Journal of Applied Engineering and Technological Science
Vol 6(2) 2025: 997-1018

SECURE E-VOTING SYSTEM UTILIZING FINGERPRINT AUTHENTICATION, AES-GCM ENCRYPTION AND HYBRID BLIND WATERMARKING

Asia Abdullah Ahmed[1], Nada Hussein M. Ali[2]
College of science, Department of Computer Science, University of Baghdad, Baghdad, Iraq[12]
asia.ahmed2201m@sc.uobaghdad.edu.iq[1], nada.husn@sc.uobaghdad. edu.iq[2]

Received: 01 October 2024, Revised: 13 January 2025, Accepted: 22 January 2025
*Corresponding Author

ABSTRACT
Ensuring security, integrity, and reliability of the election process consider as the main challenges in the electronic voting system. This paper describes the e-voting system by integrating the biometric authentication, advanced encryption, and watermarking techniques towards meeting such challenges. The system employs the fingerprint authentication by utilizing the Scale-Invariant Feature Transform (SIFT) for verifying the identity of the voter to ensure genuineness and non-repudiation of the service. The vote will be encrypted with the AES-GCM technique to be employed in securing the voting process, thus ensuring both data privacy and integrity. Hybrid Blind Watermarking employs the technique of Discrete Wavelet Transform (DWT) and Discrete Cosine Transform (DCT) for embedding the encrypted vote into the colored watermark cover image. Increased robustness against attacks with maintained vote confidentiality is achieved through this approach. The experimental results proved its imperceptibility to reach a Peak Signal-to-Noise Ratio (PSNR) of 40.7 and Normalized Correlation (NC) of 1. Thus, the proposed system enhances the theoretical foundation of secure e-voting and provides an implementation strategy for a reliable and tamper-proof voting system.
Keywords: *E-Voting, Fingerprint Authentication, Encryption, Blind Watermarking.*

1. Introduction

An election is a democratic procedure when the entire population choose a candidate to assume the leadership of the state. This concept entails switching from the traditional mode of voting, which is based on paper ballots, to voting by electronic means. It involves a number of challenges that are concerned with preventing attempts to manipulate the results of the voting and ensuring that the results are accurate. Starting with a paper-based voting procedure that has negative consequences such as multiple voting, result manipulation, and unprotected digital transmission, leading to in having issues with election integrity (Olumide S. et al., 2020) .

E-voting encompasses many methods and aims to optimize and enhance the precision of the voting, tallying, and counting processes compared to traditional approaches (Sarkar et al., 2020). The previously developed electronic voting was unable to technically address the identified issues of voter impersonation (authentication), confidentiality, integrity and secrecy (Olumide S. et al., 2020). The integration biometric technology such as the face recognition and fingerprint within the e-voting system had improve voting systems, the entire voting process and enhancing the privacy (L. Li et al., 2020) by identifying person based on their biometric traits to avoid multiple voting and impersonates (Okokpujie et al., 2021a) as well as the distinct advantages compared to other authentication methods in terms of being impossible to forget and difficult to be altered (Osama A. Salman, 2018). The standard biometrics system consists of several stages, which include enrollment, verification, identification, and matching (Hossain Faruk et al., 2024). The iris in was utilized in (Ali et al., 2023)as a secure method for the voter authentication process while in (Pasha & Jahankhani, 2024) the facial recognition is utilized to authenticate voters using algorithms such as the Haar Classifier to ensure accurate identity verification, transparency, and security in electronic voting, supported by robust database management and a secure network infrastructure.

Securing the vote after the voter being identified is a fundamental feature of any e-voting system. The encryption has undergone significant advancements in the past few years (Abdallah et al., 2022) due to its ability for converting the data to non-understandable form (Reyam Jassim Essa, 2018). The encryption incorporates key security measures to the e-voting such as

confidentiality, non-repudiation and the prevention of intermediary involvement by encrypting the voter's votes (Waheed et al., 2021) (B. O. Ahubele and Linda U. Oghenekaro, 2022). The modified ElGamal homomorphic encryption had been utilized in the secure e-voting system(Agrawal et al., 2023a) for encrypt the vote though ensuring the secrecy and enabling additive computations while the Homographic was employed for achieving balancing between efficiency and privacy as well as ensuring the voting system resistance against robust attacks(Zhan et al., 2024).

While the Watermarking concept was shown for protecting the sensitive data by embedding it into a multimedia file (Ghrare, Adim Mohamad Alamari and Emhemed, 2022) and protecting the copyrights (Mohammed et al., 2023). In the field of e-voting systems the watermark technologies adopted to ensuring the of data security by preventing unauthorized access or manipulation (Nakirya Brenda Kintu, 2018) (Agrawal et al., 2023b) in addition to enhance the security level though to the robustness to preserve the integrity verification(Han et al., 2016).

For achieving comprehensive security throughout the voting process, the proposed paper presents a secure electronic voting system that integrate the objective of fingerprint authentication for voter verification with the encryption and the watermarking techniques for securing the vote process. The voter authenticated with two authentication step including Six-digit passcode in addition to the fingerprint. SIFT algorithm was selected as the means for voter authentication. This strategy involves detecting and matching the key point of the stored and entered fingerprint image.

The consequent scenario about ensuring data integrity by perform vote encryption using the AES-GCM method. Lastly, to further enhance vote security, and achieve confidentiality the encrypted vote is embedded into a colored watermark cover image using blind hybrid DWT-DCT watermarking techniques. by convert the encrypted vote into binary representation then perform the embedding into binary watermark image and lastly embedding the watermark image into colorful image using DWT and DCT. Figure 1 presents the general framework procedure of the proposed system.

The primary contribution of the main system is:

- The development of a voter authentication system that utilizes fingerprint recognition and a unique 6-digit passcode.
- Implement a strong and reliable voting scenario by utilizing the encryption with blind watermarking technique with new imbedding procedure for ensure the robustness against attacks.
- Assess the system's performance by testing the voting results in the presence of several attacks.

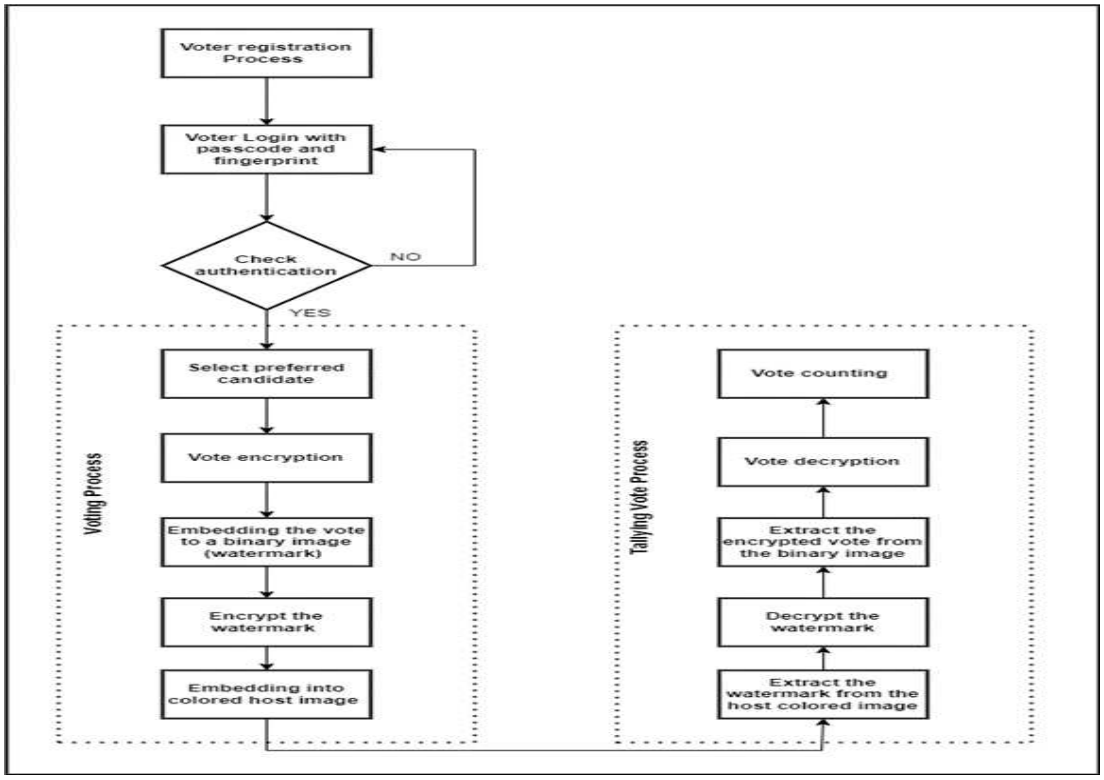

Fig. 1. The General Framework of The E-Voting Process

2. Literature Review

By analyzing the related work for both the e-voting systems and blind watermarking, the proposed work takes the advantage for integrates the voter authentication and vote securing that leveraging the encryption and the hybrid watermarking the integration for improving the system's robustness against various attacks, ensuring the reliability of vote storage and retrieval. These innovations collectively enhance the security, reliability, and scalability of e-voting systems, making them suitable for real-world applications.

2.1 E-voting systems

E-voting systems bring the future of a secure and trustworthy democracy concerned with voter authenticity and data integrity. Advanced techniques have been used the e-voting systems including voter verification and securing the votes during transmission and storing for covering challenges concerning about unauthorized access, vote confidentiality and integrity.

