

Enhanced Face Image Authentication Scheme Using Chaotic-based Bit Substitution Algorithm

Rasha Thabit ^{1,2*}, Ali Tariq Al-Tamimi ¹

¹⁾ *Al-Iraqia University, Baghdad, Iraq*

²⁾ *Al-Imam University College, Balad, Iraq*

Abstract: One of the biggest challenges in digital multimedia security is making sure the face image is safe and authentic. Various tampering reveal technologies have been presented to serve this aim which have been recently directed towards the watermarking-based Face Image Authentication (FIA) methods. The FIA schemes obtained promising results in this field; however, the restricted capacity was the main challenge. This paper presents a novel Chaotic-based Bit Substitution Algorithm (CBSA) that incorporates various techniques to enhance the performance of the proposed Enhanced-FIA (E-FIA) scheme. The embedding capacity has been improved which leads to the ability of protecting more face images that have not been protected using previous FIA schemes. Furthermore, integrating a chaotic system strengthens security by controlling the bit embedding process. In comparison to current FIA schemes, the E-FIA also preserves the greater visual quality of watermarked images. Additionally, the improved security and embedding capability guarantee wider application across a variety of image formats, including those with intricate textures and high-resolution features. Several experimental tests have been conducted which proved the efficiency of the proposed E-FIA scheme in detecting tampering in face region and recover the original face area with enhanced capacity, security, and visual quality.

Keywords: Face image authentication; Face image Security; Image authentication; Information forensics; Deepfakes detection

1. INTRODUCTION

The rapid expansion of technology and image processing applications leads to an increased exchange of digital images through the internet. The shared images are accessible and can easily be manipulated and attacked for various intentions [1,2]. Therefore, safeguarding shared images from unauthorized usage has become a high priority. The most known methods for safeguarding digital images are steganography [3-5] and watermarking [6,7]. Steganography is used for hiding the presence of secret information; thus, the protected data is unnoticeable. On the other side, watermarking is used for various purposes such as copyright protection, checking the image's authenticity, manipulation detection, and in some cases the original image can be self-recovered. While watermarking can be applied to grayscale and color images, color images are preferred because they have three channels (red, green, and blue), which provide a larger embedding space. The application of the watermarking scheme specifies the key aspects that must be obtained by the scheme such as invisibility, robustness, embedding factor selection, security, and high payload capacity to ensure effective watermarking while minimizing distortions in the host image [8-10].

Techniques for watermarking can be broadly divided into two categories: spatial domain and frequency domain. Spatial domain watermarking embeds the watermark by directly altering the host image's pixel values [11-13]. Although this approach is computationally straightforward and takes little processing time, it is susceptible to assaults like filtering, compression, and noise addition. The least significant bit (LSB) approach, which embeds the

* Corresponding author: rasha.thabit@aliraqia.edu.iq

watermark bits in the least significant bits of the pixel values, is one of the most often used spatial domain techniques. The LSB-based methods have a high embedding capacity; however, they are susceptible to even little picture changes. The other kind, known as frequency domain watermarking, is inserting the watermark inside the altered coefficients after converting the host image to a different domain. As a result, the domain gains insensitivity and resilience [14], increasing its resistance to compression, distortion, and other effects. Frequency domain watermarking employs a number of transformation techniques, such as the Discrete Hadamard Transform (DHT) [15], Lifting Wavelet Transform (LWT) [16,17], Walsh-Hadamard Transform (WHT) [18], Fourier Transform (FT) [19], Discrete Wavelet Transform (DWT) [20-22], Discrete Cosine Transform (DCT) [23,24], Integer Wavelet Transform (IWT) [25], Slantlet Transform (SLT) [26,27] and hybrid transforms [28,29]. Spatial domain watermarking offers a simple and powerful embedding method; however, it is not very resistant to attacks. Frequency domain watermarking may need intricate computations yet is more resistant to different distortions. As a result, the application requirements based on a particular approach such as security, robustness, insensitivity, and large capacity, determine which watermarking technique is best.

Various frequency-domain based watermarking techniques have been presented which have successfully attain their aims but there is always a room for improvements. **Al Haj et al. in 2017** [30] developed watermarking technology using hybrid DWT-SVD transformation that supports confidentiality, authenticity and integrity of the medical images. This method can provide robustness to the hidden data and supports the localization of tampering in the Region-of-Interest (ROI) (i.e., the important part of the medical image that is used for diagnosis). It can also be used successfully on different types of medical images but the drawbacks are the low embedding capacity (0.0469 bit per pixel (bpp)) and the inability to recover the ROI. **Rasha Thabit et al. in 2017** [31] developed a watermarking technique by employing the SLT and IWT to generate the ROI recovery data and subsequently embedding it in the Region-of-Non-Interest (RONI) of the image. This technique provides robustness, accurate detection and localization, and can recover the ROI with good visual quality but its limitation is the low embedding capacity (0.25 bpp). **Priyanka et al. in 2017** [32] developed a watermarking technique by applying IWT-SVD hybrid transformation to support integrity, confidentiality, and authenticity where the data are embedded in the RONI. The embedding process used the LSBs of the ROI to carry the patient's data. This technique works with all types of images but the drawbacks of this method are the distortions in the ROI by hiding authentication data, the inability to recover the ROI, and the low embedding capacity (0.0234 bpp). **Shaozhang Xiao et al. in 2020** [33] developed a multipurpose watermarking technique to support authentication, copyright protection, and tamper localization. Embeds ROI authentication data in ROI itself. Embeds authentication data and a visible watermark in RONI. This method provides robustness and high visual quality. The drawbacks are that it distorts the ROI which cannot be restored to its original state and the limited embedding capacity (0.2 bpp). **Swaraja et al. in 2020** [34] presented a watermarking technique based on DWT-Schur hybrid transformation. The best blocks to hide the compressed form of the ROI inside the image's RONI are determined using visual and edge entropy. This method supports robustness in the embedded data and ROI recovery. The drawbacks of this method are the absence of strong imperceptibility and the low embedding capacity (0.0625 bpp). **Mohammad Yamni et al. in 2024** [35] presented the Integer Reversible Charlier Transform (IRCT) for lossless image processing. IRCT preserves orthogonality and determinism while guaranteeing flawless input data recovery. They created a Reverse Data Hiding (RDH) strategy that is resilient in terms of image quality and resistant to statistical attacks. The drawback is the restricted embedding capacity (0.36 bpp) because of utilizing the concentrated histogram peaks of IRCT. **Geetha R et al. in 2018** [36] suggested utilizing pairwise prediction error expansion on the Integer-Integer Wavelet Transform (I-IWT) to create a reversible data hiding strategy for medical images. All sub-bands include secret data while maintaining image quality. Experimental

results demonstrate greater imperceptibility when compared to other methods, however, the embedding capacity is limited to (0.3494 bpp).

One of the emerging image watermarking applications is the Face Image Authentication (FIA) which is an important process in the field of digital image security, as it ensures the security and integrity of facial images used in biometric verification, digital forensics, and many other applications. The increasing need to facial identity verification has led to the need of introducing mechanisms and techniques that protect and detect unauthorized tampering. Several techniques have been proposed for this purpose, including watermarking-based authentication, cryptographic hashing, and machine learning-based detection. Watermarking-based authentication has received significant attention from researchers as it can securely embed data and extract data later to verify its integrity and protect the image [37].

Face image tampering can be broadly categorized into intentional (malicious) and unintentional (benign) modifications. Intentional manipulation involves deliberate attacks that aim to deceive systems or manipulate information for fraudulent purposes. Common examples include deepfake attacks, where a person's face is replaced with another identity using sophisticated photo editing tools, face warping, which blends multiple identities to create hybrid faces for identity fraud and illegal manipulation. Another deepfake example is localized modification such as changing facial features (e.g., color of the eyes, nose, or mouth). Other types of intentional manipulation include forgery attacks, where objects such as beards, masks, glasses, or even artificial facial elements are added or removed to conceal one's true identity [38-40].

On the other hand, unintentional tampering refers to modifications that are not intended to deceive systems but may affect the performance of the authentication system. These include image processing operations such as lossy compression, which results in slight distortions in pixel values and are significant, adding noise due to environmental factors for cosmetic purposes, and differences in brightness, contrast, or color balance. Additionally, resizing an image can result in slight changes in facial features, which may affect the operation of authentication systems. While these modifications are not malicious, they still affect the system and properly verify the image, so authentication systems must distinguish between original and manipulated images.

