IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 40, No. 3, June, 2023, pp. 981-993
Journal homepage: http://iieta.org/journals/ts

Enhancing Biometric Fingerprint Security Through Integrated Watermarking and Cipher Block Chaining Techniques

Abdelkrim Ghaz[1], Nadhir Nouioua[2*], Ali Seddiki[2]

[1] Communications Networks Architecture and Multimedia Laboratory, Djillali Liabes University, Sidi Bel Abbes 22000, Algeria
[2] Telecommunications and Digital Signal Processing Laboratory, Djillali Liabes University, Sidi Bel Abbes 22000, Algeria

Corresponding Author Email: nadhir.nouioua@univ-sba.dz

https://doi.org/10.18280/ts.400314

Received: 5 October 2022
Accepted: 21 April 2023

Keywords:
Advanced Encryption Standard (AES), Cipher Block Chaining (CBC), cryptography, fingerprint, Least Significant Bit (LSB), watermarking

ABSTRACT

This study presents a combined watermarking-cryptography approach to bolster the security of biometric fingerprint data. In the initial stage, a digital watermark is embedded within the host image (fingerprint scan) using the Least Significant Bit (LSB) technique. Upon completion of the embedding process, the watermarked image undergoes encryption using the Advanced Encryption Standard (AES) in Cipher Block Chaining (CBC) mode, increasing complexity and ensuring secure communication. Conversely, the extraction procedure involves reversing the embedding steps by first decrypting the received image and subsequently applying the extraction algorithm to the unencrypted image to recover the embedded watermark. The proposed method demonstrates significant imperceptibility, as measured by the Peak Signal-to-Noise Ratio (PSNR) and Normalized Correlation (NCC) metrics. Furthermore, the watermark exhibits resilience against signal processing attacks, including noise and filtering. The heightened key sensitivity of the CBC cryptosystem renders the proposed scheme more resistant to statistical attacks compared to existing methods in the literature.

1. INTRODUCTION

Today, humans stand on the edge of a new technological revolution regarding the development rates in all disciplines and the gigantic number of discoveries, where information technology represents the fundamental engine of this acceleration. The confidentiality of information transmitted over networks is a hot topic in scientific circles, and it makes internet users more concerned about their data security every day, especially with the widespread availability of communication devices such as smartphones, personal digital assistants (PDAs), computers, and high-speed internet. The fingerprint is a distinctive identification for each individual [1], belonging to biometric recognition, which is the process of identifying humans based on their vital and physical features [2]. With the advancement of fingerprint sensors and the uniqueness factor provided by fingerprints, the latter have become a powerful tool in access control, authentication systems, and crime investigations [3].

Since security represents an essential interest in people's day-to-day lives, digital watermarking and cryptography can be cited as crucial security mechanisms that guarantee a certain amount of protection and privacy for high-tech users. With the enthralling advancement of multimedia technologies, digital watermarking has overcome some copyright and malicious manipulation issues. Digital watermarking is about incorporating a secret message within a host's data to prove authenticity, integrity, and ownership. On the other hand, cryptography is the procedure of preventing data from being spied on by converting material such as images, texts, and videos from a clear to an unreadable state.

Latterly, various image watermarking and encryption techniques have been suggested [4-8] as this blend can ensure authentication and secure transfer [9]. Haddad et al. [10] presented a hybrid watermarking encryption method for medical image protection. In this technique, it is possible to access the watermark directly from the encrypted or compressed image, where this scheme has provided high incorporation capacities.

Aminuddin and Ernawan [11] suggested a blind, fragile watermarking method for colored images based on a self-recovery mechanism called AuSR1. The concept of this idea is to layer the host image into 2 by 2 non-overlapping pixel blocks, creating a block map to load information recovery bits from one specific block to another, then embed authentication and recovery data on separate far blocks. Since each pixel bit-depth is 8 bits, the 6 most significant bits (MSBs) are used for the authentication and recovery while the LSBs are utilized for the position indexation. This method provided high imperceptibility and good endurance against tampering.

Mata-Mendoza et al. [12] proposed a robust dual watermarking scheme for telemedicine applications, which associates the visual and robust watermarking paradigms for the aim of electronic patient records (EPR) disconnection of the medical image prevention and source verification, where the first watermark is inserted in the spatial domain and the last is placed in the discrete cosine transform (DCT) utilizing the quantization index modulation algorithm under dither modulation (QIM-DM). This method delivered high performance in terms of imperceptibility and similitude.

Garg and Jain [13] suggested an invisible watermarking scheme for biometric images based on the discrete wavelet

transform (DWT). In this technique, the host image was segmented using the DWT based on the edge entropy to select the convenient block for the watermark insertion, which was encrypted by visual cryptography (VC). The embedding was conducted using a reversible technique. On the other hand, secret keys were generated by the VC to retrieve the hidden watermark. High robustness against various attacks was noticed in this research.

Shankar and Kannammal [14] presented a joint watermarking and encryption framework. In this scheme, the medical image was subdivided into regions of interest (ROI) and regions of non-interest (RONI), where the reason behind this segmentation is to keep the region of interest safe and avoid misdiagnosis. A reversible watermark is exerted on the ROI using difference expansion (DE) as an embedding function. Furthermore, a robust watermark is applied to RONI with the aim of resisting attacks. Once watermarking is done, ROI and RONI are concatenated, and afterward, an advanced encryption standard is performed to increase image security. This method delivers high visual quality and satisfactory robustness.