According to (Agarwal et al., 2020) the system aims to prevent booth capturing, fraudulent voting, and tampering in the voting process by utilizing Arduino microcontroller, fingerprint sensors, and a keypad interface, fingerprint technology to verify the identity of the voter. However, the system may not be accessible in regions with limited network connectivity furthermore lack of securing data mechanism during the transmission and storage.

In (Okokpujie et al., 2021b) the author suggested utilizing two distinct biometric traits (iris and fingerprint) using specialized sensors (Irishield-UART MO2120 and Digital Persona U&U 4500) to enhance the overall security and reliability of electoral procedures. However, the report does not sufficiently address the detection of data tampering inside the database and the dependency on centralized database could possess a potential bottleneck causing data tampering.

(Sherine et al., 2022) propose a three-step mobile e-voting security solution. Captcha, phone OTP, and fingerprint verification are security measures. The e-voting program has robust verification requirements, however there is not enough information about the communication protocol's encryption technology and the evaluation of the system performance with university student may pose large scale election issues.

(Tamilselvi et al., 2023) proposed an AI-driven facial detection and identification system for online voting uses machine learning and deep learning to evaluate facial traits. This study success in improving online voting security, eligibility, preventing repeated votes, voter confidentiality, and accurate vote tallying are the main goals. While the research lacks a complete analysis of measures against counterfeit face representations and focuses on MySQL's role in data administration, ignoring data security.

The study (Adeniyi et al., 2024) presents a blockchain-based e-voting system that integrates fingerprint biometrics. The voter fingerprints utilized to generate unique private and public cryptographic keys will help maintain voter anonymity and avoid any tampering. The use of blockchain's unchangeable ledger and smart contracts will create a clear place for vote casting and verification, solving the main problems that exist within these traditional systems of voting. 400 voters' testing showed good performance; further research is recommended to enhance the robustness, including hybrid encryption. The implementation of this system in a real-world scenario with a big population is still pending.

The use of encryption methods is seen as an effective means of securing data during transit. In a recent study(Rahman et al., 2024), the author proposes a blockchain and biometric verification integrated online voting system with special concern to secure data transmission through RSA encryption. The main objective is to use RSA encryption and digital signature as a robust technique in ensuring the security, privacy, and transparency of the election by implementing end-to-end confidentiality and authenticity of the votes. The positive side of RSA includes its wide acceptance and well-established mathematical background in securing communication. However, cryptographic weaknesses are established as inefficient due to the large size of keys, non-performing speed with modern algorithms like ECC, and susceptibility to quantum computing.

In the study referenced as (Jayakumari et al., 2024), the author suggested a system comprising the Key Generation Center (KGC), Election Commission Authority (ECA), IoT devices, Edge Server, Cloud Server, and Hybrid Blockchain Network. The purpose of this system is to improve the security, transparency, and reliability of the existing E-voting system. Despite the system's outstanding performance, users still require more time to adapt and be educated on a wide scale.

2.2 blind watermarking

Blind watermarking is plays a critical role in securing the communication; an idea we shall use throughout this series of articles. The proposed system employs a hybrid watermarking technique which incorporates advanced embedding methodologies for maintaining the imperceptibility as well as the robustness of information.

In (Tian et al., 2020) the author combined the Contourlet Transform (CT), Discrete Cosine Transform (DCT), and Singular Value Decomposition (SVD). For enhancing the robustness the low-frequency band is selected for the embedding after applying the CT to the host image. Perform the DCT on non-overlapping block for obtaining the D matrix coefficient. Lastly in the SVD the embedding procedure done by adjusting the largest value in SVD in the carrier matrix that obtained form preforming Zigzag on the D matrix. The reached PSNR of the study about 40.4.

The research in (X. Zhang et al., 2021) aims to create blind watermarking for protect the copy right in the 5G network environment by embedding the watermark into color watermark host employing the discrete Hartley transform (DHT) in the spatial domain. While the embedding capacity 0.0625 bits per pixel that suitable for many applications, probably not enough in situations that need large amount of watermarking data. The Achieved PSNR about 40 db.

While the research (Lee et al., 2021) propose to protect the copy right by scrambling the host image using Arnold transform map, then converting the scrambling image into YCbCr. for the watermark, encryption with private key performed and abending into the DCT coefficients of 8*8 non overlapping block within Y, Cb and Cr. lastly the embedding applied multiple times and perform voting mechanism during the extraction in order to improve the robustness. The

multiple embedding may degrade the robustness as a potential drawback. The reached PSNR about db37 to 45db

In (D. Liu et al., 2021) the authors propose a color image watermarking scheme in the frequency domain with Schur decomposition and quaternary coding for balancing visual imperceptibility and robustness against attacks as well as increasing watermark capacity. Though it has quite appreciable visual imperceptibility (the average PSNR is higher than 36 dB) and strong robustness (NC values are from 0.95 to 1.0) against attacks.

The authors in (Mohammed et al., 2023a)propose a self-adaptive scheme to choose either green or blue for more robustness. DCT-DWT determined for embedding the watermark. To increase the level of security the watermark image is encrypted using chaotic logistic map. regardless of robustness the watermark image not recognizable on rotation attack as the drawback of the proposed scheme.

The propose technique in (Mahagaonkar et al., 2023) combines DWT and SVD using Human Visual System (HVS) where the input image converted form RGB into HVS to apply the 2-level DWT to the v channel decomposing it into LL, LH, HL, and HH sub-bands. The SVD implemented on LH, HL and HH that divided into 4*4 blocks where the random binary sequence applied in the LH and the watermark logo embedded in HL and HH sub-bands by modifying singular values based on calculated means and an optimal threshold. Despite that selecting of the optimal threshold may leads to potential complexity. The PSNR of the proposed work about 30db to 37 db.

The proposed work in (Bao and Wang, 2024) is a robust blind color watermarking algorithm based on Radon and DCT transforms. Watermark bits are incorporated into the mid-frequency coefficients of the DCT of Radon transformed blocks of the U component in the YUV color space. Security is enhanced using the Arnold transform and random permutation, whereas geometric correction ensures robustness against attacks. The experimental results gave an average PSNR above 37 dB and NC=0.9769 on average for all attacked samples.

The method proposes in (Su et al., 2024) to introduce a fusion-domain blind color image a watermarking approach using Graph-Based Transform (GBT) to improve efficiency, robustness, and security. GBT coefficient computation is simplified in the spatial domain of GBT while using a simplified Chen chaotic encryption process and finally, adaptive embedding strength using Particle Swarm Optimization (PSO). The average PSNR is more than 40 dB while NC above 0.95.

3. Preliminaries

In this section the employed method in the proposed e- voting system will be viewed.

3.1 SIFT

SIFT is a feature extraction technique was presented by David G. Lowe(Lowe, 2004) that extract features that not effected by objects operation like scaling and rotation. The sift take the input image and convert it into large group of local feature vector known as key points(Alamri et al., 2022(. The SIFT devided into four steps (Rajab, 2023): (1) Scale-Space Extrema Detection: searching the scales in the image by using difference-of-Gaussian to identify potential key points that are rotation and scaling invariant. (2) Keypoint Localization: A detailed model is fitted for identifying the location and scale at each potential location. based on indicators of stability the key points are chosen. (3) Orientation Assignment: One or more local image gradient orientations are assigned to each key point location. All subsequent processes use image data transformed to account for feature orientation, scale, and location. (4) Keypoint Descriptors: Each key point location is assigned one or more orientations based on the local image gradient orientations.

3.2 AES-GCM

The AES is a symmetric block cipher algorithm(Yousif et al., 2024) that has key sizes of 128, 192, and 256 bits. The length of the key corresponds to the number of 32-bit words in the key. The AES considered as a symmetric key encryption algorithm(Harba et al., 2021).The National Institute of Standards and Technology (NIST) developed the incorporation of Galois

Counter Mode (GCM) is a cryptographic mode of operation and the Advanced Encryption Standard (AES)(Hussein et al., 2022). The AES-GCM has three main concepts: firstly, the authentication encryption that considered as a cryptographic method offering the confidentiality and authenticity. transforming of plaintext into ciphertext by incorporating a random sequence that is generated by encrypting an incrementing counter with AES. This ensures both encryption and authentication. And lastly the GHASH as a hash function within AES-GCM to generating authentication tag that ensures the data integrity(Takaki et al., 2020).

3.3 DCT

DCT is a technique used to convert the image from the spatial domain to the frequency domain where the DCT compress the image by transforming it into sum of frequencies and applying the quantization(Garg et al., 2022). DCT has been employed in numerous image processing technologies, including JPEG compression. The DCT of a N × N image f (i, j) can be defined by Eq.(1) (Z. Li et al., 2021).

$$C(u,v)=\alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)cos\left[\frac{((2x+1)u\pi)}{2N}\right] cos\left[\frac{((2y+1)u\pi)}{2N}\right] \quad (1)$$

Where C(u,v) is the DCT coefficient at the u, v position , $f(x, y)$ the input image at the position x, y , N is the size of the block and α(u)α(v) is the scaling factor .