By employing image watermarking techniques for tamper detection, recent researchers have put forth a number of strategies to prevent tampering with face photographs. The Face Image Manipulation Detection (FIMD) scheme was presented by **Z. A. Salih et al. (2023)** [41]. It uses watermarking to identify tampering and separates the image into ROI (that refers to the face region) and RONI (that refers to the remaining part of the image). Without the need for intricate training processes, this method successfully recognizes various forms of manipulation and locates the tampered area. The inability of FIMD to restore the original face region once tampering has been detected is the drawback of this scheme. Furthermore, this technique has limited capacity (0.25 bpp). **M. H. Al-Hadaad et al. (2023)** [42] developed FIA to handle the recovery problem. The scheme has the ability to recognize tampering in the face area and restore the original face region after tampering is detected. However, the capacity is still restricted to 0.25 bpp, which limits the quantity of embedded watermark information. **Assma H. Jawad et al. (2024)** [43] presented an improved form of FIA called (I-FIA), in an attempt to increase capacity. This method restores tampered areas while preserving excellent visual quality by using watermarking techniques in conjunction with a recovery algorithm. The primary enhancement of I-FIA is the capacity increment to 0.37 bpp, which permits more embedded data and raises the accuracy of detection and recovery. Even with this improvement, there are still some image situations that cannot be protected because of the restricted embedding capacity. **Rasha et al. (2025)** [44], presented a novel FIA scheme in which the visual quality of the watermarked images and the robustness of the embedded watermark can be adjusted using different threshold values and different blocks sizes. The scheme obtained promising results in terms of visual quality and accurate tampering reveal process which make

it a good candidate compared to various deep-learning based FIMD schemes; however, the embedding capacity is limited to 0.25 bpp.

Although these schemes have made significant advancements in FIA, they still have limitations, particularly in capacity and visual quality of the watermarked images. The authors of FIA [45] and I-FIA [43] suggested the use of other watermarking technologies for future researches to overcome these limitations. Inspired by this suggestion, part of the work in this paper has been dedicated to study various image watermarking techniques to find out the way of improving the capacity while keeping high visual quality. Table 1.1 summarizes a comparison between the abovementioned watermarking schemes in terms of embedding domain, method, region of embedding data, and embedding capacity.

The use of transform-based watermarking is widely preferred in cutting-edge research due to its superior security and robustness against attacks. Recent studies have shown that embedding data in the transform domain enhances security and resistance to distortions better than the spatial domain. Therefore, this research has been directed toward transform-based watermarking. This work aims to develop a new FIA scheme with improved embedding capacity, enhanced visual quality, and increased security.

In the proposed scheme, the Integer Wavelet Transform (IWT) using lifting scheme is adopted, which produces integer coefficients free of fractions and negatives, allowing for faster and more efficient embedding and extraction processes. This property enables fine-grained control over the watermarking processes, facilitating a more accurate and improved approach to securing facial image. Unlike the traditional DWT and SLT, which produce floating-point coefficients and may introduce rounding errors during reconstruction, the IWT performs an integer-to-integer mapping, thereby preserving the original pixel precision and enabling lossless reconstruction of the transformed image. This property minimizes numerical distortion after repeated transform and inverse transform operations, contributing to higher visual quality of the watermarked image, in addition, it prepares the coefficients for the proposed bits' substitution algorithm.

Because a chaotic system has better security features than traditional deterministic or pseudo-random embedding techniques, it is used to regulate the watermark embedding process in the prepared IWT coefficients. The chaotic system is a mathematical model based on a nonlinear time series and exhibits unpredictable behavior based on simple initial conditions, which generate random and unpredictable keys, making them ideal and suitable for enhancing information security. They are widely used in multiple fields such as cryptography and image processing, where the generated sequences can greatly improve data protection by accurately identifying the locations where watermarks are embedded. Even though the embedding sites are determined by the chaotic sequence, its selection is driven by a number of intrinsic characteristics, such as a vast key space, severe sensitivity to beginning conditions, and pseudo-random behaviour. These features guarantee that even a slight alteration in the secret key results in an entirely different embedding pattern, greatly increasing the difficulty of detecting or extracting watermarks without authorization.

Consequently, the combination of the lifting-based IWT and chaotic embedding control achieves an effective balance between imperceptibility, robustness, computational efficiency, and security, making it particularly suitable for secure facial image authentication.

To generate recovery bits, Bicubic interpolation has been applied as in [42,43]. The generated bits are embedded in the RONI using the proposed Chaotic-based Bit Substitution Algorithm (CBSA). By incorporating the proposed algorithms, the embedding capacity is greatly increased, allowing the scheme to support images that previously failed under existing FIA methods due to limited capacity. This improvement enhances the security, reliability, and applicability of FIA across a wider range of images.

Table 1.1. Comparison of the state-of-the-art schemes

Ref.	Embedding domain/methodology	Region of embedding	Embedding capacity (bpp)
------	------------------------------	---------------------	--------------------------

[30]	Transform domain / SVD + DWT	RONI	0.0469
[31]	Transform domain / IWT + SLT	ROI carries patient's data RONI carries authentication data	0.25
[32]	Spatial and Transform domain / LSB for ROI IWT + SVD for RONI	ROI carries patient's data RONI carries authentication data	0.0234
[33]	Transform domain / IWT + SVD	ROI (authentication watermark), RONI (visible watermark)	0.2
[34]	Transform domain / DWT + Schur	RONI	0.0625
[35]	Transform domain / IRCT	Entire image	0.36
[36]	Transform domain / I-IWT	Entire image (all subbands of the transformed image).	0.3494
[41]	Transform domain / SLT + FIA	RONI	0.25
[42]	Transform domain / SLT + Bicubic + FIA	RONI	0.25
[43]	Transform domain / SLT + FIA + Adjacent embedding	RONI	0.37
[44]	Transform domain / SLT + FIA + Adjustable threshold and block size	RONI	0.25

The main contributions of this work include:

1. Increased embedding capacity: The proposed CBSA enhances the storage capacity thus enabling the protection of more images that were previously unsupported due to the limited embedding space.
2. Improved security: By utilizing a chaotic system, the scheme achieves higher security while embedding data bits in the carrier blocks.
3. Better quality: The proposed scheme maintains higher visual quality of the watermarked images compared to previous FIA techniques.
4. Enhanced applicability: The improved embedding capacity and security ensure that the proposed method is applicable to a broader range of image types, including those with complex textures or high-resolution features, which were previously difficult to protect.

The remainder of the paper includes Section 2, offers a detailed explanation of the proposed Enhanced-FIA (E-FIA) scheme. Section 3 presents the experimental results and their discussions, and **Section 4** concludes this research.

2. PROPOSED SCHEME

The proposed scheme employs two major algorithms one of them is used at the sender side to generate the watermarked image from the input face image, and the other one is used at the receiver side to extract the embedded data from the watermarked image and perform the authentication procedure. The algorithms at both sides start by reading the input face image and applying the Face Region Separation (FRS) process. To reduce the amount of data generated from the selected face region (FR), the Bicubic Interpolation (BI) algorithm is applied. Then, a Chaotic System (CS) is applied to generate a chaotic sequence that specifies the locations for data embedding. Thereafter, the channels of the RGB (i.e., Red, Green, Blue) color image are separated and each channel is divided into blocks of size (16×16) pixels. The blocks that are outside the selected FR, are transformed using IWT where the resultant coefficients are divided into four sub-bands: Low-Low (LL), High-Low (HL), Low-High (LH), and High-High (HH). The data is embedded in the HL and LH sub-bands to achieve high quality and robustness. The following subsections illustrate the details of the proposed algorithms.

2.1. Region Separation

In the proposed scheme, the FRS process is applied at the beginning of the sender and receiver sides algorithms. The process starts by reading the input image and applying the MTCNN-based algorithm to detect FR. The selected FR is called ROI and the remaining part of the image is called RONI. A binary mask image is generated in which the pixels at ROI positions are set to ones and the pixels at RONI positions are set to zeros as shown in Figure 1. The generated mask image and the original image channels are divided into (16×16) blocks, followed by the classification of the channel's blocks as follows:

$$\text{Average of mask image block } (i,j) \begin{cases} = 0 & \text{block } (i,j) \in \text{RONI} \\ \neq 0 & \text{block } (i,j) \in \text{ROI} \end{cases}$$

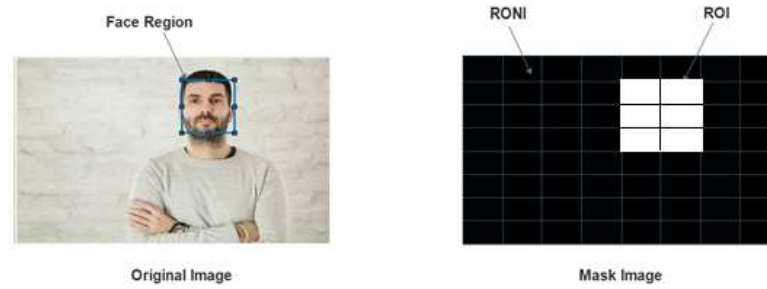


Fig. 1. Mask image generated using MTCNN-based algorithm

2.2. Recovery Data Generation

After the image is divided into ROI and RONI, the BI algorithm is applied to the ROI with a scale (0.5) to reduce the data size in the embedding process as shown in Figure 2. The resultant pixels are converted to binary sub-sequences each of length 8 bits. Then, the binary sub-sequences are concatenated into one binary sequence.

