

[26] M. Bharti, S. Jain, and H. Jindal, Framework for Image Denoising Employing Different Thresholding Techniques. *International Journal of Sensors Wireless Comm. and Control*, vol. 14, no. 3, pp. 185-203, 2024.

[27] Z. H. Abed, and G. K. AL-Khafaji, Adaptive pixel-based technique for grayscale image compression. *Journal of Engineering*, vol. 30, no. 05, pp. 52-69, 2024.

[28] N. Cao, and Y. Liu, High-Noise Grayscale Image Denoising Using an Improved Median Filter for the Adaptive Selection of a Threshold. *Applied Sciences,* vol. 14, no. 2, pp. 636, 2024.

[29] I. Astawa, N. Saptarini, S. Asri, P. Sukarata, and I. Atmaja, Histogram Equalization and Gaussian Filtering Combination Method for Face Image optimization. In *2018 International Conference on Applied Science and Technology (iCAST)*, pp. 190-193, 2018. IEEE