3.4 DWT

DWT considered as a multi-resolution approach, used for transform the signal from the spatial domain into different levels of the time-frequency domain. It has a great energy compaction property, which is why it is used in image processing applications, such as image denoising and image compression (Mohammed et al., 2023b). The DWT decompose the image into four sub bands called LL, LH, HL, HH. In order to determine the coefficients of each sub-band, we can compute them using the Haar filter in the following manner in the Eq. (2) (3) (4) (5)(Fares et al., 2021):

$$LL(m,n)=\frac{p(m,n)+p(m,n+1)+p(m+1,n)+p(m+1,yn+1)}{2} \quad (2)$$

$$LH(m,n)=\frac{p(m,n)+p(m,n+1)+p(m+1,n)+p(m+1,yn+1)}{2} \quad (3)$$

$$HL(m,n)=\frac{p(m,n)+p(m,n+1)+p(m+1,n)+p(m+1,yn+1)}{2} \quad (4)$$

$$HL(m,n)=\frac{p(m,n)+p(m,n+1)+p(m+1,n)+p(m+1,yn+1)}{2} \quad (5)$$

2.5 Arnold cat`s map

The Arnolds cat's theory of map considers that transition in math that is random in the pixels of images. applying this transformation multiple times will lead to increase in the pixel scrambling, but after a specific number of iterations the original image will appear again. The Arnold transform is defined by the equation (6).

$$\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix}\begin{pmatrix}x_{n+1}\\y_{n+1}\end{pmatrix}=A\begin{pmatrix}x_n\\yn\end{pmatrix}(Mod\ N)=\begin{pmatrix}1 & a\\ b & ab+1\end{pmatrix}\begin{pmatrix}x_n\\yn\end{pmatrix}(Mod\ N) \quad (6)$$

Where N is the image size, a and b positive integer, $x_n \ and \ y_n$ is the pixel original position while x_{n+1} and y_{n+1} is the new position of the pixel (Pourjabbar Kari et al., 2021).

2.6 Logistic Map

The logistic map is one of the Most essential type of chaotic map(Saleh et al., 2022) and consider as a one-dimensional map that produces one value every iteration called an iterate. The logistic map employs a single parameter called r which is between 0 and 4, and the x_n iterate which is between 0 and 1. Equation (7) calculates the new value as follows:

$$\boldsymbol{x_{n+1}}= r\cdot \boldsymbol{x_n}\ (1-\boldsymbol{x_n}) \quad (7)$$

Where n ∈ {1,2,3…. N} and N referring to the total number of iterations. To achieve unpredictable chaotic behavior, the transient period that refer to the first 1000 iteration is discarded (Oravec, Ovsenik and Papaj, 2021).

4. Research Methods

The proposed system methodology contains several stages for completing reliable voting procedure.

4.1 Registration process

The first stage in the voting system is obtaining the voters information to be inserted within the system database. The voters information including voter name, age, workplace and phone number in addition core data Represented by the voter fingerprint and auto-generated unique pass-code to ensure firstly only eligible voters could vote and each voter vote once.

4.2 Authentication process

In authentication procedure the voter authenticated firstly by matching the six-digit passcode then matching the voter fingerprint relying on SOCOfing dataset that contain in image for 6000 African subjects. SIFT is the technique used to detect and extract the features form the stored and interred fingerprint. The technique used to detect key points and compute the descriptors. For matching process the SIFT algorithm employs the FLANN (Fast Library for Approximate Nearest Neighbours) matcher. The total number of good matches are compared with the static threshold with matching of the stored and entered passcode to decide either the voter authenticated or not and preparing for the voting process.

4.3 Voting process

In the proposed work the voting process including several steps:

Step 1: In Voting scenario the voter passcode with the candidate id will be concatenated into single string. Initializing AES within GCM mode to encrypt the string with the secret key and nonce.

Step 2: The obtained cipher text will be converted to binary string of 0`s and 1`s to be ready for the embedding to binary watermark of size 32*32. Next, the watermarked image will be scrambled with logistic map as shown in Figure 2.

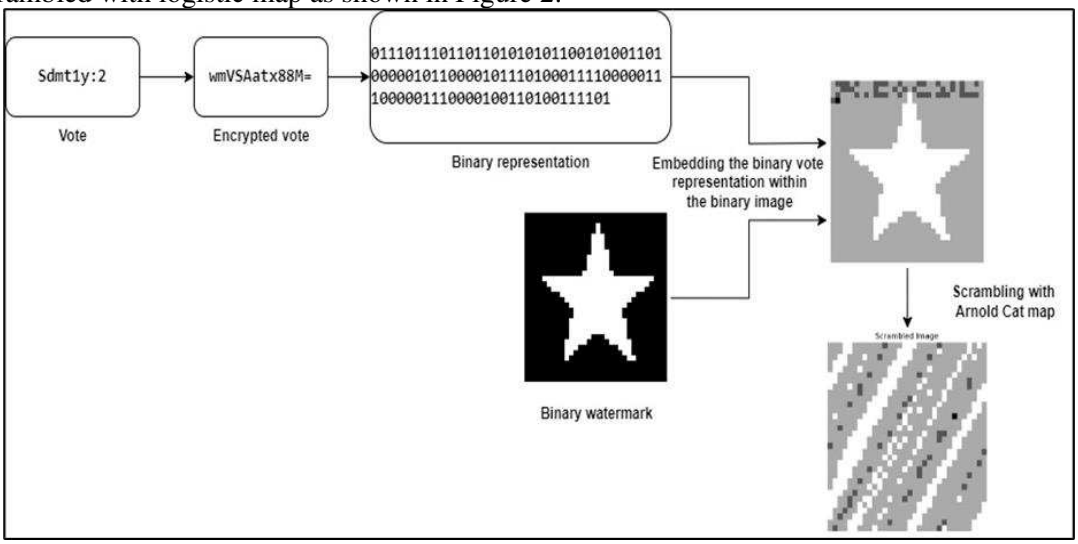

Fig. 2. The Watermark Preparing Process

Step 3: start embedding the watermark image into colored host image. Firstly, the colored image converted into YCbCr to embed the binary watermark in the Y component then apply the DWT to the extracted Y component using Haar wavelet transform for decomposing the image into the frequency bands.

Step 4: divide the HH frequency band into 4*4 non-overlapping sub-block then initialize a list of 4*4 matrices to embed the sub-blocks within the list.

step 5: perform chaotic map to choose the 4*4 sub-block that will be modified during the embedding of the binary watermark. And apply the DCT is applied to the selected 4x4 block. In this case, the DCT is used to change the spatial domain of the image block into the frequency domain, which helps in separating low-frequency from high-frequency components within the block.

The combination of DCT and DWT was chosen due to the DCT ability in minimizing the visual distortion associated with watermarking by embedding the watermark within low or mid-range components, while DWT provides a variety of resolution levels, this enables the watermark to be robust against attacks. This hybrid method is essential to preserving the invisibility and robustness of the watermarking process. Within each transformed block, the top left 2x2 sub-matrix that corresponds to the low-frequency components will be modified based on the watermark bit value.

Phase 6: Applying the max-average-threshold equation to the top left 2*2 sub matrices that represent the low frequency part, where the total summation of the max value of the 2*2 sub-block with the average of the 2*2 sub block will be added to a constant value determined to be 110 as shown in (6).

$$T= MAX (|A\_(2*2)|) + AVG (|A\_(2*2)|) + 110 \quad (6)$$

Where: A_(2*2)Represents a 2x2 sub-matrix of DCT coefficients transformed block, MAX (| |) refer to the maximum absolute value in the 2x2 sub-matrix , AVG (|A_(2*2)|) denotes to absolute average values of all elements in the 2x2 sub-matrix. And 110 is static threshold value added to ensure robustness.

This equation computes a T value that combine the maximum value and an average of the values in the 2x2 sub-matrix. Where the max value refers to the strongest feature in the block while the average spread out the change across the overall block and the value 110 controls the strength of the modification hence the modification is both stable and imperceptible. The 110 further. Such a formula makes sure that embedding changes are consistent with block characteristics and not too much of disruption to vision content, thus giving robustness to the embedding.

The embedding done by checking the watermark bit if the bit equal to 1 then the top left coefficient of block [0,0] will be modified by adding the T value result from the equation, If the bit equal to 0, the coefficient at [1, 0] is modified. For the bit equal to -1, the top-right coefficient [0, 1] is changed, and when the bit value , the bottom-right coefficient [1, 1] is adjusted.