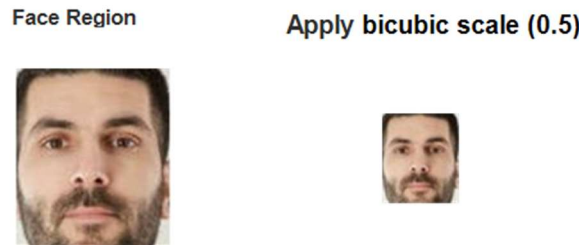


Fig. 2. Bicubic interpolation on ROI with a scale (0.5)

2.3. Chaotic Sequence Generation

Chaotic Sequence Generation (CS) is widely used in information hiding due to their sensitivity to initial conditions and pseudo-random behaviour thus can enhance the security and imperceptibility of the embedded data. In this work, a chaotic system is employed to generate a chaotic sequence, which is then utilized to determine the embedding locations of secret bits within the coefficients of the RONI blocks. By initializing the system with specific parameters, a sequence of values is produced and mapped to pixel positions, ensuring a secure and unpredictable embedding process.

The initialization process of the chaotic map starts with a secret key, K , to guarantee the security and repeatability of the proposed E-FIA scheme. Crucially, the created sequence is made to prevent index recurrence, guaranteeing that every embedding position is distinct and non-overlapping. This keeps the integrity of the embedded data and the host picture intact and avoids conflicts during the embedding process. The security of the entire process hinges on K

which acts as the seed for producing the chaotic sequence. The control parameter μ and the initial value S_1 are generated by applying the SHA-256 hash function to the key K . The resulting 256-bit hash value is then partitioned, and a 128-bit segment is normalized to map μ into the desired chaotic range of the logistic map. The formula used is:

$$\mu = 3.57 + 0.43 \times \frac{\text{decimal}(H_\mu)}{2^{128}} \quad (2.1)$$

where H_μ , represents the 128-bit segment of the hash designated for generating μ , thus, mapping the control parameter to the range $[3.57, 4.0]$. This specific range is widely recognized in the literature for producing the highly unstable and non-periodic behavior essential for secure and unpredictable sequence generation. For experimental tests of the E-FIA scheme, $\mu = 3.8$ has been set which provides a good balance between complexity and computational stability.

Additionally, the system starts with $S_1 = 0.5$, which is in the middle of the chaotic interval. This decision maximizes the sensitivity to beginning conditions by avoiding convergence to fixed spots or periodic orbits that might happen close to the map's edges. To ensure that the generated values are entirely inside the intended pseudo-random regime, a delay factor $t = 2$ is used to avoid unstable transients that arise during the initial few rounds of the chaotic sequence. Beyond this point, increasing t resulted in a loss of some computational efficiency but no discernible increase in statistical entropy. The sequence length $P = 128$ is chosen to match the maximum embedding capacity per 16×16 carrier block. While maintaining non-redundancy and preventing collisions in index mapping, this alignment between sequence length and data payload guarantees full use of embedding space.

The mathematical representation of the CS is given in equation (2.2) as follows [46]:

$$S_n = \text{mod} \left(\mu S_{n-1} * (1 - S_{n-1}) + (4 - \mu) * \frac{\sin(\pi S_{n-1})}{4}, 1 \right) \quad (2.2)$$

where μ is the control parameter whose chaotic range is $[0, 4]$.

The proposed CSG algorithm starts by reading the input parameters (μ , t , S_1 , P) where μ refers to the control parameter that determines the system's behavior, t refers to the delay to avoid unstable values at the beginning of the chaotic sequence, S_1 refers to the initial value of the sequence, and P refers to the desired length of the chaotic sequence. The output of the algorithms is the Quantized Chaotic sequence (Q_k) of length P values. The resultant Q_k sequence will be used at the embedding procedure to specify the locations at which the bits are embedded. The algorithm can be summarized as follows:

The proposed CSG algorithm

Input: μ , t , S_1 , P .

Output: Quantized Chaotic sequence (Q_k).

Step1: Generate the Chaotic Sequence:

Start with the initial value S_1 , then compute subsequent values using the logistic map equation (2.3) as follows:

$$S = (S_{t+1}, S_{t+2}, \dots, S_{t+p}), \text{ where } S = \{S_{t+u} | u \in [1, p]\} \quad (2.3)$$

Step 2: Quantize the generated S sequence using equations (2.4) and (2.5) as follows:

$$q = \text{floor}(S_{t+u} \times 10^{14}) \quad (2.4)$$

$$Q = (\text{mod}(q, 3)) + 1 \quad (2.5)$$

Step 3: Return the resultant quantized sequence of length P using equation (2.6) follows:

$$Q_k = (Q_{t+1}, Q_{t+2}, \dots, Q_{t+p}) \quad (2.6)$$

2.4. Data Embedding Procedure

In the proposed scheme, the IWT is used to transform the RONI blocks and the data bits are embedded in HL and LH subbands of the resultant coefficients. Then the proposed chaotic-based embedding process is performed in which a data bit is selected from the secret sequence and a position is selected from Q_k , thereafter, the IWT coefficient is converted to binary and the secret bit is embedded at the selected position. After embedding the data bits in the HL and LH coefficients, the inverse IWT is applied to each modified RONI block to obtain the watermarked RONI block. The procedure of data bits embedding in RONI blocks is shown in Figure 3. For example, if an IWT coefficient is 209, and the bit to be embedded is '1', and the embedding position in Q_k is 3, then the watermarked coefficient is 213. This is achieved by modifying the third bit in the binary representation of 209 by replacing '0' with '1' as illustrated in Figure 3.

The resultant watermarked RONI blocks and the original ROI blocks are reorganized to form the watermarked channel image. The embedding procedure is repeated for the two remaining channels to obtain the other two watermarked channels. The final watermarked channel image is constructed from the three watermarked channels. The procedure of the main embedding algorithm can be summarized as shown in Figure 4 and the details of the algorithm are as follows:

Step 1: Let the original face image (I_{org}) of size ($M \times N \times 3$), where M and N represent the height and width of the image. Apply MTCNN to generate binary mask image that is used for splitting the image blocks into two groups called ROI blocks and RONI blocks.

Step 2: Compress the ROI (face area) using bicubic interpolation algorithm with a scale factor of 0.5, as discussed in Section 2.2. Then, generate the Binary Sequence (BS) for ROI recovery.

Step 3: Apply the Integer Wavelet Transform (IWT) on the RONI blocks, obtaining four sub-bands: LL, LH, HL, and HH.

Step 4: Read a 128-bit window from the Binary Sequence (BS) and embed it into the LH and HL sub-bands of the RONI using chaotic-based embedding technique, as described in Section 2.3. Repeat this process until all BS bits are embedded.

Step 5: Perform the inverse IWT to reconstruct the watermarked channel image (I_{wchl})

Step 6: Repeat Steps 2 to 5 to construct the watermarked version of the remaining two channels.

Step 7: Reconstruct the watermarked face image I_w by combining the three watermarked channels.