A digital semi-fragile watermarking technique for medical images in the transform domain for cohesion verification and patient identification was proposed by Moad et al. [15]. The scheme is performed in two major phases: the watermark generation as the first step, which is based on hashing the patient records and image acquisition data utilizing the message digest hash function (MD5), where the concatenation result is used as a key for the Rivest Cipher 4 (RC4) algorithm, which is used to encrypt the compressed patient photography, where this latter was compressed using the Absolute Moment Block Truncation Coding (AMBTC) in the aim of rendering the system more secure, and then a combination is done to obtain the watermark. Secondly, the watermark is incorporated into the medium frequencies obtained after the decomposition made on the discrete wavelet transform. The results of this algorithm show that it works because it is resistant to attacks.

Kamble and Agrawal [16] proposed a method for image watermarking based on wavelets and quad-tree decomposition, where the main concept of the algorithm is embedding the segregated watermark using the quad-tree into the mid-frequencies obtained from the lifting wavelet transform of the cover image blue channel to prevent the hidden message from attacks. This technique reported high PSNR, SSIM, and normalized correlation results and provided good resilience against several attacks in general and contrast enhancement in particular.

Geetha and Geetha [17] suggested a reversible scheme for electronic patient records hidden within medical images. This technique is based on up-sampling the original image using Rhombus Mean Interpolation (RMI) as a preprocessing stage to decrease image size, where its product is considered the host image, and then the checksum is applied for tamper detection. The embedding phase is realized using an Intermediate Significant Bit (ISB). This method provides high visual quality values validated with PSNR and SSIM metrics.

Benseddik et al. [18] presented a digital reversible watermarking framework for fingerprint security based on interpolation. This technique is about incorporating two watermarks for authenticity and tamper detection, respectively, utilizing the Lifting Wavelet Transform (LWT) and the intermediate significant bit substitution. The method provides acceptable PSNR results and enhances robustness against Joint Photographic Experts Group (JPEG) and salt and pepper noise attacks.

Zhang [19] suggested a way to encrypt images using a piecewise linear chaotic map and a cubic S-Box. In this research, an encryption algorithm called a unified image encryption algorithm is made up of the same encryption and decryption steps. This means that the plain image and the key stream result in the cipher image, and vice versa. The cubic S-box is used to generate a key stream, which is a two-dimensional S-box transformed into a three-dimensional cubic S-box by dividing the initial S-box into 4 equal regions and then stacking the divided blocks. The reason behind using the cubic S-box is the generation of less similar values. This technique showed high key space due to the largely used key (512 bits), high sensitivity, and fast computation.

Rachmawanto et al. [20] suggested block-based image encryption using Arnold's chaotic map. The framework principle is about segmenting the image into sub-blocks and then ciphering each sub-block individually using the same chaotic formula and iteration number. This method's cipher image results appear in insignificant mosaic forms. Furthermore, this technique has shown acceptable values in terms of the number of pixels change rate (NPCR), unified average change intensity (UACI), and high imperceptibility results, which confirm its effectiveness.

Sreenivasan et al. [21] presented a consolidation of five chaotic maps and a DNA encoding method for image encryption. Where in the first stage, the chaotic sequence is generated based on sine, tent, henon, sine-cosine, and logistic maps, correspondingly, the provided sequence is employed in the encryption system, following the next stages: pixel-level scrambling, bit-level scrambling, DNA encryption, and DNA complementary rules. The findings demonstrate that the suggested technique is efficient as regards the obtained correlation, NPCR, UACI, and entropy values.

Gollagi et al. [22] presented an encryption scheme based on the ameliorated Rivest–Shamir–Adleman (RSA) algorithm for image security. In short, the main idea behind the proposed work was to encrypt an image with two codes and then use Arnold's chaotic map to shuffle the image's parts. The proposed method achieved good results in terms of entropy, NPCR, and UACI.

In this research, a hybrid fragile watermarking and encryption technique for the security of biometric fingerprints is suggested. The principle consists of embedding a watermark using the LSB fragile watermarking technique into a fingerprint image. Then the obtained watermarked image is ciphered using CBC. At the succeeding stage, the received cipher image is deciphered utilizing the CBC decryption algorithm. Immediately after this last procedure, the watermark is extracted based on the LSB extraction function. This method is meant to increase protection levels to prevent misuse, harmful changes, and copies made without permission.

The remainder of this paper is organized as follows: Section 2 presents an overview of the Cipher Block Chaining algorithm and the evaluation metrics. Section 3 elucidates the proposed techniques and algorithms. Section 4 illustrates the experimental results and comparisons. Finally, the paper is concluded in Section 5.

2. PRELIMINARIES

This section elucidates the used technical materials in the proposed algorithm.

2.1 Advanced encryption standard

After years of competition, in 2001, the National Institute of Standards and Technology (NIST) approved a new encryption system named Advanced Encryption Standard [23]. The standard is an iterative cipher block [24], based on the Rijndael algorithm [25]. This standard is a symmetric block cipher, where the symmetry notion in cryptography means Alice and Bob partage the same key utilized for encryption and decryption procedures. The maximum data size that can be treated by this system is 128 bits [26], exploiting cipher keys of 128, 192, and 256-bit lengths. The AES was designed to gain the following essential features:

- Attack resistance
- High speed and low energy consumption
- Uncomplicated architecture

The Advanced Encryption Standard cryptosystem's experimental outcomes may be impacted by key lengths. Although longer key lengths typically bring additional protection, more processing resources will be required, which could slow down the encryption and deciphering procedures. For the majority of applications, a key value of 128 bits is usually considered to be secure. However, a larger key value, such as 192 or 256 bits, may be advised for extremely confidential data.

The following guidelines ought to be adhered to when choosing AES keys:

- Utilize robust, random keys to prevent intruders from predicting or brute-forcing using a sophisticated random number generator.
- Employ unique keys for each message or session to guarantee that the attacker cannot access other protected messages or sessions if one key is compromised.
- Keys should be stored away from unauthorized people. To further improve security, key regeneration, and rotation should be considered as well.