Step 7: finally, perform inverse DCT (IDCT) to the modified coefficient, to convert the host image back to the spatial domain resulting a colored image containing the watermark image.
Figure 3 and Algorithm 1 describes the embedding process precisely:

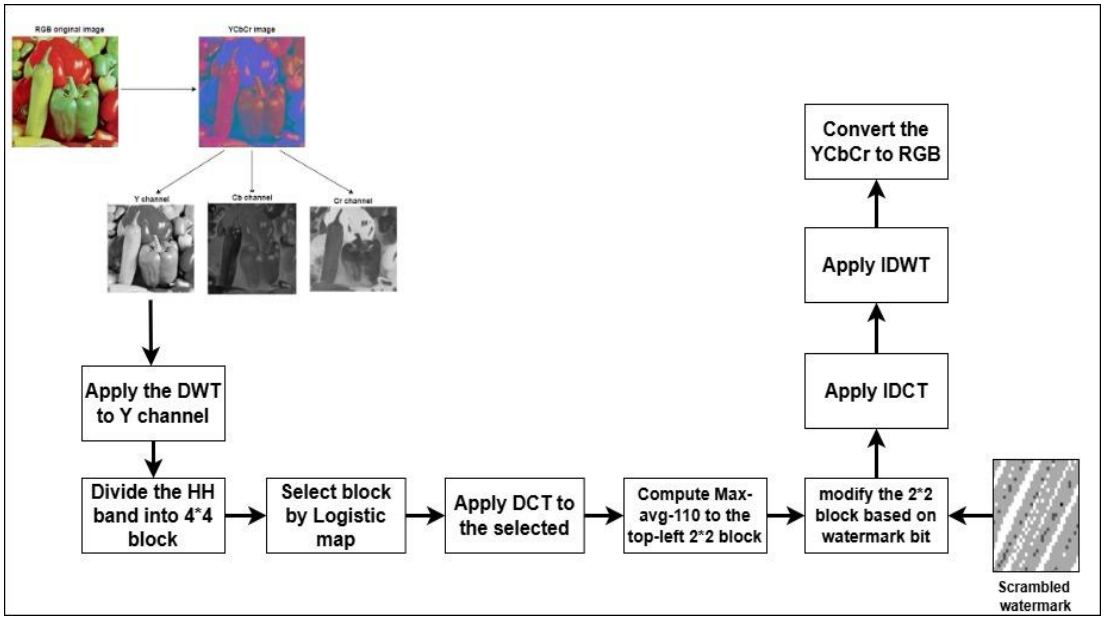

Fig. 3. The Embedding Process

Algorithm 1 : The embedding process
Inputs: bw //Binary watermark data, CI //colored image
Output: HH new Modified HH sub-band with embedded data

Begin
Step 1: Convert CI from RGB to yCbCr.
Step 2: Apply DWT to the Y component.
Step 3: Divide the HH into 4*4 sub bands.
Step 4: Assign value to the variable
- Set w, h ← dimensions of HH
- Set wn ← w // 4 //width size
- Set hn ← h // 4 //height size
- Set wh ← wn * hn // total size

Step 5: Initialize TR list of 4*4 matrices
TR ← list of wh 4x4 zero matrices
Step 6: Extract 4x4 Blocks from HH:
Set k ← 0
For i from 0 to wn-1 do :
For j from 0 to hn-1 do :
x ← i * 4
y ← j * 4
TR[k] ← Y[x:x+4, y:y+4]
k ← k + 1

Step 7: select the embedding index by logistic map
- Set Lw ← length of bw // the size of watermark
- Set X ← logistic_map(wh, Lw)

Step 8: Embed Binary Data into 4x4 Blocks:
For all i from 0 to Lw -1 do :
hdd ← DCT(TR[x[i]], norm='ortho')
T ← (max(abs(hdd[:2, :2])) + sum(abs(hdd[:2, :2])) / 4) + 110
If bw [i] == 1 do:
hdd[0, 0] ← abs(round(hdd[0, 0])) + T

```
                Else if bw im[i] == 0 do:
                      hdd[1, 0] ← abs(round(hdd[1, 0])) + T
                 Else if im[i] == -1 do:
                        hdd[0, 1] ← abs(round(hdd[0, 1])) + T
                 Else if im[i] == -2 do:
                        hdd[1, 1] ← abs(round(hdd[1, 1])) + T
step 9: Apply IDCT // inverse DCT
              TR[x[i]] ← IDCT(hdd, norm='ortho')
Step 10: Apply IDWT // inverse dwt
Step 11: convert YCbCr to RGB
End
```

4.4 Tallying Votes

Step 1: The RGB color space is converted into YCbCr color space. Separating luminance (Y) and chrominance (Cb and Cr) components. The watermark extraction is conducting in the Y component, since during the watermark embedding phase, the watermark was incorporated into this component.

Step 2: DWT Applied to Decompose the Y Component into the four sub-bands. The HH sub-band is divided into 4x4 non-overlapping blocks and these blocks are stored in a list, with each entry containing a 4x4 matrix representing a block.

Stage 3: A chaotic sequence is generated using a logistic map, which was also used during the embedding phase to select the blocks for embedding. This ensures that the extraction process accesses the same 4x4 blocks in the correct sequence, guaranteeing the consistency of the watermark retrieval.

Step 3: For every block that has been identified by the chaotic sequence, the DCT is applied to change the block from the spatial domain into the frequency domain. The watermark bit is then extracted by analyzing the top-left 2x2 sub-matrix of DCT coefficients in the block. The absolute values of four specific DCT coefficients, located at positions [0,0], [1,0], [0,1], and [1,1], are analyzed. The coefficient with the highest absolute value is identified and used to determine the corresponding binary value for the watermark. Fig. 4. Presents the watermark extraction.

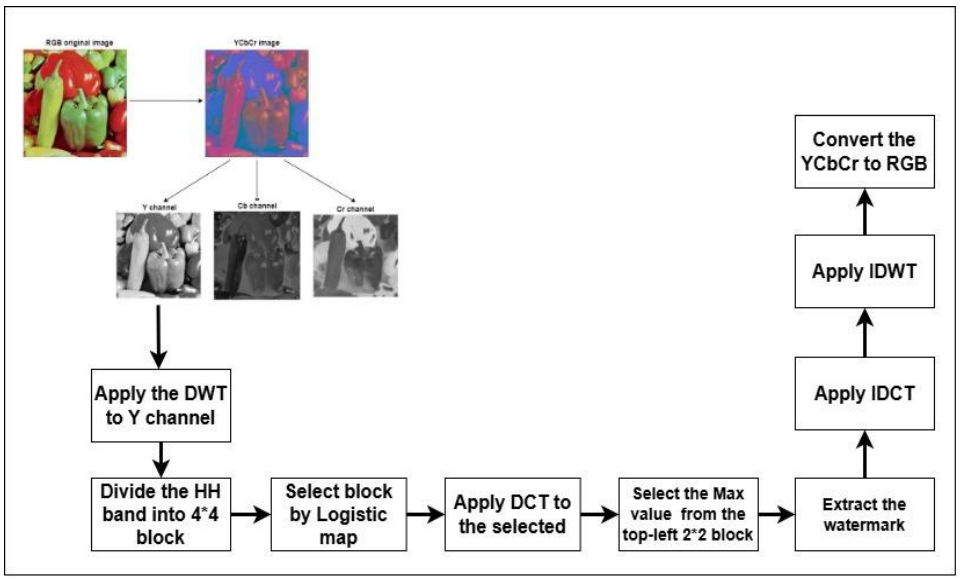

Fig. 4. The Extraction Process

The extracted watermark converted to into binary format then convert the binary to string. After obtaining string the AES-GCM decryption will be able to decrypt the string and obtaining

the voter passcode in addition to the preferred candidate. in this way each candidate counter will be increment after being chosen by the voter. In Algorithm 2, the Etraction process explained in details.

Algorithm 2 : The extracting process

Inputs: CI //colored image

Output: string //contain the voter passcode and the candidate Id

```
Begin
Step 1: Convert CI from RGB to YCbCr.
Step 2: Apply DWT to the Y component.
Step 3: Divide the HH into 4x4 sub-bands.
Step 4: Assign values to the variables:
        -Set w, h ← dimensions of HH.
        -Set wn ← w // 4 //width size.
        -Set hn ← h // 4 //height size.
        -Set wh ← wn * hn // total size.
Step 5: Initialize TR list of 4x4 matrices:
        TR ← list of wh 4x4 zero matrices.
Step 6: Extract 4x4 Blocks from HH:
        Set k ← 0.
        For i from 0 to wn-1 do:
            For j from 0 to hn-1 do:
                x ← i * 4.
                y ← j * 4.
                TR[k] ← HH[x+4, y+4].
                k ← k + 1.
Step 7: Select the embedding index by logistic map:
        -Set Lw ← length of bw // the size of watermark.
        -Set X ← logistic_map(wh, Lw).
Step 8: Extract Binary Data from 4x4 Blocks:
        For all i from 0 to Lw-1 do:
            hdd ← DCT(TR[x[i]], norm='ortho').
            T ← max(abs(hdd[:2, :2])).
            If hdd[0, 0] == T do:
                bw[i] ← 1.
            Else if hdd[1, 0] == T do:
                bw[i] ← 0.
            Else if hdd[0, 1] == T do:
                bw[i] ← -1.
            Else if hdd[1, 1] == T do:
                bw[i] ← -2.
Step 9: Reshape the extracted binary watermark to its original shape.
Step 10: Convert the binary watermark to text.
Step 12: Decrypt the extracted text to retrieve the encrypted vote.
Step 13: Tally the votes for each candidate based on the decrypted data.
End
```

5. Result and Discussion

The proposed system has been implemented utilizing python as programming language incompatible with SQLite as database for storing and managing the system data.

5.1 System evaluation metrics

Imperceptibility and robustness are the two indicators that refer to the watermark performance, where the Imperceptibility refer to the visual quality of the image that must not be

affected by the watermark's embedding(Y. Zhang et al., 2019). The PSNR is the metric employed to measure the imperceptibility Eq (7).

$$PSNR=10\ log_{10}\left(\frac{255^2}{MSE}\right) \quad (7)$$

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{i=j}^{n}(p(i,j)-q(i,j))^2 \quad (8)$$

Where p and q represent the host image and the watermark image respectively while i and j refer to the pixels coordinated.