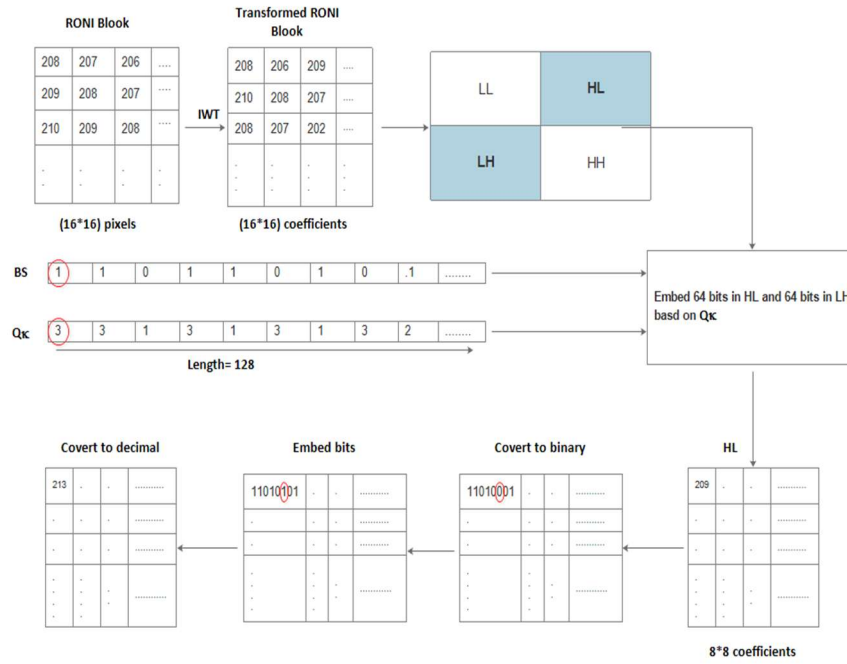


Fig. 3. Numerical example of data embedding in RONI block

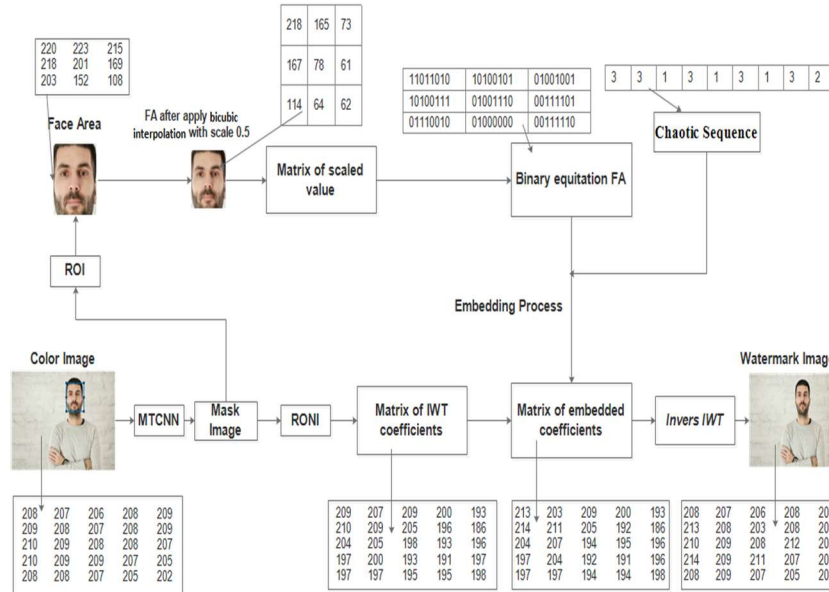


Fig. 4. Block diagram of the proposed embedding algorithm

2.5. Data Extraction and Image Authentication Procedure

The data extraction process is performed to extract the embedded bits from the watermarked RONI blocks where IWT is first applied to the to obtain the coefficients. Then HL and LH sub-bands are then selected to retrieve the embedded Binary Sequence (BS). For each coefficient, the extraction is performed by identifying the bit position from Q_k and reading the corresponding bit from the binary representation of the coefficient.

For example, if the extracted coefficient is 213, and the bit position determined is 3, then the third bit in the binary representation of 213 is retrieved. Since 213 (in binary: 11010101) has '1' in the third position, the extracted bit is '1'. This process is repeated for all coefficients to reconstruct the original BS, as illustrated in Figure 5.

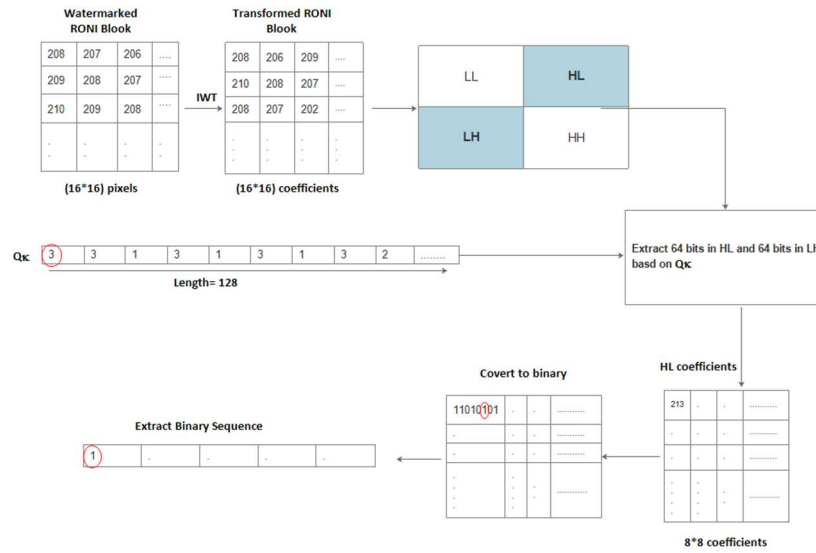


Fig. 5. Numerical example of data extraction from RONI block

The procedure of the proposed data extraction and image authentication is illustrated in Figure 6 and the steps can be summarized as follows:

Step 1: Let the original face image (I_W) of size $(M \times N \times 3)$, where M and N represent the height and width of the image. Apply MTCNN to generate binary mask image that is used for splitting the image blocks into two groups called ROI blocks and RONI blocks.

Step 2: Compress the ROI using bicubic interpolation algorithm with a scale factor of 0.5. Then, generate the binary sequence (b_s) from I_W for comparison with the Extracted Binary Sequence (BSE) from the RONI blocks.

Step 3: Apply IWT on the watermarked RONI blocks, obtaining four sub-bands: LL, LH, HL, and HH.

Step 4: Extract the bits from the HL and LH coefficients as explained in the extraction process at the beginning of this subsection.

Step 5: Compare the Extracted Binary Sequence (BSE) with the ROI binary sequence b_s (generated from step 2) as follows:

- If $BSE = b_s$, the image is authentic and the algorithm stops here.
- If $BSE \neq b_s$, the image is not authentic and the algorithm continues.

Step 6: The entire face region of the channel image is reconstructed using the extracted BSE, then bicubic interpolation with scale (2) is applied to retrieve the original size of the face region. The tampered face region in I_W is replaced with the recovered face region.

Step 7: Repeat step 6 to reconstruct the remaining channels.

Step 8: Reconstruct the recovered face image by combining the three watermarked channels.

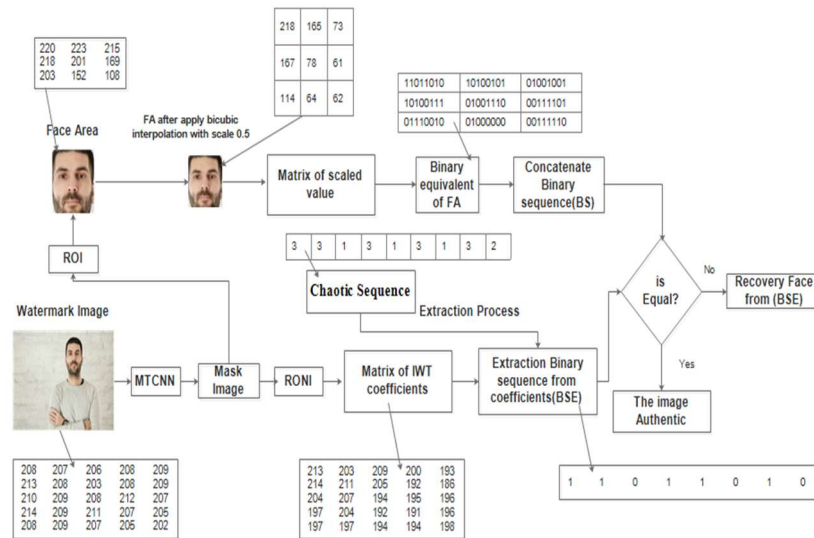


Fig. 6. Block diagram of the proposed data extraction and image authentication algorithm

3. RESULTS AND DISCUSSION

The following subsections present the description of the selected dataset followed by the experimental tests for authentication, visual quality, capacity, payload, and execution time where the experiments have been applied in a computer with the following properties: 1.80 GHz Intel® Core TM i7 CPU and 16 GB memory using MATLAB (R2020a). Thereafter, comparisons with the state-of-the-art schemes are presented which proved the efficiency of the proposed E-FIA scheme in terms of visual quality, capacity, and applicability.

3.1. Dataset Description

The experimental dataset consists of 70 facial images collected from the publicly available datasets containing images with diverse facial characteristics, including variations in facial size, pose, expression, illumination conditions, image resolution, and background, providing representative test cases for FIA [47,48]. The selected images were separated into two groups according to the evaluation objective. The first group contains 50 challenging images with relatively large facial regions, which generate larger watermark payloads. These images were intentionally selected to evaluate the proposed high-capacity watermarking scheme because several existing methods were unable to embed the generated watermark due to their limited embedding capacities. The second group contains 20 images that satisfy the embedding capacity constraints of the compared methods and were therefore used exclusively for quantitative comparison under identical experimental conditions.

3.2. Authentication of ROI

The proposed scheme was tested on a set of images to identify tampering in ROI and recover the face region after detecting tampering in the watermarked image. By applying the authentication procedure that has been explained in the proposed E-FIA scheme, the bits extracted from the RONI are compared with the bits obtained from the ROI of the watermarked image. The bits are identical when an authentic watermarked image is received, otherwise, the image is not authentic. Figure 7 shows examples of image tampering, authentication, and recovery processes.