Algorithms 1 and 2 summarize the principles of encryption and decryption operations for the advanced encryption standard.

Algorithm 1: AES encryption

Begin

- AddRoundKey
  for *round = 1 to Nr - 1* **do**
    SubBytes
    Shif tRows
    MixColumns
    AddRoundKey
  end for
- SubBytes
- ShiftRows
- AddRoundKey

End

SubBytes substituting bytes in accordance with a certain table, the so-called S-Box, significantly affects the encryption process in a non-linear way. The first row is left untouched while the remaining three rows, which comprise a 4×4 byte matrix, undergo a *ShiftRows* operation to add complexity. In *MixColumns*, instead of treating each byte as an integer, each column is multiplied by a constant matrix that fills the Galois field. The round key and the initial input block are XORed together by Assafli and Hashim [27].

Algorithm 2: AES decryption

Begin

- Inverse AddRoundKey
  for *round = 1 to Nr - 1* **do**
    InverseShiftRows
    InverseSubBytes
    InverseAddRoundKey
    InverseMixColumns
  end for
- Inverse ShiftRows
- Inverse SubBytes
- Inverse AddRoundKey

End

Moreover, similar results to the electronic code-book (ECB), which is a deterministic operation mode, will be obtained if the Rijndael algorithm is directly applied using the exact same key, consequently, susceptibility may be provoked due to the poorly concealed data patterns [28]. Cipher Block Chaining (CBC), cipher feedback (CFB), output feedback (OFB), and counter mode (CTR) are non-deterministic (probabilistic) operation modes employed in cryptography [29].

Each of the aforementioned probabilistic operation modes has its own application scenarios, advantages, and disadvantages, which are briefly discussed as follows:

1. Cipher Block Chaining (CBC) is frequently used in data transfer when the message's secrecy and stability are crucial.
   - Pros: Besides providing unpredictability to the encryption process, CBC prevents plaintext patterns from being visible in the ciphertext.
   - Cons: Because CBC employs a chaining structure and each block's encryption or decoding relies on the preceding block, it is slower than some other forms of operation.
2. Cipher Feedback (CFB) is utilized in real-time applications, where data is transmitted in a continuous stream, such as audio and video data encryption.
   - Pros: CFB enables encryption and decryption of single bits or bytes of data, which is advantageous in real-time applications requiring fast processing of tiny data elements.
   - Cons: CFB is susceptible to error spread, which means that if an error occurs during the encryption or decryption of one block, it might also impact consecutive blocks.
3. Output Feedback (OFB) is commonly employed when data encryption and decryption must be conducted separately in conjunction with each other. Along with file and drive encryption, it is employed to secure access sessions.
   - Pros: By using OFB, a series of pseudo-random bits can be produced to be applied to data protection and decoding. Additionally, it might be used for both error detection and correction.
   - Cons: OFB is susceptible to attacks where the encryption function's output can be predicted based on previous output.
4. Counter Mode (CTR): Similar to the OFB, the counter mode is used in situations where the encryption and decryption of data need to be performed independently of each other.
   - Pros: CTR can be used to produce a sequence of pseudo-random bits for data encryption and

decryption since it does not implement a chaining framework.

- Cons: As each data element requires a unique counter, CTR can be challenging to manage.

In summation, the Advanced Encryption Standard represents a widely employed cryptosystem that offers safe and effective data protection. However, as with any cryptosystem, it has its advantages and weaknesses. The pros and cons of the AES concept are covered below.

Advantages:

- Security: AES is a common option for safe data transmission since it offers robust security against a variety of assaults, including brute-force attacks.
- Efficiency: In terms of efficiency and resource utilization, AES is very effective. It can rapidly encode and decode data and uses little computing power, making it appropriate for use in settings with limited resources.
- Standardization: AES is a widely used and compatible encryption method that has been accepted by numerous groups and countries around the globe.
- Flexibility: AES can be used in a variety of apps because it allows a variety of key and block sizes.

Disadvantages:

- Key management: The quality of the encryption key used determines how secure AES is.
- Key administration can be difficult because they must be disseminated to approved parties and safely kept. Although AES is thought to be extremely safe, it is not impervious to attacks. There have been cases where the algorithm's weaknesses have been found and used against it.
- Execution problems: If AES is not applied properly, its security may be jeopardized. Wrong application techniques, such as vulnerable random number generation or poor key generation, can degrade the cryptosystem.

AES is an effective option for data protection because its encryption and decoding principles offer robust security and effectiveness. AES possesses certain restrictions and deficiencies. Therefore, effective key management and execution procedures are essential to ensuring its viability.

2.2 Cipher Block Chaining

The Cipher Block Chaining mechanism (see Figure 1) is about encrypting determined blocks, where each block is dependent on all previous cipher blocks [30], except for the initial block, which requires an initialization vector (IV) for the encryption. Thus, in this operation mode, an XOR operation is exerted on each plain text block and its earlier ciphered block, exempting the first block, which is XORed with the initialization vector [23]. The encryption and decryption processes are expressed in Eqns. (1) and (2), correspondingly. Moreover, the Cipher Block Chaining operation mode can be summarized as follows [31]:

- Every block depends on preceding blocks
- Each earlier encrypted block result recurs in the ruling block
- The initialization vector is mandatory for the initial block encryption
- IV can be generated manually or randomly

$$C_i = E_k(P_i \oplus C_{i-1}); C_0 = IV \quad (1)$$

$$P_i = D_k(C_i) \oplus C_{i-1}; C_0 = IV \quad (2)$$

Thanks to the chaining structure, the CBC consumes more computational time than other operation modes.