While the robustness refers to the resistance of embedding watermark against attacks(Araghi et al., 2019). The NC is the metric utilized to measure the coefficients of correlation between the original and the extracted watermark. Eq (9).

$$NC=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}w(i,j).e(i,j)}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}w(i,j)^2\ \sum_{i=1}^{M}\sum_{j=1}^{N}e(i,j)^2}} \quad (9)$$

Where w and e represent the original and extracted watermark respectively and M , N refer to the height and width of the watermark image.

5.2 Result and analysis

For testing and verifying the system performance, the testing mechanism was applied on five colored images 512*512 that considered as standard images (baboon, Lena, airplane, girl and pepper) and the binary watermark image with size 32*32. Figure 5 shows the hosted colored image the binary watermark.

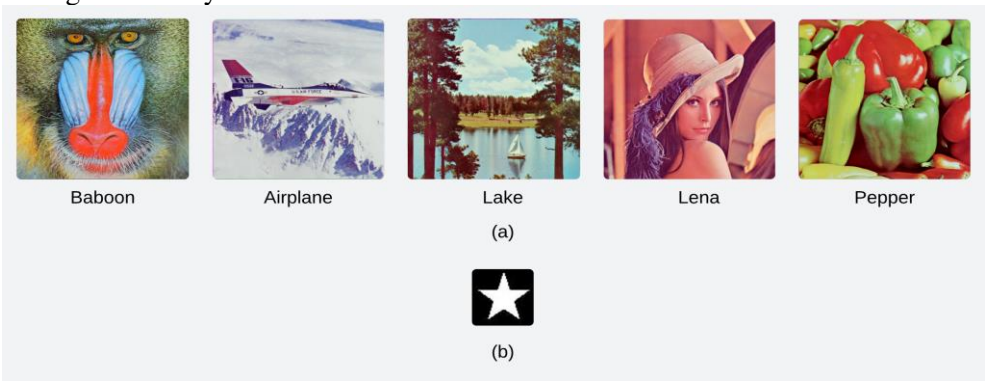

Fig. 5. (a) Host coloured images, (b) binary watermark

5.2.1 Imperceptibility analysis

In watermarking technique, the preserve of high Imperceptibility should be a major concern

In the proposed system the binary watermark in Figure 5 b will be imbedded in the hosted color image in Figure 5 a. The achieved PSNR in Figure 8 was greater than 40 db ranging from 40.2 to 41.9. Figure 6 show the host-colored image before and after embedding where the original and the watermarked images appear nearly identical, there is no visible difference or corruption caused by the watermark's embedding. This watermarking process preserve the visual quality and confirms the effectiveness of the watermarking algorithm in achieving imperceptibility.

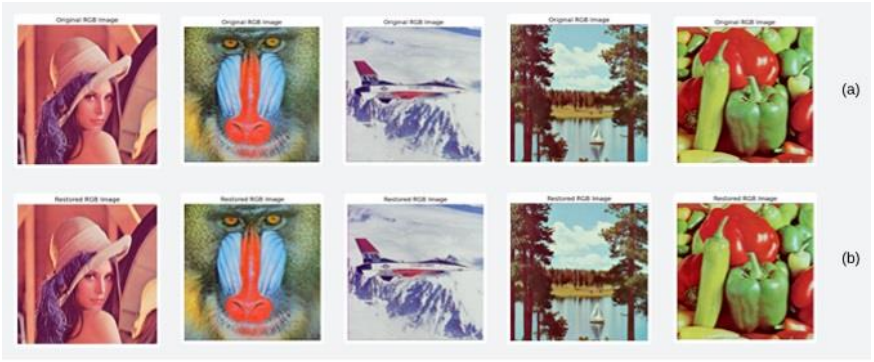

Fig. 6. (a) host colored image before embedding the water mark. (b) host colored image before embedding the watermark.

The Figure 7 represents the histogram of the original and watermarked image shows minimal differences in pixel intensity distributions across the red, green, and blue channels. The original shape of the histogram remains unchanged after the embedding process. the minor change in the histogram refers to the presence of the watermark that not effect on the visual quality of the watermarked images.

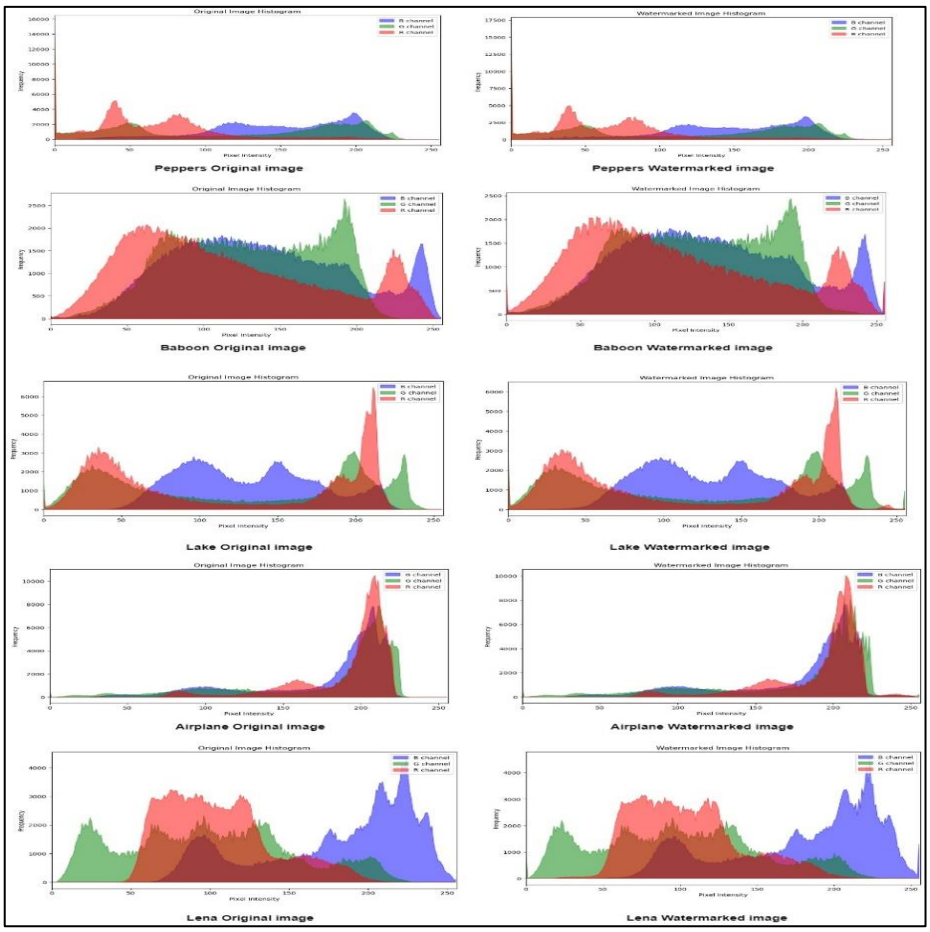

Fig. 8. The Histogram Of The Host Image Before And After Embedding

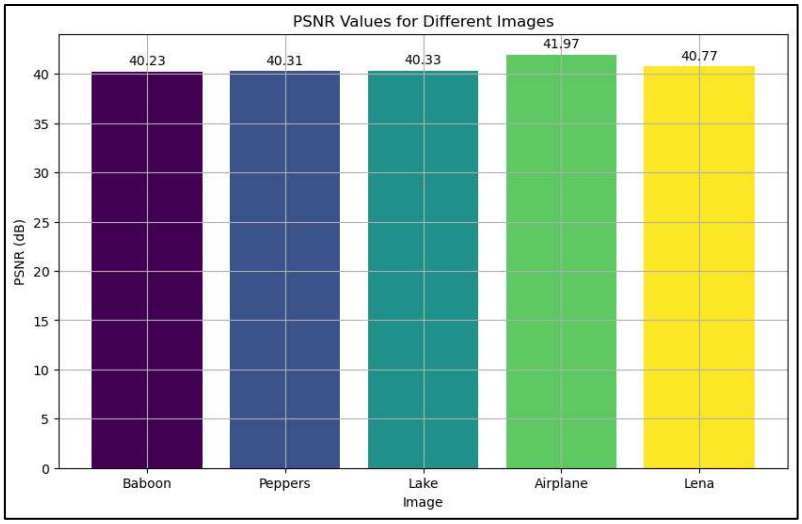

Fig. 8. The PSNR value within test images

5.2.2 Robustness analysis

The robustness of the image refers to the ability of watermark image to endure several type of attack and ensuring the safety of the extracted watermark. As the proposed work is an e-voting system, the focus on preserving the watermark Undamaged was a main concern to retrieve accurate voting result. Though several attacks has been tested (salt and pepper, gaussian noise, histogram equalization, sharpening and compression). The NC was the evaluation metric to measure the robustness as mentioned in eq 3. The achieved ns was in the most attacks 1 that referring the robustness and the efficiency of the proposed work without losing the quality of watermark image. Table 1 show the Nc value without attacks.

Table 1- the Nc value without attack

Image	Baboon	Lake	Airplane	Lena	peppers
NC	1	1	1	1	1

By throwing an attack to the host image, the salt and pepper resulting 0.9 NC value while preserving the NC value equalling 1 with the rest attacks. Table 2- 6 and Figures demonstrates The NC value within applying the attacks.