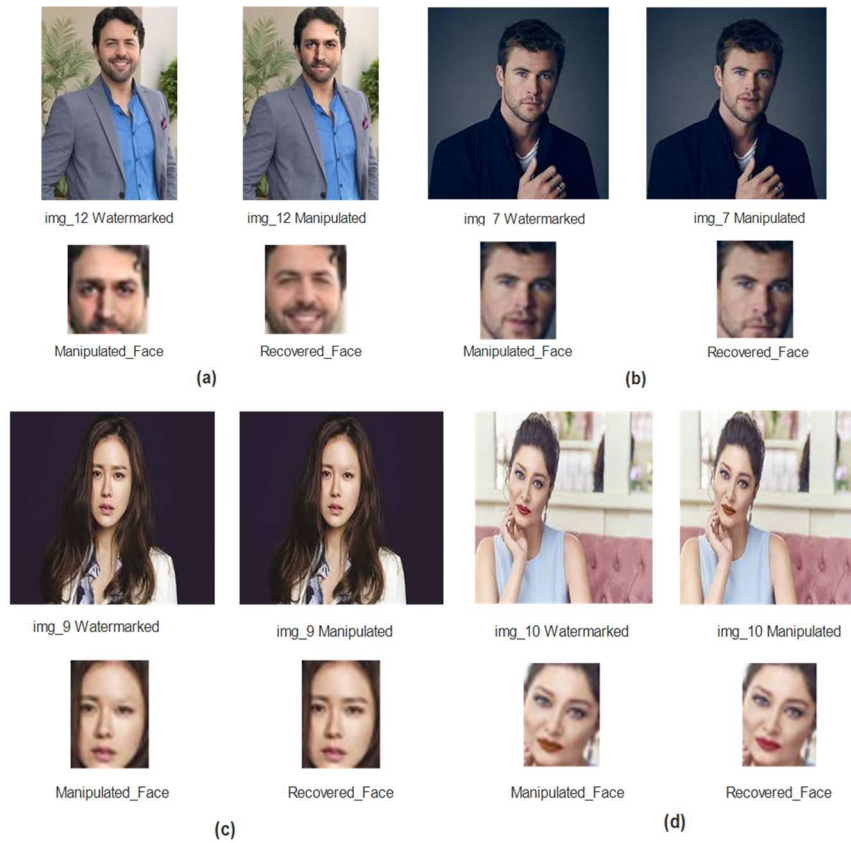


Figure 7. Samples of manipulations and recovery of the ROI after: (a) face swap attack, (b) expression swap attack, (c) attributes attack, and (d) retouching attack

3.3. Visual Quality

To test the visual quality after watermarking the test images are watermarked using the proposed E-FIA scheme, the Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), and Similarity Index Measure (SSIM) have been calculated and the outcomes are as shown in Table 3.1. The results proved that the watermarked images have high visual quality results. The visual quality depends on the size of ROI, the larger the size of the ROI to the size of the image, the lower the visual quality. Samples of the watermarked images are shown in Figure 8 which proved the efficiency of the proposed E-FIA scheme in embedding authentication data in the face image without generating visual artifacts.

To demonstrate the reproducibility and stability of the proposed E-FIA scheme, descriptive statistical analysis was performed over the 50-image group of the evaluation dataset. The confidence interval (CI) with 95 % certainty has been calculated using:

$$CI = x \pm 1.96 \left(\frac{\sigma}{\sqrt{N}} \right) \quad (3.1)$$

with x denoting the sample mean, σ the standard deviation (Std), and N the number of tested images. The statistical results for the test images are shown in Table 3.2. The proposed method achieved an average PSNR of 49.38 ± 0.48 dB, an average SSIM of 0.9962 ± 0.0024 , and an average MSE of 0.7540 ± 0.0796 . The narrow confidence intervals and low standard deviations indicate that the proposed watermarking scheme provides consistent and stable performance across different facial images.

Table 3.1. Visual quality of the watermarked images using the E-FIA

Image name	Image size	Size of ROI	PSNR (dB)	MSE	SSIM
img_1	236×213×3	80× 64×3	48.9813	0.8221	0.9953
img_2	227×222×3	80×64 ×3	49.104	0.7992	0.996
img_3	192×262×3	80×64 ×3	49.0424	0.8107	0.999
img_4	194×259×3	64× 64×3	50.0375	0.6447	0.9952
img_5	194×259×3	80× 64×3	48.9922	0.8201	0.9957
img_6	183×275×3	64× 64×3	50.0142	0.6481	0.9943
img_7	225×225×3	80× 64×3	49.0854	0.8027	0.9977
img_8	266×190×3	80×64 ×3	49.0871	0.8024	0.9958
img_9	184×274×3	80×64 ×3	48.956	0.827	0.9945
img_10	183×275×3	80×64 ×3	49.1116	0.7978	0.9957
img_11	182×276×3	80× 64×3	49.0249	0.8139	0.9925
img_12	259×194×3	64×64 ×3	49.9952	0.651	0.9982
img_13	237×213×3	64× 64×3	49.9697	0.6548	0.9966
img_14	251×201×3	64×64×3	49.9852	0.6525	0.9948
img_15	179×281×3	64×64×3	50.0038	0.6497	0.9978
img_16	192×262×3	64×64×3	49.9934	0.6512	0.9994
img_17	168×300×3	80×64×3	49.1167	0.7969	0.998
img_18	265×190×3	80×64×3	49.0641	0.8066	0.9997
img_19	192×262×3	80×64×3	49.0868	0.8024	0.9928
img_20	240×210×3	80×64×3	49.0059	0.8175	0.9953

Table 3.2. Visual quality statistical results using E-FIA

Metric	N	Mean	Std	Min	Max	CI
PSNR (dB)	50	49.38211417	0.476796616	48.78263393	50.34224845	49.38 ± 0.48 dB
MSE	50	0.753995166	0.079626025	0.600973768	0.860630965	0.7540 ± 0.0796
SSIM	50	0.996231557	0.00242502	0.989556875	0.999743952	0.9962 ± 0.0024

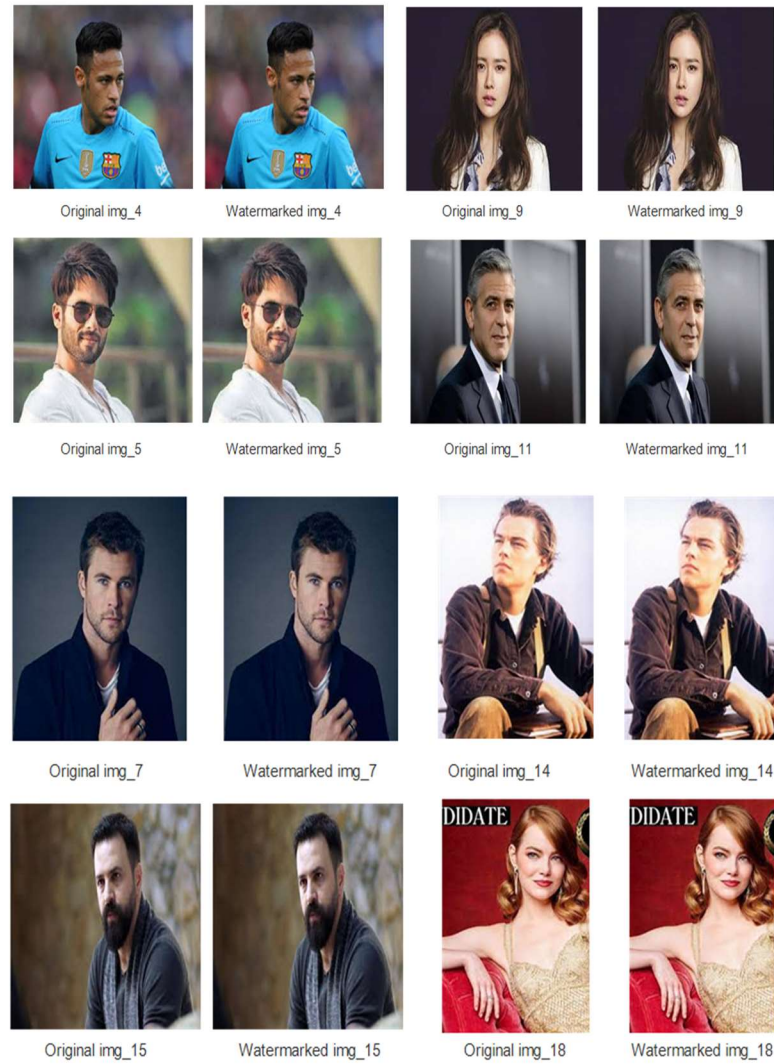


Fig. 8. Sample watermarked images using E-FIA scheme

3.4. Capacity and Payload

Embedding Capacity (EC) and Payload are important factors to evaluate the performance of the proposed scheme. These tests aim to measure the amount of data that can be included in the watermarked image without affecting the image quality. Table 3.3 shows the results where the EC is calculated by multiplying the number of RONI blocks by 128 bits because each block can carry 128 bits. The total payload refers to the total number of bits that are generated from the recovery data and embedded in the RONI.