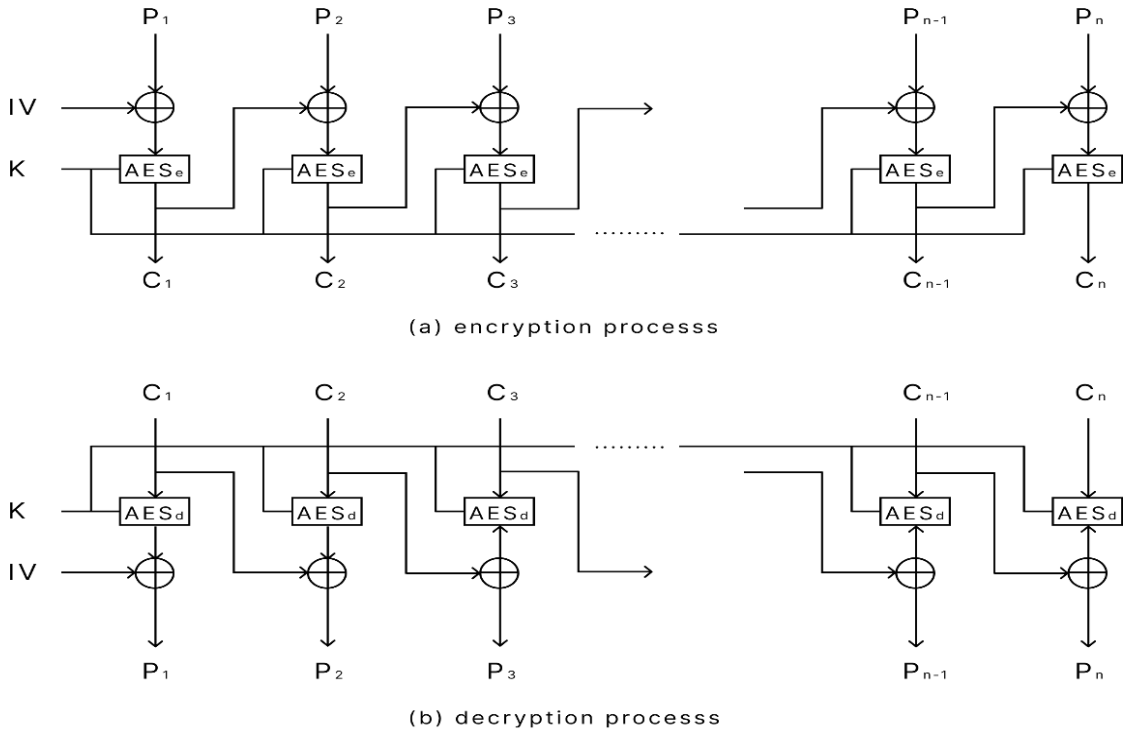

Figure 1. Cipher Block Chaining operation mode

The encryption and decryption time consumption of the Cipher Block Chaining method is *Time(n)*, where *(n)* is the number of message blocks since each block depends on the preceding block. The electronic codebook mode has a time complexity of *Time(1)* for encryption and decryption since ECB does not involve a chaining structure and each block is encrypted or decrypted separately. As a result, CBC is slower than some other modes of operation due to the chaining structure that increases the computational cost needed for encryption and decryption. However, CBC provides unpredictability and avoids patterns of information from being apparent within the ciphertext, which results in additional protection than ECB.

CBC mode's implementation of the chaining technique leads to reduced performance in terms of computational cost. It is crucial to note that the method's processing time could also be influenced by the amount of input data as well as the accessible computing capabilities. Using potent professional machines could indeed help minimize the processing time. Powerful processors, more RAM, and efficient storage devices can help process large volumes of data more quickly. Moreover, using parallel processing techniques and implementing the proposed method on specialized hardware can also enhance its performance. It's also noteworthy that the encryption mode selection depends on the requirements of the application. Even though CBC mode might be slower than other modes, it is typically considered to be more solid. Therefore, even though it requires a longer exertion duration, CBC mode represents a viable option for utmost security.

3. METHODOLOGY

Figure 2 illustrates the proposed method flowchart. It mainly comprises two major phases: the watermarking stage using the least significant bit to maintain proprietary rights and the encryption stage based on the advanced encryption standard in the Cipher Block Chaining mode to ensure confidentiality and high security levels during transmission. On the other hand, the decryption and watermark extraction operations consist of exerting the AES decryption algorithm on the cipher image using the exact key employed in the encryption phase, and then the previously inserted watermark is extracted from the least significant bits of the obtained plain image.

The digital watermarking and encryption mechanisms outlined in this study are based on the speculative notion of integrating digital watermarking and cryptography methods to increase the security of biometric fingerprint data. The watermark is therefore inserted into the fingerprint image using the Least Significant Bit (LSB) method. This phase is designed to make the watermark imperceptible and render it difficult for an assailant to notice its existence. The watermarked image is encrypted in the second phase using the Advanced Encryption Standard in the Cipher Block Chaining mode, which increases intricacy and guarantees secure transmission. The utility of this suggested method is that it combines the resilience of encryption with the imperceptibility of watermarking to deliver biometric fingerprint data with a considerable level of safety. Moreover, the CBC mode's high key sensitivity makes the strategy more immune to statistical attacks.

The following is a representation of the suggested scheme's broad mathematical expression:

$$\mathrm{C} = AES_{CBC\_enc}(M, K) \tag{3}$$

where, K is the encryption private key, M is the watermarked image, and C is the decrypted watermarked image. The encryption procedure can be illustrated as follows:

$$\mathrm{M} = AES_{CBC\_dec}(C, K) \tag{4}$$

where, M stands for the initial watermarked image, C for the protected version, and K for the deciphering key.