Table 2 - the NC value of Baboon image with several attack

Image name	PSNR	NC	Attack
Baboon	40.2258	1.0	No
Baboon	38.9951	0.9919	Salt and pepper 0.01
Baboon	40.2010	1.0	Gaussian noise
Baboon	27.9016	1.0	Histogram equalization
Baboon	27.8194	1.0	Sharpening
Baboon	29.4674	1.0	JPEG Compression QF=50
Baboon	29.5448	1.0	JPEG Compression QF=55
Baboon	29.6705	1.0	JPEG Compression QF=63
Baboon	29.7275	1.0	JPEG Compression QF=66
Baboon	29.7512	1.0	JPEG Compression QF=67
Baboon	29.8107	1.0	JPEG Compression QF=70

Table 3 - the NC value of Peppers image with several attack

Image name	PSNR	NC	Attack
Peppers	40.3109	1	No
Peppers	39.0574	0.97847 No result back	Salt and pepper 0.01
Peppers	40.2693	1.0	Gaussian 0.3

Peppers	28.4266	1.0	Histogram equalization
Peppers	27.9930	1.0	Sharpening
Peppers	27.8031 31.35457133791792	0.9703 The passcode and Id note back	JPEG Compression QF=50
Peppers	31.4533	0.9865 The Id and passcode retrieved	JPEG Compression QF=55
Peppers	31.5320	0.9919 The Id and passcode retrieved	JPEG Compression QF=60
Peppers	31.5320	0.99195 The Id and passcode retrieved	JPEG Compression QF=66
Peppers	31.5931	0.99463 The Id and passcode retrieved	JPEG Compression QF=63
Peppers	31.6896	1.0	JPEG Compression QF=67
Peppers	31.7962	1.0	JPEG Compression QF=70

Table 4 - the NC value of Lake image with several attack

Image name	PSNR	NC	Attack
Lake	40.3286	1	No
Lake	39.0191	0.9892	Salt and pepper 0.01
Lake	40.2935	1.0	Gaussian noise
Lake	28.5356	1.0	Histogram equalization
Lake	27.7074	1.0	Sharpening Beta -0.5
Lake	30.5628	0.9973	Compression QF=50
Lake	30.6502	0.9973 The Id and passcode not retrieved	Compression QF=55
Lake	30.7264	1.0	Compression QF=60
Lake	30.8497	1.0	Compression QF=66
Lake	30.7864	1.0	Compression QF=63
Lake	30.8738	1.0	Compression QF=67
Lake	30.9421	1.0	Compression QF=70

Table 5 - the NC value of Lena image with several attack

Image name	PSNR	NC	Attack
Lena	40.7755	1	No
Lena	39.4008	0.9811 The id and passcode not retrieved	Salt and pepper noise 0.01
Lena	40.7315	1.0	Gaussian noise
Lena	27.7291	0.1	Histogram equalization
Lena	27.7802	1.0	Sharpening Beta -0.5
Lena	31.9852	1.0 The passcode and Id not back	Compression QF=50
Lena	32.1435	1.0 The Id and passcode not retrieved	Compression QF=55

Lena	32.2681	1.0 The Id and passcode not retrieved	Compression QF=60
Lena	32.4418	1.0 The Id and passcode retrieved	Compression QF=66
Lena	32.3448	1.0	Compression QF=63
Lena	32.4837	1.0	Compression QF=67
Lena	32.6098	1.0	Compression QF=70

Table 6 - the NC value of airplane image with several attack

Image name	PSNR	NC	Attack
Airplane	41.9661	1	No
Airplane	40.0915	0.9622 The id and passcode not retrieved	Salt and pepper 0.01
Airplane	41.9316	1.0	Gaussian noise
Airplane	27.3495	0.9973 The id and passcode retrieved	Histogram equalization
Airplane	27.4223	1.0	Sharpening Beta -0.5
Airplane	32.3557	0.9920	Compression QF=50
Airplane	32.5500	0.9973	Compression QF=55
Airplane	32.6996	1.0	Compression QF=60
Airplane	32.8913	1.0	Compression QF=66
Airplane	32.7794	1.0	Compression QF=63
Airplane	32.9463	1.0	Compression QF=67
Airplane	33.1371	1.0	Compression QF=70

The results in Tables 2–6 show the proposed system to be very robust against attacks of various kinds; for NC, values remained almost entirely at 1.0 (in most cases,) meaning the embedded watermark was only slightly degraded. These fluctuations in NC values obtained for different images under the same type of attack may largely be attributed to the inherent characteristics of the images themselves and the manner in which a particular attack affects the frequency domain. For example, high-texture images like "Baboon," which depicts a large variance of different frequency components, can often withstand salt-and-pepper noise better since they have spread the information of the watermark much better over various frequencies. Therefore, in such cases, the high Texture images will better resist salt-and-pepper noise. Smoother images such as "Lena," on the other hand, exhibit very few spatial details. For instance, they may have slightly lower values of NC under noise-based attacks since these images can clearly exhibit a few selected damaged regions that can obscure localized distortions. Likewise, some attacks, for instance, the compressive or sharpening ones, may be less effective since the frequencies of the image are in resonance with the embedding strategy. Very close, consistent NC values around 1.0 for most scenarios drive home the point of steadfastness of the hybrid watermarking scheme under consideration based on DWT-DCT, giving an assertion of it being able to provide invariance for the watermark under a host of practical conditions.

5.2.3 comparison analysis

The proposed work imperceptibility achieves PSNR higher than in the researches (Bao & Wang, 2024), (X. Zhang et al., 2021) ,(Lee et al., 2021) and (Su et al., 2024) .where the binary watermark has been tested in size 23*32. The result of the proposed system focusing on preserving the robustness of the watermarking process refers to the ability of retrieve the encrypted vote and safeguard the vote confidentiality. While the achieved PSNR indicates

minimal distortion in compression with the previous study reducing the likelihood of detecting embedding vote within the hosted image by the attacker. The table 7 and Figure 8 shows the PSNR comparison.

Table 7 - PSNR comparison

Scheme	Lena	Baboon	Peppers	Airplane	Lake
(Bao and Wang, 2024b)	38.7824	37.5208	38.2924	38.0927	-
(Su et al., 2024)	40.583	40.408	40.103	40.600	40.323
(Zhang and Su, 2021b)	40.0338	-	-	-	-
(Lee et al., 2021)	37.7	39.4	37.1	38.4	-
(D. Liu et al., 2021)	36.5	36.2	35.6	-	-
Proposed	40.829	40.165	40.257	41.950	40.326

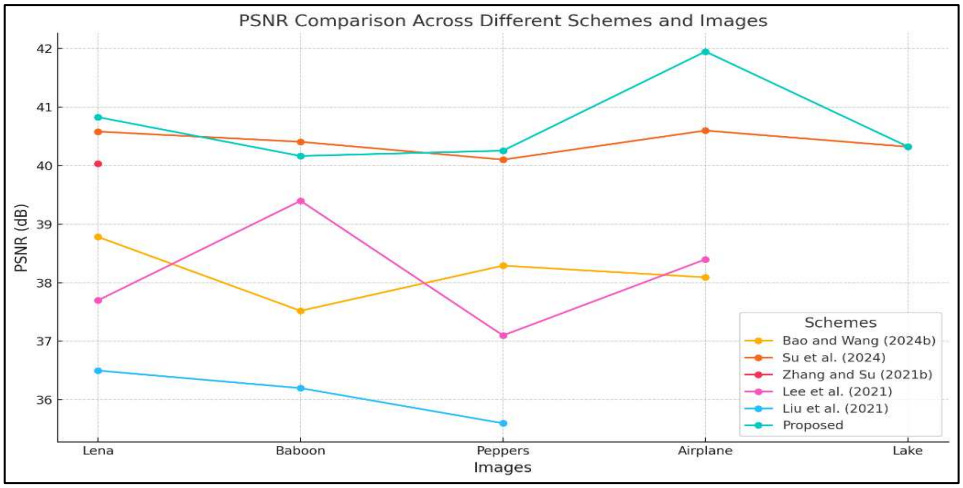

Fig. 8. PSNR comparison

In the concept of robustness, the proposed scheme has proven its ability to maintain the watermark even after repelling attacks, as the value of the NC within salt and pepper attack was ranging from 9.9 to 9.6 while in JPEG Compression, Sharpening, Histogram equalization and Gaussian noise the scheme success in preserving the watermark without any damage and consequently preserving the vote retrieving and the NC value is 1. Table 8 and Figure 9 display the NC value compared with other researches.