Table 3.3. Capacity and Payload Results

Image name	RONI blocks	EC (bits)	Payload for Single channel (bits)	Total payload (bits)
img_1	152×3	58368	10240	30720
img_2	152×3	58368	10240	30720
img_3	162×3	62208	10240	30720
img_4	167×3	64128	8192	24576
img_5	162×3	62208	10240	30720
img_6	162×3	62208	8192	24576
img_7	166×3	63744	10240	30720
img_8	151×3	57984	10240	30720
img_9	157×3	60288	10240	30720
img_10	157×3	60288	10240	30720
img_11	157×3	60288	10240	30720
img_12	167×3	64128	8192	24576

img_13	162×3	62208	8192	24576
img_14	155×3	59520	8192	24576
img_15	162×3	62208	8192	24576
img_16	172×3	66048	8192	24576
img_17	150×3	57600	10240	30720
img_18	152×3	58368	10240	30720
img_19	162×3	62208	10240	30720
img_20	165×3	63360	10240	30720

3.5. Execution Time

To test the execution time of the proposed scheme, which is an important factor to prove the applicability of the implemented algorithms, MATLAB's built-in timing functions, tic and toc have been employed to measure the execution times of the watermark embedding and extraction processes. Table 3.4 summarizes the relationship between the ROI size, total payload, and the corresponding execution times. The experimental results indicate that the proposed scheme achieves consistently low processing times despite variations in the embedded payload. The evaluated images contain two ROI sizes, namely $64 \times 64 \times 3$ and $80 \times 64 \times 3$, corresponding to payloads of 24,576 bits and 30,720 bits, respectively. As expected, images with the larger ROI generally require longer embedding and extraction times because additional image blocks and transform coefficients must be processed during watermark insertion and recovery. For example, Image 'img_18', which contains a payload of 30,720 bits, required the longest embedding time of 0.3398 s, while Image 'img_6', with a payload of 24,576 bits, achieved one of the shortest embedding times of 0.2151 s. Similarly, the extraction time varied from 0.1370 s for 'img_6' to 0.2741 s for 'img_17'. For the examined '50 images' dataset, the proposed scheme needed an average embedding time of 0.3188 seconds and an average extraction time of 0.2252 seconds. These findings show that the suggested watermarking methodology supports comparatively high embedding capacities with only a small computational overhead. As a result, the suggested method is computationally effective and ideal for real-world FIA applications that call for quick watermark embedding and verification.

Table 3.4. Execution time test for embedding and extraction algorithms

Image name	Size of ROI	Total payload (bits)	Embedding time (seconds)	Extraction time (seconds)
img_1	$80 \times 64 \times 3$	30720	0.21805106	0.17242562
img_2	$80 \times 64 \times 3$	30720	0.34343674	0.24573818
img_3	$80 \times 64 \times 3$	30720	0.27307805	0.14844764
img_4	$64 \times 64 \times 3$	24576	0.33856559	0.16326878
img_5	$80 \times 64 \times 3$	30720	0.33903408	0.24541448
img_6	$64 \times 64 \times 3$	24576	0.21507858	0.13702264
img_7	$80 \times 64 \times 3$	30720	0.33305993	0.26957405
img_8	$80 \times 64 \times 3$	30720	0.22327616	0.14671358
img_9	$80 \times 64 \times 3$	30720	0.33882084	0.25087169
img_10	$80 \times 64 \times 3$	30720	0.31779670	0.15936861
img_11	$80 \times 64 \times 3$	30720	0.23350304	0.14374434
img_12	$64 \times 64 \times 3$	24576	0.33194068	0.21419788
img_13	$64 \times 64 \times 3$	24576	0.30138191	0.17092257
img_14	$64 \times 64 \times 3$	24576	0.25611080	0.17402263
img_15	$64 \times 64 \times 3$	24576	0.33330029	0.21975446
img_16	$64 \times 64 \times 3$	24576	0.29197091	0.13822570
img_17	$80 \times 64 \times 3$	30720	0.27493161	0.27406032
img_18	$80 \times 64 \times 3$	30720	0.33983752	0.15037833
img_19	$80 \times 64 \times 3$	30720	0.31672524	0.25123132
img_20	$80 \times 64 \times 3$	30720	0.24322542	0.16624226
Average time (seconds) for "50 images" dataset			0.31877503	0.22520050

3.6. Comparisons with the State-of-the-Art

To highlight the superiority of the proposed scheme, the comparative analysis is organized into two balancing perspectives. The first subsection presents a quantitative comparison with representative watermarking-based FIA methods, including the previous FIA and I-FIA schemes [41-s43], since these methods address the same authentication problem under similar assumptions and performance metrics. This comparison enables a direct assessment of improvements in embedding capacity, image quality, authentication accuracy, and computational performance.

The second subsection provides a general comparison with deep learning-based facial image authentication and forgery detection approaches. Although these methods represent an important division of the current state-of-the-art intelligent image authentication, they differ fundamentally from watermarking-based schemes in their underlying methodology. Deep learning approaches typically rely on large annotated training datasets, computationally intensive model training, and inference using pre-trained neural networks, whereas the proposed scheme performs authentication through watermark verification without requiring any training process or large-scale datasets. Consequently, a direct quantitative comparison would not constitute a fair evaluation. Instead, this subsection discusses the relative strengths, limitations, and application scenarios of both paradigms, thereby positioning the proposed method within the broader context of contemporary FIA research.

3.6.1. Comparison with the Previous FIA Schemes

In this section, the proposed scheme is compared with previous schemes [41-43] in terms of EC and visual quality. The embedding capacity depends on the number of RONI and the number of bits that can be embedded in each block. The proposed scheme shows high improvements over the previous schemes, as shown in Table 3.5. Where 128 bits are embedded in the IWT coefficients in the sub-bands (LH, HL) within each block of size (16*16) pixels, compared to the previous schemes I-FIA which includes 96 bits in the sub-bands (LH, HL, HH), and the FIMD and FIA schemes which include 64 bits in the sub-bands (LH, HL) within a single block of size (16×16) pixels. The same test images used in schemes [41-43] are used in this test which are shown in Figure 9.

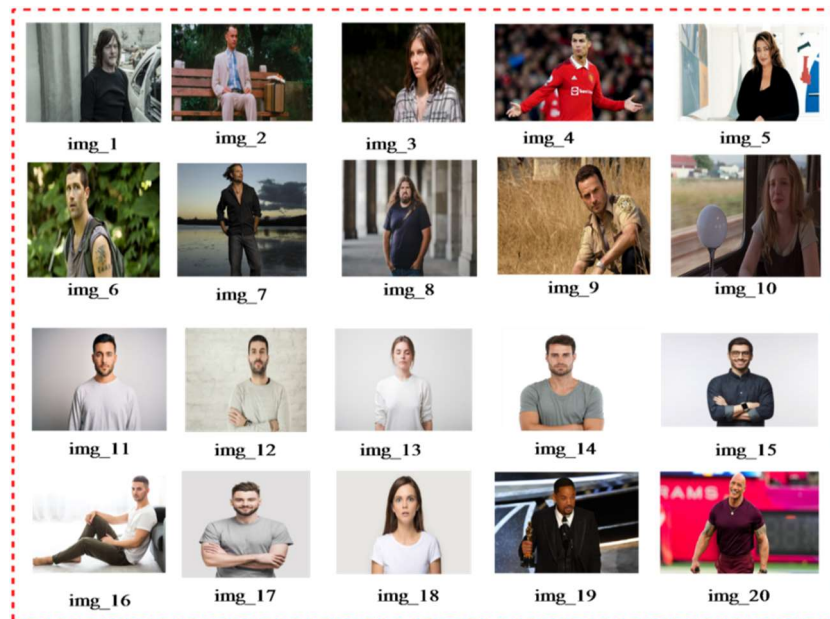


Fig. 9. Sample test images for comparisons schemes [41–43]

Table 3.5. Comparison of capacity for sample test images

Image name	Image size	Size of the face area	Capacity of FIMD [41]	Capacity of FIA [42]	Capacity of I-FIA [43]	Capacity of E-FIA
img_1	570×1014×3	160×128×3	404352	404352	606528	808704
img_2	600×1200×3	112×80×3	523584	523584	785376	1047168
img_3	1152×2048×3	432×384×3	1639872	1639872	2459808	3279744
img_4	1152×2048×3	288×224×3	1714752	1714752	2572128	3429504
img_5	536×1024×3	144×144×3	386304	386304	579456	772608
img_6	600×1200×3	224×192×3	495360	495360	743040	990720
img_7	640×800×3	80×64×3	378240	378240	567360	756480
img_8	1669×2500×3	256×224×3	3069312	3069312	4603968	6138624
img_9	455×728×3	128×128×3	226368	226368	339552	452736
img_10	608×1080×3	224×176×3	454272	454272	681408	908544
img_11	360×540×3	112×80×3	130176	130176	195264	260352
img_12	408×612×3	112×96×3	171648	171648	257472	343296
img_13	339×509×3	80×64×3	119232	119232	178848	238464
img_14	365×473×3	112×80×3	113280	113280	169920	226560
img_15	408×612×3	96×80×3	174336	174336	261504	348672
img_16	351×492×3	64×48×3	117120	117120	175680	234240
img_17	612×506×3	128×112×3	212352	212352	318528	424704
img_18	339×509×3	128×96×3	112896	112896	169344	225792
img_19	1667×2500×3	464×384×3	2971008	2971008	4456512	5942016
img_20	742×1320×3	160×128×3	27072	27072	1057824	1410432

Table 3.6 presents the visual quality comparison which proved that the E-FIA scheme obtained higher visual quality results compared to previous schemes. In addition, the proposed scheme obtained narrow CI results compared to FIA and I-FIA schemes resulting in performance that is remarkably consistent across a variety of images. This statistical data demonstrates that the suggested scheme offers consistent embedding behaviour and dependable perceptual quality under various image situations. The proposed E-FIA scheme demonstrates a significant improvement in embedding capacity compared to previous schemes. The proposed method achieves an embedding capacity of 0.5 bpp, whereas schemes [30-35], [41-44] achieve embedding capacities between 0.02 bpp to 0.37 bpp. Table 3.7 provides a comprehensive comparison across different FIA schemes.