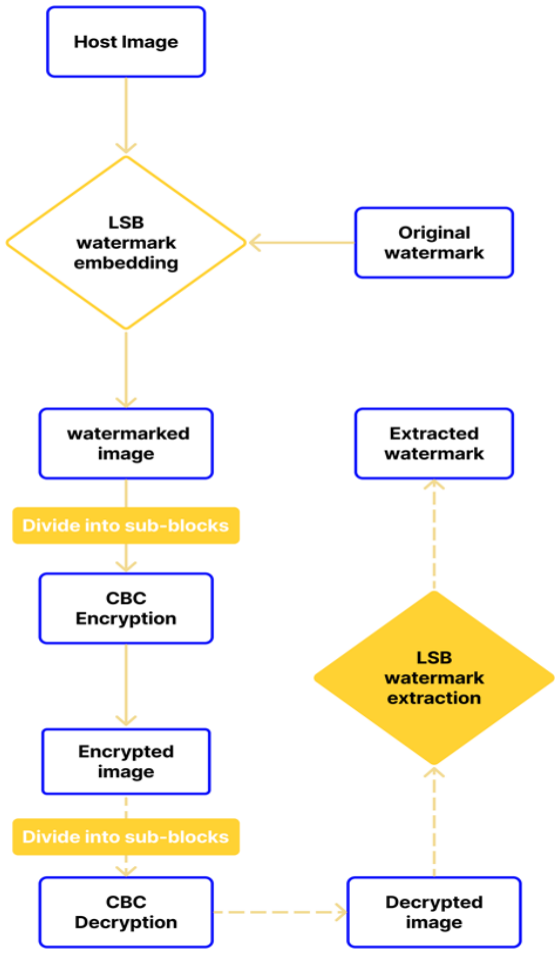

Figure 2. Proposed method framework

3.1 Watermark embedding and encryption phase

1. Read the biometric fingerprint image denoted "I"
2. Read the binary watermark image "W"
3. Store sequentially the host image elements
4. Each watermark bit should be bitset into the LSB (first bit) location of the host image as follows:

for i = 1: h **do**
  for j = 1: w **do**
    $W\ I(i, j) = bitset(I(i, j), I, watermark(i, j)$
  end for
end for

w and h denote the height and width

5. Save the watermarked image called "WI"
6. Apply the AES encryption as mentioned in Algorithm 1 on the watermarked image "WI"

3.2 Decryption and watermark extraction phase

1. Load the cipher image "WI"
2. Exert the AES decryption illustrated in Algorithm 2 on "WI"
3. the watermark is extracted from the obtained plain image "PI" using the bitget function

for i = 1: h **do**
  for j = 1: w **do**
    $WI(i, j) = bitget(PI(i, j), 1)$;
  end for
end for

4. EXPERIMENTAL RESULTS

The algorithm was applied to a series of fingerprint images collected from the study [32] to verify the performance of the suggested method. The algorithm was examined using MATLAB 2019 on an Intel® Xeon® processor with a 16 GB memory machine, where the images' size was 192×256. The suggested scheme was evaluated using the metrics indicated in the sequel.

4.1 Performance evaluation

As imperceptibility represents a crucial element in digital watermarking evaluation, the following metrics are addressed to serve this operation:

- A Peak Signal to Noise Ratio (PSNR) is about computing the numerical differences between an original (host image) and a manipulated image (watermarked image) using the next equation:

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (5)$$

The Mean Square Error (MSE) formula is expressed as:

$$MSE = \frac{1}{X\times Y}\sum_0^{X-1}\sum_0^{Y-1}(H(i,j) - Wi(i,j))^2 \quad (6)$$

The host and the watermarked images are denoted H and Wi respectively, and X and Y represent the dimensions.

- Structural similarity index metric as its name indicates, calculates the similarity between modified and reference images.

$$\text{SSIM}\ (x, y) = I(l(x, y), C(x, y), S(x, y)) \quad (7)$$

The I, C, and S are the luminance, contrast, and structure correspondingly.

- The normalized correlation compares the extracted watermark to the integrated one. It is defined as follows:

$$NCC = \frac{\sum_{i=1}^{x}\sum_{j=1}^{y}(W_{or}(i,j)\times W_{ex}(i,j))}{\sum_{i=1}^{x}\sum_{j=1}^{y}W_{or}^2(i,j)} \quad (8)$$

where, W_{or} is the original watermark, and W_{ex} is the extracted watermark.

- The Bit Error Rate is calculated by dividing the total number of transferred bits by the total number of errors.

$$BER = \frac{\text{Errors}}{\text{Number of bits}} \quad (9)$$

Table 1. Performance analysis of the watermarked fingerprints test images

Fingerprint	PSNR (dB)	MSE	SSIM
Fingerprint 1	51.1342	0.1244	0.9993
Fingerprint 2	51.0774	0.1063	0.9988
Fingerprint 3	51.2965	0.1094	0.9985
Fingerprint 4	50.9758	0.1017	0.9988
Fingerprint 5	51.2059	0.1149	0.9987

To assess the suggested technique, Table 1 shows the performance analysis in terms of high fidelity and indistinguishability, where high peak signal-to-noise ratio results were obtained with an average of 51 dB, which is higher than the accepted range, compromising values from 29 to 35 dB [33]. The conducted method results are displayed in Figure 3. On the other hand, the mean square error is relatively low due to the minor error recorded. As known, the structural similarity index metric is more efficient compared to PSNR with regard to subjective quality [34]. The suggested technique revealed SSIM values with an average of 0.9988, confirming the heightened similarity between the host and the watermarked image, where zero difference can be noticed by the human vision system.