Table 8 - NC comparison

Attack	(Bao and Wang, 2024b) NC	(Su et al., 2024) NC	(Zhang and Su, 2021b) NC	(Lee et al., 2021) NC	(D. Liu et al., 2021) NC	**Proposed** NC
Salt & pepper	0.9955	-	0.9621	0.9642	0.9475	0.980
Gaussian noise	0.9963	(0,0.001) 0.970	-	0.9983	0.965	0.983
Sharpening	0.999	-	-	0.9923	-	1.0
Histogram equalization	-	-	-	1	-	1.0
JPEG compression until 65 QF	0.9881	(70 QF) 0.989	1.0	0.9974	1.0	1.0

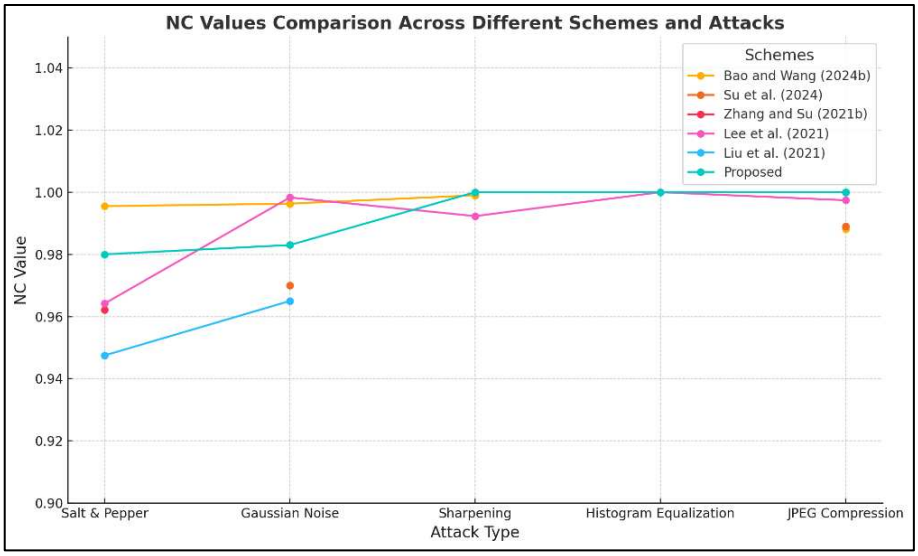

Fig. 9. NC comparison

5.2.4 imperceptibility Analysis

A better imperceptibility achieved by the proposed system due to the embedding of the watermark bits in the Y component of the YCbCr color space, resulting in very few visual distortion. (Bao et al., 2024b) work on DCT-transformed blocks at middle frequency coefficients, that may be conspicuous in high-quality images (Su et al., 2024) depended on GBT and chaotic encryption, that make a lot of influence in the visual appearance of the image due to the complexity of the estimated embedding domain. DWT and DCT are particularly embedded methods where the most visual changes are not imposed, and high imperceptibility is achieved. DHT implemented in spatial resolution was highly effective but comparably crude compared to frequency-based embedding techniques for obvious reasons as cited by (X. Zhang et al., 2021). Repetitive embedding using voting techniques certainly deteriorates output quality as discussed by (Lee et al., 2021). (D. Liu et al., 2021)), using simpler DCT-based embedding, did not optimize for imperceptibility as effectively as our approach. By setting the embedding process with the max-average-threshold equation while concentrating on the low-frequency components, a balanced trade-off between robustness and imperceptibility is achieved by the proposed system, which is highly workable for real applications such as secure e-voting.

5.2.5 Robustness Analysis

Proposed system exceeds other studies in robustness by using the chaotic logistic map, and the max-average-threshold equation that adjusts embedding strength dynamically. For ensuring the watermark is robust against different attacks. Unlike (Bao et al., 2024b) who applied Radon and DCT transforms with fixed mid-frequency embedding, and (Su et al., 2024) who applied Graph-Based Transform (GBT) with adaptive embedding strength based on Particle Swarm Optimization, our method embeds watermark bits in selected low-frequency components. Such components are not much sensitive to usual image processing attacks, which enhances the proposed method's robustness. (X. Zhang et al., 2021), utilized discrete Hartley transform (DHT) less robust against noise and compression attacks compared to frequency-based techniques. Additionally, the embedding capacity is limited, making the method unsuitable for applications requiring larger watermark data and (Lee et al., 2021) that employs repetitive DCT embedding with voting mechanisms that introduced a distortion compromised image quality. (D. Liu et al., 2021) concentrated more on unsophisticated DCT-based embedding without the positive robustness enhancements inherent in their proposed technique.

6. Practical Implications

The proposed work has several implication aspects within the e-voting system. Regarding the voter authentication process the proposed system utilized the SIFT algorithm for detecting

and matching the distinct features along with utilizing passcode matching as dual authentication step. Regarding the voting securing, encrypting the vote with AES_GCM ensuring both integrity and confidentiality where the vote remain secure during the transmission and storage. The robustness of the embedding procedure against attacks enhances the reliability of the voting process. In the real-world framework retrieving the vote despite the accidental or intention distortion referring to the robustness of safeguarding the vote. Though, preserving the vote integrity. While the higher PSNR referring to the minimal distortion to the host image and preserving the visual quality.

7. Limitations

Although the proposed system gives satisfactory results in terms of robustness and stealth, the system may be subject to limitations in terms of engineering attack, and the need to test the system in the real world in terms of latency, storage overhead, and processing capacity in high-demand scenarios may require further optimization. The robustness of the watermark is also affected by the quality of the host image, as low-quality or over-compressed images affect the extraction accuracy, posing challenges in real-world environments with variable image quality.

8. Conclusion

The proposed work focus on achieving authenticity and vote secrecy in the e-voting system. In concept of voter authenticity, the unique Six-digit passcode in addition to fingerprint as biometric traits will be able to prevent ineligible people from vote. The SIFT algorithm is the method utilized of identified the voter biometrically. While the securing the vote implemented within several stages, starting with encrypting the vote by the AES-GCM method for keeping the vote integrity. Then, the embedding of the vote within colored host image using the blind, robust and hybrid DWT-DCT algorithms with utilizing the chaotic map techniques for increasing the security level and keeping the vote process reliable and robust against several attacks. The experimental results of the proposed the system had ability to maintain high imperceptibility and robustness to distortions, achieving a PSNR above 40 dB and an NC value of 1 in most scenarios. While the system's performance is exceptional in securing and verifying votes, future enhancements could focus on addressing geometric attacks and improving the scalability of large- scale elections, this would lead to a more secure, reliable, and popular e-voting system.

References

Abdallah, A. A., & Farhan, A. K. (2022). A New Image Encryption Algorithm Based on Multi Chaotic System. *Iraqi Journal of Science*, 324–337. https://doi.org/10.24996/ijs.2022.63.1.31

Adeniyi, J. K., Ajagbe, S. A., Adeniyi, E. A., Mudali, P., Adigun, M. O., Adeniyi, T. T., & Ajibola, O. (2024). A biometrics-generated private/public key cryptography for a blockchain-based e-voting system. *Egyptian Informatics Journal*, *25*, 100447. https://doi.org/10.1016/j.eij.2024.100447

Agarwal, S., Haider, A., Jamwal, A., Dev, P., & Chandel, R. (2020). Biometric Based Secured Remote Electronic Voting System. *2020 7th International Conference on Smart Structures and Systems (ICSSS)*, 1–5. https://doi.org/10.1109/ICSSS49621.2020.9202212

Agrawal, A., Sethi, K., & Bera, P. (2023a). *Blockchain-Based Cardinal E-Voting System Using Biometrics, Watermarked QR Code and Partial Homomorphic Encryption* (pp. 411–436). https://doi.org/10.1007/978-981-19-6414-5_23

Agrawal, A., Sethi, K., & Bera, P. (2023b). *Blockchain-Based Cardinal E-Voting System Using Biometrics, Watermarked QR Code and Partial Homomorphic Encryption* (pp. 411–436). https://doi.org/10.1007/978-981-19-6414-5_23

Alamri, H., Alshanbari, E., Alotaibi, S., & Alghamdi, M. (2022). Face Recognition and Gender Detection Using SIFT Feature Extraction, LBPH, and SVM. *Engineering, Technology & Applied Science Research*, *12*(2), 8296–8299. doi: 10.48084/etasr.4735

Ali, H. H., & Shaker, S. H. (2023). *Secured E-voting system based on iris identification*. 030025. doi: 10.1063/5.0119826

Araghi, T. K., & Manaf, A. A. (2019). An enhanced hybrid image watermarking scheme for security of medical and non-medical images based on DWT and 2-D SVD. *Future Generation Computer Systems*, *101*, 1223–1246. doi: 10.1016/j.future.2019.07.064

B. O. Ahubele and Linda U. Oghenekaro. (2022). Secured Electronic Voting System Using RSA Key Encapsulation Mechanism. *European Journal of Electrical Engineering and Computer Science*, *6*(2).

Bao, B., & Wang, Y. (2024a). A robust blind color watermarking algorithm based on the Radon-DCT transform. *Multimedia Tools and Applications*, *83*(24), 64663–64682. https://doi.org/10.1007/s11042-023-17875-5

Bao, B., & Wang, Y. (2024b). A robust blind color watermarking algorithm based on the Radon-DCT transform. *Multimedia Tools and Applications*, *83*(24), 64663–64682. https://doi.org/10.1007/s11042-023-17875-5

Fares, K., Khaldi, A., Redouane, K., & Salah, E. (2021). DCT & DWT based watermarking scheme for medical information security. *Biomedical Signal Processing and Control*, *66*, 102403. https://doi.org/10.1016/j.bspc.2020.102403

Garg, P., & Kishore, R. R. (2022). An efficient and secured blind image watermarking using ABC optimization in DWT and DCT domain. *Multimedia Tools and Applications*, *81*(26), 36947–36964. https://doi.org/10.1007/s11042-021-11237-9

Han, B., & Li, J. (2016). A New Zero-Watermarking Algorithm Resisting Attacks Based on Differences Hashing. *Cybernetics and Information Technologies*, *16*(2), 135–147. https://doi.org/10.1515/cait-2016-0026

Harba, E. S., Harba, H. S., Abdulmunem, I. A., & Hussein, S. S. (2021). Improving security of the crypto-stego approach using time sequence dictionary and spacing modification techniques. *Iraqi Journal of Science*, *62*(5), 1721–1733. https://doi.org/10.24996/ijs.2021.62.5.35

Hossain Faruk, M. J., Alam, F., Islam, M., & Rahman, A. (2024). Transforming online voting: a novel system utilizing blockchain and biometric verification for enhanced security, privacy, and transparency. *Cluster Computing*, *27*(4), 4015–4034. https://doi.org/10.1007/s10586-023-04261-x

Hussein, N., Ali, M., & Kadhum, R. N. (2022). Using steganography techniques for implicit authentication to enhance sensitive data hiding. *Article in The Journal of Nonlinear Sciences and Applications*, *13*, 2008–6822. https://doi.org/10.22075/ijnaa.2022.6211

Jayakumari, B., Sheeba, S. L., Eapen, M., Anbarasi, J., Ravi, V., Suganya, A., & Jawahar, M. (2024). E-voting system using cloud-based hybrid blockchain technology. *Journal of Safety Science and Resilience*, *5*(1), 102–109. https://doi.org/10.1016/j.jnlssr.2024.01.002

Lee, C.-F., Chang, C.-C., Wang, Z.-H., & Di, Y.-F. (2021). A High Robust and Blind Image Watermarking Using Arnold Transform Mapping in the DCT Domain of YCbCr Color Space. *Taiwan Ubiquitous Information*, *6*(3).