Table 3.6. Comparison of visual quality for sample test images

Image name	I-FIA [43]		FIA [42]		E-FIA	
	PSNR (dB)	Payload	PSNR (dB)	Payload	PSNR (dB)	Payload
img_1	48.9278	171072	45.0347	170880	53.6385	122880
img_2	56.6902	74880	54.0723	74880	58.2047	53760
img_3	46.59	1379520	44.3761	1379520	50.9363	995328
img_4	48.7514	537408	48.2209	537216	54.7857	387072
img_5	43.5744	173088	42.1832	172992	53.3869	124416
img_6	48.719	358560	46.1039	358464	51.4087	258048
img_7	56.2599	42912	53.1853	43008	59.0923	30720
img_8	58.637	477216	56.3953	477120	57.7784	344064
img_9	42.3823	136800	38.2976	136896	52.2256	98304
img_10	49.933	328608	46.1612	328512	51.3714	236544
img_11	49.0912	74880	47.2324	170880	52.5324	53760
img_12	50.5864	89856	48.0929	89856	52.8369	64512
img_13	52.5211	42912	49.9867	43008	54.5718	30720
img_14	40.0546	74880	39.1851	74880	52.2835	53760
img_15	51.2567	64224	49.6399	64320	54.2926	46080
img_16	42.9934	25920	42.8503	25920	57.0702	18432

img_17	50.4725	119808	47.5625	119808	52.3634	86016
img_18	44.7854	102816	42.5819	102720	50.8493	73728
img_19	48.8336	1482624	46.0244	1482432	52.7686	1069056
img_20	46.1141	171072	45.807	170880	55.9908	122880
CI	48.88 ± 2.34		46.69 ± 2.09		53.92 ± 1.10	

Table 3.7. General comparison with previous FIA schemes

Property	FIMD [41]	FIA [42]	I_FIA [43]	E_FIA
Method	SLT-based Watermarking	SLT-based Watermarking + bicubic interpolation algorithm	SLT-based Watermarking + bicubic interpolation algorithm + EAC algorithm + BSE algorithm	Lazy wavelet-based Watermarking + bicubic interpolation algorithm + Chaotic-based Bit Substitution Algorithm (CBSA)
Various manipulations	✓	✓	✓	✓
Manipulation detection ability	✓	✓	✓	✓
Face region recovery	✗	✓	✓	✓
Capacity	$EC \text{ (bits)} = \text{total number of } RONI \times 64$ $EC \text{ (bpp)} = 0.25$	$EC \text{ (bits)} = \text{total number of } RONI \times 64$ $EC \text{ (bpp)} = 0.25$	$EC \text{ (bits)} = \text{total number of } RONI \times 96$ $EC \text{ (bpp)} = 0.37$	$EC \text{ (bits)} = \text{total number of } RONI \times 128$ $EC \text{ (bpp)} = 0.5$

3.6.2. General Comparison with Deep Learning-Based Authentication

The recent deep learning-based facial authentication and forgery detection methods have demonstrated high detection accuracy under various manipulation scenarios. Nevertheless, these approaches typically require large-scale annotated training datasets, extensive model training, and considerable computational resources during both training and inference. In contrast, the proposed scheme belongs to the class of watermarking-based authentication methods, which authenticate image integrity by verifying embedded watermark information without any prior training process. Since the objectives, computational models, and evaluation protocols of these two categories are fundamentally different, direct quantitative comparisons may not provide a fair assessment. However, a general comparison is shown in Table 3.8 to highlight the major differences between the watermarking-based FIA and the deep learning-based FIA schemes.

Table 3.8. General comparison with deep learning-based FIA schemes

Feature	Watermarking-Based FIA Authentication	Deep Learning-Based FIA Authentication
Training required	No	Yes
Large dataset required	No	Yes
Authentication mechanism	Watermark verification	Learned feature representation
Computational complexity	Low	High
Suitable for edge/IoMT devices	Yes	Limited
Detects image integrity	Yes	Usually yes
Model retraining	Not required	Often required

5. CONCLUSIONS

This paper presents an enhanced face image authentication (E-FIA) scheme designed to detect tampering and recover the original face region. The face image is divided into two parts (i.e., ROI and RONI). To improve capacity and enable more data to be included across a larger

number of images, the proposed scheme uses lazy wavelet transform and chaotic-based bit substitution algorithm (CBSA) to embed authentication data into each block of (16×16) pixels from the RONI. The proposed algorithm achieves a payload capacity of 0.5 bpp, outperforming various previous schemes, and allows for more comprehensive image protection. In addition, the experimental results demonstrate improved visual quality and less distortion in watermarked face images compared to existing methods. The use of CBSA increased the security of the data embedding process thus the proposed E-FIA is highly recommended for practical applications. Future research may focus on developing an improved algorithm with greater embedding capacity.

FUNDING

No fund available for this study.

ACKNOWLEDGEMENTS

The authors would like to thank College of Engineering in Al-Iraqia University for encouraging and supporting their scientific research.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

- [1] Thabit, R. (2019) Multi-biometric watermarking scheme based on interactive segmentation process, *Periodica Polytechnica Electrical Engineering and Computer Science*, **63**(4), 263–273. doi: 10.3311/PPee.14219
- [2] Manivannan, D. & Brindha, M. (2022) Secure image cloud storage using homomorphic password authentication with ECC based cryptosystem, *Advances in Systems Science and Applications*, **22**(1), 92–116. doi: 10.25728/assa.2022.22.1.1175
- [3] Sharma, S., Zou, J. J., Fang, G., Shukla, P. & Cai, W. (2024) A review of image watermarking for identity protection and verification, *Multimedia Tools and Applications*, **83**(11), 31829–31891. doi: 10.1007/s11042-023-16843-3
- [4] Muhuri, P. K., Ashraf, Z. & Goel, S. (2020) A novel image steganographic method based on integer wavelet transformation and particle swarm optimization, *Applied Soft Computing*, **92**, 106257. doi: 10.1016/j.asoc.2020.106257
- [5] Thabit, R. (2019) Improved steganography techniques for different types of secret data, *Advances in Systems Science and Applications*, **19**(3), 38–51. doi: 10.25728/assa.2019.19.3.724
- [6] Gull, S. & Parah, S. A. (2024) Advances in medical image watermarking: A state-of-the-art review, *Multimedia Tools and Applications*, **83**(1), 1407–1447. doi: 10.1007/s11042-023-15396-9
- [7] Thabit, R., Fadhil, H. M., Fakhruddin, H. F., Shather, A. H. & Al-Askari, M. A. (2024) A new face swap detection technique for digital images, *Advances in Systems Science and Applications*, **24**(1), 142–162. doi: 10.25728/assa.2024.24.1.1378
- [8] Shi, H., Yan, K., Geng, J. & Ren, Y. (2024) A cross-embedding based medical image tamper detection and self-recovery watermarking scheme, *Multimedia Tools and Applications*, **83**(10), 30319–30360. doi: 10.1007/s11042-023-16679-x