Table 2. PSNR and SSIM comparison

Images	PSNR	SSIM
Moad et al. [15]	43.59	0.9891
Kamble and Agrawal [16]	47.84	0.9985
Geetha and Geetha [17]	42.34	0.9801
Benseddik et al. [18]	34.61	0.9981
Proposed method	51.14	0.9988

Furthermore, Table 2 exhibits a comparison in terms of PSNR and SSIM between the presented method and other digital watermarking methods, where the method in hand revealed increased results, which affirms the proposed method's competence.

Digital image watermarking attacks are about manipulating or tampering with an image, intentionally or unintentionally, and as robustness is as necessary as imperceptibility for digital watermarking schemes, a group of attacks was exerted to evaluate the capacities of the suggested framework. Table 3 illustrates the results in terms of normalized correlation and the bit error rate of the extracted watermark in a zero-attack scenario, where the presented method delivered ideal results. Furthermore, even under attack, the proposed method withstands various attack types as reported in Table 4.

Figure 3 shows the original cover image, the original watermark, the watermarked image, and the retrieved watermark, where it is clear that the testing images were not affected during the embedding and extraction procedures. Moreover, it is visible in Figure 4 that the extracted watermarks are still recognizable even after attack conduction, which confirms the resilience of this technique to a variety of manipulations such as noise, translation, and filtering.

Table 3. NCC and BER results of the retrieved watermark from testing

Fingerprints	NCC	BER
Fingerprint 1	1.00	0.00
Fingerprint 2	1.00	0.00
Fingerprint 3	1.00	0.00
Fingerprint 4	1.00	0.00
Fingerprint 5	1.00	0.00

Table 4. NCC and BER results of the extracted watermarks under attacks

Attack type	NC	BER
Salt & Pepper 5%	0.9372	0.0248
Salt & Pepper 10%	0.8784	0.0488
Translation (5.5)	0.7570	0.0973
Median filter (3:3)	0.8642	0.0522
Median filter (5:5)	0.7231	0.1065

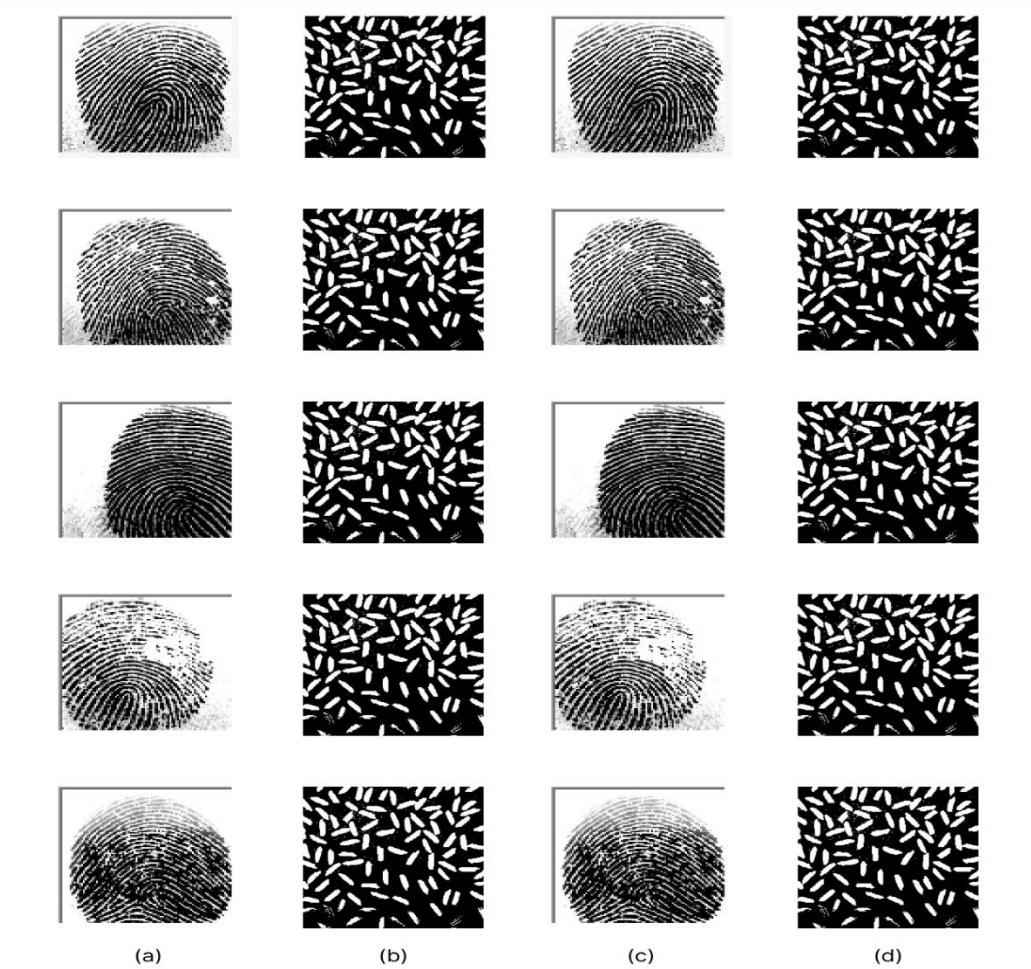

Figure 3. (a) Host fingerprints, (b) embedded watermark, (c) watermarked fingerprints, (d) extracted watermark