Li, L., Mu, X., Li, S., & Peng, H. (2020). A Review of Face Recognition Technology. *IEEE Access*, *8*, 139110–139120. https://doi.org/10.1109/ACCESS.2020.3011028

Li, Z., Zhang, H., Liu, X., Wang, C., & Wang, X. (2021). Blind and safety-enhanced dual watermarking algorithm with chaotic system encryption based on RHFM and DWT-DCT. *Digital Signal Processing*, *115*, 103062. https://doi.org/10.1016/j.dsp.2021.103062

Liu, D., Su, Q., Yuan, Z., & Zhang, X. (2021). A color watermarking scheme in frequency domain based on quaternary coding. *The Visual Computer*, *37*(8), 2355–2368. https://doi.org/10.1007/s00371-020-01991-6

Lowe, D. G. (2004). Distinctive Image Features from Scale-Invariant Keypoints. In International Journal of Computer Vision (Vol. 60, Issue 2).

Mahagaonkar, R. V, & Shiurkar, U. D. (2023). A two way secured high imperceptible digital color image watermarking. *Sādhanā*, *48*(4), 220. https://doi.org/10.1007/s12046-023-02299-6

Mohammed, A. O., Hussein, H. I., Mstafa, R. J., & Abdulazeez, A. M. (2023a). A blind and robust color image watermarking scheme based on DCT and DWT domains. *Multimedia Tools and Applications*, *82*(21), 32855–32881. https://doi.org/10.1007/s11042-023-14797-0

Mohammed, A. O., Hussein, H. I., Mstafa, R. J., & Abdulazeez, A. M. (2023b). A blind and robust color image watermarking scheme based on DCT and DWT domains. *Multimedia Tools and Applications*, *82*(21), 32855–32881. https://doi.org/10.1007/s11042-023-14797-0

Okokpujie, K., Abubakar, J., John, S., Noma-Osaghae, E., Ndujiuba, C., & Princess Okokpujie, I. (2021a). A secured automated bimodal biometric electronic voting system. *IAES International Journal of Artificial Intelligence (IJ-AI)*, *10*(1), 1. https://doi.org/10.11591/ijai.v10.i1.pp1-8

Okokpujie, K., Abubakar, J., John, S., Noma-Osaghae, E., Ndujiuba, C., & Princess Okokpujie, I. (2021b). A secured automated bimodal biometric electronic voting system. *IAES International Journal of Artificial Intelligence (IJ-AI)*, *10*(1), 1. https://doi.org/10.11591/ijai.v10.i1.pp1-8

Olumide S., A., Olutayo K., B., & E. Adekunle, S. (2020). A Review of Electronic Voting Systems: Strategy for a Novel. *International Journal of Information Engineering and Electronic Business*, *12*(1), 19–29. https://doi.org/10.5815/ijieeb.2020.01.03

Oravec, J., Ovsenik, L., & Papaj, J. (2021). An Image Encryption Algorithm Using Logistic Map with Plaintext-Related Parameter Values. *Entropy*, *23*(11), 1373. https://doi.org/10.3390/e23111373

Osama A. Salman, S. M. H. (2018). User Authentication via Mouse Dynamics. *IRAQI JOURNAL OF SCIENCE*, *59*(2B). https://doi.org/10.24996/ijs.2018.59.2B.18

Pasha, X., & Jahankhani, H. (2024). Securing E-Voting Authentication: A Framework Integrating AI-Based Facial Recognition. In *Navigating the Intersection of Artificial Intelligence, Security, and Ethical Governance: Sentinels of Cyberspa*ce (pp. 19-46). Cham: Springer Nature Switzerland.

Pourjabbar Kari, A., Habibizad Navin, A., Bidgoli, A. M., & Mirnia, M. (2021). A new image encryption scheme based on hybrid chaotic maps. *Multimedia Tools and Applications*, *80*(2), 2753–2772. https://doi.org/10.1007/s11042-020-09648-1

Rahman, K. N., Hridoy, M. W., Mizanur Rahman, M., Islam, M. R., & Banik, S. (2024). Highly secured and effective management of app-based online voting system using RSA encryption and decryption. *Heliyon*, *10*(3), e25373. https://doi.org/10.1016/j.heliyon.2024.e25373

Rajab, M. (2023). Human Identification Based on SIFT Features of Hand Image. *International Journal of Computing and Digital Systems*, *14*(1), 367–375. https://doi.org/10.12785/ijcds/140128

Reyam Jassim Essa, N. A. Z. A. R. D. A.-D. (2018). Steganography Technique using Genetic Algorithm. *IRAQI JOURNAL OF SCIENCE*, *59*(3A). https://doi.org/10.24996/ijs.2018.59.3A.19

Saleh, F. F., & Ali, N. H. M. (2022). Generating Streams of Random Key Based on Image Chaos and Genetic Algorithm. *Iraqi Journal of Science*, 3652–3661. https://doi.org/10.24996/ijs.2022.63.8.39

Sarkar, A., & Singh, B. K. (2020). A review on performance,security and various biometric template protection schemes for biometric authentication systems. *Multimedia Tools and Applications*, *79*(37–38), 27721–27776. https://doi.org/10.1007/s11042-020-09197-7

Sherine, A., Peter, G., Stonier, A. A., Leh Ping, D. W., Praghash, K., & Ganji, V. (2022). Development of an Efficient and Secured E-Voting Mobile Application Using Android. *Mobile Information Systems*, *2022*, 1–11. https://doi.org/10.1155/2022/8705841

Su, Q., Hu, F., Tian, X., Su, L., & Cao, S. (2024). A fusion-domain intelligent blind color image watermarking scheme using graph-based transform. *Optics and Laser Technology*, *177*. https://doi.org/10.1016/j.optlastec.2024.111191

Takaki, T., Li, Y., Sakiyama, K., Nashimoto, S., Suzuki, D., & Sugawara, T. (2020). An Optimized Implementation of AES-GCM for FPGA Acceleration Using High-Level Synthesis. *2020 IEEE 9th Global Conference on Consumer Electronics, GCCE 2020*, 176–180. https://doi.org/10.1109/GCCE50665.2020.9291973

Tamilselvi, M., Manimaran, B., & Inunganbi, S. C. (2023). Empirical Assessment of Artificial Intelligence Enabled Electronic Voting System Using Face Biometric Verification

Strategy. *2023 Eighth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, 1–7. https://doi.org/10.1109/ICONSTEM56934.2023.10142923

Tian, C., Wen, R.-H., Zou, W.-P., & Gong, L.-H. (2020). Robust and blind watermarking algorithm based on DCT and SVD in the contourlet domain. *Multimedia Tools and Applications*, *79*(11–12), 7515–7541. https://doi.org/10.1007/s11042-019-08530-z

Waheed, A., Din, N., Umar, A. I., Ullah, R., & Amin, N.-. (2021). Novel Blind Signcryption Scheme for E-Voting System Based on Elliptic Curves. *Mehran University Research Journal of Engineering and Technology*, *40*(2), 314–322. https://doi.org/10.22581/muet1982.2102.06

Yousif, H. M., & Hameed, S. M. (2024). Preserving Genotype Privacy Using AES and Partially Homomorphic Encryption. *Iraqi Journal of Science*, 1663–1678. https://doi.org/10.24996/ijs.2024.65.3.38

Zhan, Y., Zhao, W., Zhu, C., Zhao, Z., Yang, N., & Wang, B. (2024). Efficient Electronic Voting System Based on Homomorphic Encryption. *Electronics*, *13*(2), 286. https://doi.org/10.3390/electronics13020286

Zhang, X., & Su, Q. (2021). A spatial domain-based color image blind watermarking scheme integrating multilevel discrete Hartley transform. *International Journal of Intelligent Systems*, *36*(8), 4321–4345. https://doi.org/10.1002/int.22461

Zhang, Y., & Sun, Y. (2019). An image watermarking method based on visual saliency and contourlet transform. *Optik*, *186*, 379–389. https://doi.org/10.1016/j.ijleo.2019.04.091