- [9] Hu, F., Cao, H., Su, Q., Wang, G. & Yao, T. (2023) EBOF: A fusion-domain color image watermarking scheme based on approximate Hessenberg factorization, *Optik*, **287**, 171084. doi: 10.1016/j.ijleo.2023.171084
- [10] Kishore, R. R. (2020) A novel and efficient blind image watermarking in transform domain, *Procedia Computer Science*, **167**, 1505–1514. doi: 10.1016/j.procs.2020.03.361
- [11] Rahman, A. U., Sultan, K., Musleh, D., Aldhafferi, N., Alqahtani, A., et al. (2018) Robust and fragile medical image watermarking: A joint venture of coding and chaos theories, *Journal of Healthcare Engineering*, **2018**, 8137436. doi: 10.1155/2018/8137436
- [12] Halshanbari, H. S. (2021) Medical image watermarking for ownership & tamper detection, *Multimedia Tools and Applications*, **80**, 16549–16564. doi: 10.1007/s11042-020-08814-9
- [13] Parah, S. A., Ahad, F., Sheikh, J. A. & Bhat, G. M. (2017) Hiding clinical information in medical images: A new high capacity and reversible data hiding technique, *Journal of Biomedical Informatics*, **66**, 214–230. doi: 10.1016/j.jbi.2017.01.006
- [14] Rakhmawati, L., Wirawan, W., Suwadi, S., Delpha, C. & Duhamel, P. (2022) Blind robust image watermarking based on adaptive embedding strength and distribution of quantified coefficients, *Expert Systems with Applications*, **187**, 115906. doi: 10.1016/j.eswa.2021.115906
- [15] Xia, Y., Hu, F., Cao, H., Tian, X. & Su, Q. (2023) A blind color image watermarking algorithm based on Hadamard transform and TLBO algorithm, *Optik*, **290**, 171277. doi: 10.1016/j.ijleo.2023.171277
- [16] Singh, A. K. (2019) Robust and distortion control dual watermarking in LWT domain using DCT and error correction code for color medical image, *Multimedia Tools and Applications*, **78**(21), 30523–30533. doi: 10.1007/s11042-018-7115-x
- [17] Bolourian Haghighi, B., Taherinia, A. H. & Harati, A. (2018) TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and halftoning technique, *Journal of Visual Communication and Image Representation*, **50**, 49–64. doi: 10.1016/j.jvcir.2017.09.017
- [18] Chen, S., Su, Q., Wang, H. & Wang, G. (2022) A high-efficiency blind watermarking algorithm for double color image using Walsh Hadamard transform, *The Visual Computer*, **38**(6), 2189–2205. doi: 10.1007/s00371-021-02277-1
- [19] Fares, K., Amine, K. & Salah, E. (2020) A robust blind color image watermarking based on Fourier transform domain, *Optik*, **208**, 164562. doi: 10.1016/j.ijleo.2020.164562
- [20] Gupta, S., Saluja, K., Solanki, V., Kaur, K., Singla, P., et al. (2022) Efficient methods for digital image watermarking and information embedding, *Measurement: Sensors*, **24**, 100520. doi: 10.1016/j.measen.2022.100520
- [21] Dwivedi, R., Awasthi, D. & Srivastava, V. K. (2024) An optimized dual image watermarking scheme based on redundant DWT and randomized SVD with Henon mapping encryption, *Circuits, Systems, and Signal Processing*, **43**(1), 408–456. doi: 10.1007/s00034-023-02479-z
- [22] Begum, M., Ferdush, J., Uddin, M. S., Islam, M. R. & Islam, M. S. (2024) Image watermarking using discrete wavelet transform and singular value decomposition for enhanced imperceptibility and robustness, *Algorithms*, **17**(1), 32. doi: 10.3390/a17010032
- [23] Begum, M., Ferdush, J. & Uddin, M. S. (2022) A hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value

decomposition, *Journal of King Saud University – Computer and Information Sciences*, **34**(8, Part B), 5856–5867. doi: 10.1016/j.jksuci.2021.07.012

[24] Yuan, Z., Liu, D., Zhang, X. & Su, Q. (2020) New image blind watermarking method based on two-dimensional discrete cosine transform, *Optik*, **204**, 164152. doi: 10.1016/j.ijleo.2019.164152

[25] Dey, A., Chowdhuri, P. & Pal, P. (2024) Integer wavelet transform based watermarking scheme for medical image authentication, *Multimedia Tools and Applications*, **83**(32), 78001–78022. doi: 10.1007/s11042-024-18183-2

[26] Thabit, R. & Khoo, B. E. (2014) A new robust reversible watermarking method in the transform domain. In: Mat Sakim, H. & Mustaffa, M. (Eds.) *Lecture Notes in Electrical Engineering* (pp. 191–201). Singapore: Springer Singapore. doi: 10.1007/978-981-4585-42-2_19

[27] Mohammed, R. T. & Khoo, B. E. (2013) Robust reversible watermarking scheme based on wavelet-like transform, *Proc. of the IEEE International Conference on Signal and Image Processing Applications* (Melaka, Malaysia), 354–359. doi: 10.1109/ICSIPA.2013.6708032

[28] Verma, U. & Sharma, N. (2019) Hybrid mode of medical image watermarking to enhance robustness and imperceptibility, *International Journal of Innovative Technology and Exploring Engineering*, **9**(1), 351–359. doi: 10.35940/ijitee.A4126.119119

[29] Assini, I., Badri, A., Sahel, K. S. A. & Baghdad, A. (2018) A robust hybrid watermarking technique for securing medical image, *International Journal of Intelligent Engineering and Systems*, **11**(3), 169–176. doi: 10.22266/IJIES2018.0630.18

[30] Al-Haj, A., Mohammad, A. & Amer, A. (2017) Crypto-watermarking of transmitted medical images, *Journal of Digital Imaging*, **30**(1), 26–38. doi: 10.1007/s10278-016-9901-1

[31] Thabit, R. & Khoo, B. E. (2017) Medical image authentication using SLT and IWT schemes, *Multimedia Tools and Applications*, **76**(1), 309–332. doi: 10.1007/s11042-015-3055-x

[32] Priyanka & Maheshkar, S. (2017) Region-based hybrid medical image watermarking for secure telemedicine applications, *Multimedia Tools and Applications*, **76**(3), 3617–3647. doi: 10.1007/s11042-016-3913-1

[33] Xiao, S., Zhang, Z., Zhang, Y. & Yu, C. (2020) Multipurpose watermarking algorithm for medical images, *Scientific Programming*, **2020**, 8848885. doi: 10.1155/2020/8848885

[34] Swaraja, K., Meenakshi, K. & Padmavathi, K. (2020) An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine, *Biomedical Signal Processing and Control*, **55**, 101665. doi: 10.1016/j.bspc.2019.101665

[35] Yamni, M., Daoui, A., Pławiak, P., Alfarraj, O. & El-Latif, A. A. A. (2024) Novel integer reversible Charlier transform for image reversible data hiding application, *IEEE Access*, **12**, 98480–98491. doi: 10.1109/ACCESS.2024.3427357

[36] Geetha, R. & Geetha, S. (2018) Improved reversible data embedding in medical images using I-IWT and pairwise pixel difference expansion. In: Bhattacharyya, P., Sastry, H., Marriboyina, V. & Sharma, R. (Eds.) *Smart and Innovative Trends in Next Generation Computing Technologies: Third International Conference*. Singapore: Springer Singapore (pp. 601–611). doi: 10.1007/978-981-10-8660-1_45

[37] Salih, Z. A. A., Thabit, R., Zidan, K. A. A., & Khoo, B. E. E. (2022). Challenges of face image authentication and suggested solutions. In *Proceedings of the 2022 International Conference on Information Technology Systems and Innovation (ICITSI)*, 189–193, <https://doi.org/10.1109/ICITSI56531.2022.9970797>

- [38] Silva, S. H., Bethany, M., Votto, A. M., Scarff, I. H., Beebe, N., et al. (2022) Deepfake forensics analysis: An explainable hierarchical ensemble of weakly supervised models, *Forensic Science International: Synergy*, **4**, 100217. doi: 10.1016/j.fsisyn.2022.100217
- [39] Malik, A., Kuribayashi, M., Abdullahi, S. M. & Khan, A. N. (2022) DeepFake detection for human face images and videos: A survey, *IEEE Access*, **10**, 18757–18775. doi: 10.1109/ACCESS.2022.3151186
- [40] Liu, K., Perov, I., Gao, D., Chervoniy, N., Zhou, W., et al. (2023) DeepFaceLab: Integrated, flexible and extensible face-swapping framework, *Pattern Recognition*, **141**, 109628. doi: 10.1016/j.patcog.2023.109628
- [41] Salih, Z. A., Thabit, R. & Zidan, K. A. (2023) A new manipulation detection and localization scheme for digital face images, *Journal of Engineering Science and Technology*, **18**(2), 1164–1183.
- [42] Al-Hadaad, M. H., Thabit, R. & Zidan, K. A. (2023) A new face image authentication scheme based on bicubic interpolation, *Al-Iraqia Journal of Scientific Engineering Research*, **2**(2), 29–36. doi: 10.58564/IJSER.2.2.2023.68
- [43] Jawad, A. H., Thabit, R. & Zidan, K. A. (2024) Improved face image authentication scheme based on embedding in adjacent coefficients, *International Journal of Informatics and Visualization*, **8**(3), 1126–1133. doi: 10.62527/joiv.8.3.2488
- [44] Thabit, R., Al-Askari, M. A., Mohammed, D. Z., Jawad, A. H., Zidan, K. A., et al. (2025) Face image authentication scheme based on MTCNN and SLT, *Multimedia Tools and Applications*, **84**, 38159–38201. doi: 10.1007/s11042-025-20684-7
- [45] Al-Hadaad, M. H. M., Thabit, R. & Zidan, K. A. (2023) A new face region recovery algorithm based on bicubic interpolation, *International Journal of Informatics and Visualization*, **7**(3), 1000–1006. doi: 10.30630/joiv.7.3.1671
- [46] Ravichandran, D., Praveenkumar, P., Rajagopalan, S., Rayappan, J. B. B. & Amirtharajan, R. (2021) ROI-based medical image watermarking for accurate tamper detection, localisation and recovery, *Medical & Biological Engineering & Computing*, **59**(6), 1355–1372. doi: 10.1007/s11517-021-02374-2
- [47] SAEID. (2023). *Human Faces*, [Online]. Available <https://www.kaggle.com/datasets/sbaghbidi/human-faces-object-detection>
- [48] iMerit. (2025). *Top 14 free image datasets for facial recognition*, [Online]. Available <https://imerit.net/blog/5-million-faces-top-14-free-image-datasets-for-facial-recognition-all-pbm/>