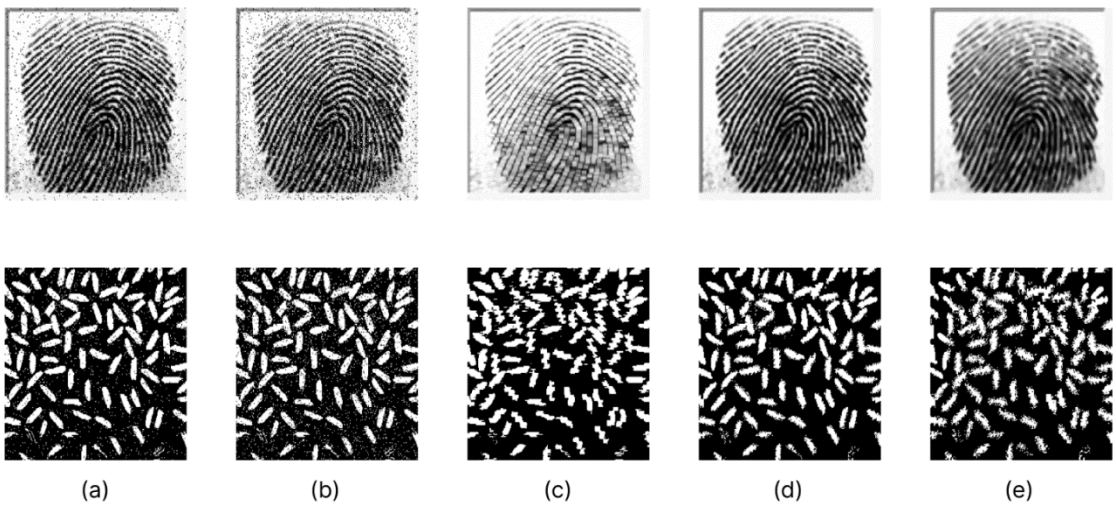

Figure 4. Watermarked image and extracted watermark under attacks, (a) Salt & Pepper 5%, (b) Salt & Pepper 5%, (c) Translation (5.5), (d) Median filter (3:3), (e) Median filter (5:5)

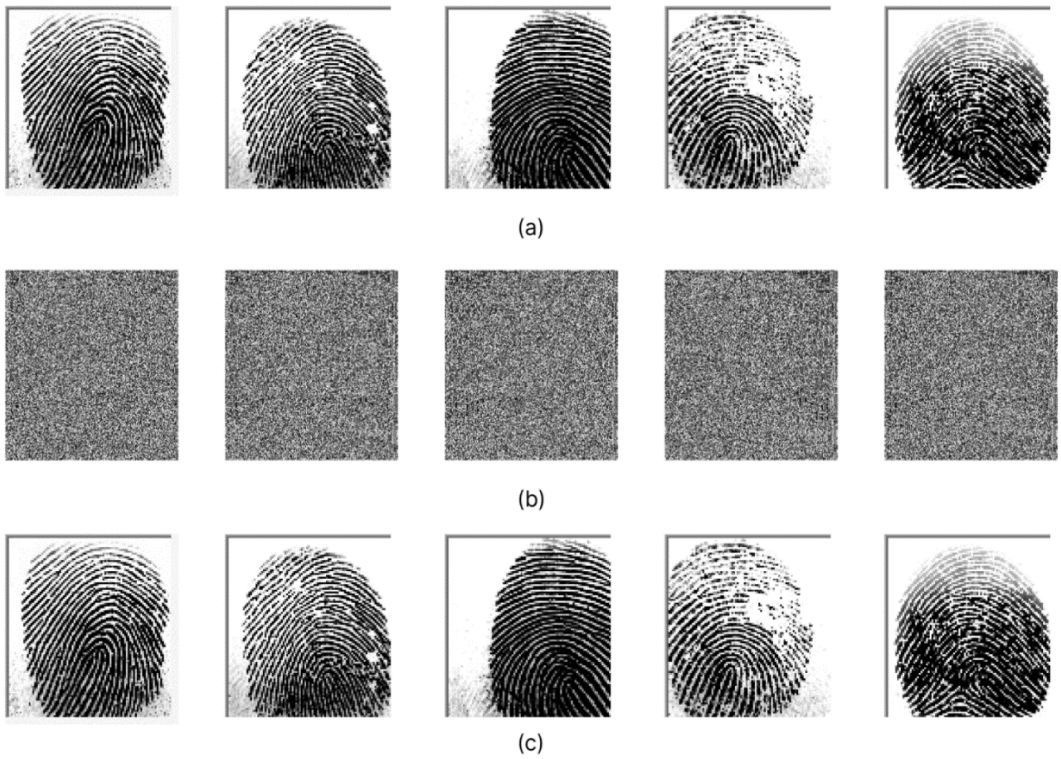

Figure 5. (a) Original fingerprint images, (b) cipher fingerprint images, (c) plain fingerprints images

4.2 Correlation analysis

Correlation analysis is about calculating the correlation between adjacent pixels for plain and cipher images, where it is mathematically given by the following formulas:

$$r_{u,v} = \frac{E((u-E(u))(v-E(v)))}{\sqrt{D(u)D(v)}} \quad (10)$$

$$E(u) = \frac{1}{N}\sum_{i=1}^{N} u_i \quad (11)$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N} (u_i - E(u))^2 \quad (12)$$

Table 5 depicts the correlation coefficient results of the plain and cipher testing images, where positive correlation is acclaimed for plain fingerprints in vertical, horizontal, and diagonal distribution since results are near 1, contrary to the encryption, where obtained values must be close to 0 [35, 36], which signify the dissimilarity between the encrypted and the decrypted images. The proposed method reveals results approximately equal to 0 for the cipher fingerprint images, which proves the crypto-system efficiency.

To affirm the results demonstrated in Table 5, The fingerprint image encryption and decryption results are shown in Figure 5. Furthermore, where cipher images appear random and unpredictable, no changes can be noticed by the human visual system between the original and the deciphered fingerprint images. The correlation results of the encryption and decryption images are illustrated in Figure 6, where it is remarkable that the crypto-system made adjacent pixels irrelevant, which is a sign of robustness against statistical attacks.

Table 5. Correlation coefficients results

Fingerprints		Plain image	Cipher image
Fingerprint 1	Horizontal	0.9175	0.007
	Vertical	0.8702	0.002
	Diagonal	0.7618	0.005
Fingerprint 2	Horizontal	0.9274	-0.004
	Vertical	0.8565	0.0252
	Diagonal	0.7775	0.0012
Fingerprint 3	Horizontal	0.9762	-0.0053
	Vertical	0.8892	0.0296
	Diagonal	0.8722	-0.0034
Fingerprint 4	Horizontal	0.9420	-0.0104
	Vertical	0.8825	0.0354
	Diagonal	0.8263	0.0011
Fingerprint 5	Horizontal	0.9507	-0.0096
	Vertical	0.8909	0.0212
	Diagonal	0.8576	0.0053

Table 6. Correlation coefficients comparison

Methods	Zhang [19]			Proposed method		
	H	V	D	H	V	D
Lena						
Plain	0.984537	0.976635	0.953663	0.9477	0.9615	0.9144
Cipher	-0.009448	0.024064	-0.041171	0.0022	-0.0006	0.0037
Pepper						
Plain	0.977792	0.978929	0.958526	0.9785	0.9728	0.9492
Cipher	0.001899	0.026099	0.046131	0.0081	0.0018	0.0055

Referring to Table 6 that displays the results of a comparison between the suggested approach and the method in the study [19], it is evident that the utilized crypto-system delivers considerable unpredictability levels where subordinate correlation values were achieved in horizontal, vertical, and diagonal directions. Thus, the decryption procedure needs the appropriate encryption key to provide accurate results.

4.3 Key sensitivity

Keyspace represents an essential criterion for a shielded crypto-system since it becomes less predictable and more resilient to brute-force attacks which implies high-security [37], a key length of a 128-bits is utilized in the proposed scheme, where 2^{128} iteration must be executed in order to obtain the exact key. In the aim of analyzing the key sensitivity, a plain image is encrypted by employing two different keys with slight variations, then a decryption process is also done by utilizing the accurate and alternate keys. Figure 7 displays the obtained results, where it is obvious that the key is eminently sensitive to any transition, and where disturbed results will be delivered if any extra manipulation is involved.

4.4 Differential attacks analysis

The differential attacks consist of measuring the impact of changing a single bit of the original image on the encryption resultant [38]. The number of pixels change rate (NPCR) and unified average change intensity (UACI) are metrics used to calculate the encryption method robustness of an image. NPCR and UACI compute the average difference among encrypted images. Mathematically, the metrics are defined as:

$$\mathrm{NPCR} = \frac{\sum_{ij} D(i,j)}{N \times M} \times 100\% \tag{13}$$

$D(i, j)$ return to 1
when $P_1(i, j) = P_2(i, j)$, and 0 i $P_1(i, j) \neq P_2(i, j)$

$$\mathrm{UACI} = \frac{1}{M \times N} \sum_{ij} \frac{|P_1(i,j) - P_2(i,j)|}{255} \times 100\% \tag{14}$$

where, $P1$, $P2$ are the encrypted images, M, N and i, j represents the dimensions and the position of gray scale value (0 - 255) respectively.

Furthermore, Table 7 depicts the NPCR and the UACI results, where the average result of the NPCR is 0.9963 and the UACI average is 0.404, which are approximate 0.9961 and 0.3346 the theoretical values of the NPCR and UACI metrics correspondingly [39].

Table 7. NPCR and UACI results

Fingerprint	NPCR (%)	UACI (%)
Fingerprint 1	99.61	39.04
Fingerprint 2	99.64	39.47
Fingerprint 3	99.63	41.89
Fingerprint 4	99.60	40.70
Fingerprint 5	99.66	40.78

To confirm the proposed method's effectiveness, Tables 8 and 9 show NPCR and UACI comparison results of different techniques, including the suggested, where the presented scheme presented acceptable and favourable values.

Table 8. NPCR (%) comparison

Methods	Method [20]	Method [21]	Method [22]	Suggested technique
Lena	94.65	99.588	99.7012	99.62
Pepper	98.17	99.6017	-	99.5890

Table 9. UACI (%) comparison

Methods	Method [20]	Method [21]	Method [22]	Suggested technique
Lena	14.02	33.4096	33.3020	28.5901
Pepper	16.99	33.5166	-	29.5816

4.5 Information entropy

Intending to study the texture of images, entropy answers the purpose by statically computing the pixels' randomness in an encrypted image [40]. In short, high entropy is noticed in regions with uniform intensities and vice versa. It is mathematically given by:

$$\mathrm{E} = -\sum_{i=0-255} p(i) \log_2 (p(i)) \tag{15}$$

where, p stands for the associated probability

Table 10 reveals the entropy results of the original and the encrypted watermarked images, where maximum entropy results were captured for the cipher images, which translates the results traced in Figure 8. Histograms show the uniform distribution of encrypted images. This uniform distribution can be interpreted by confirming the force of the crypto-system, where the plain image color distribution manifests anarchic and scrambled after the encryption process. Moreover, if the entropy value is close to 8 for an 8-bit image, it augurs optimum randomness.

Table 10. Entropy results of plain and cipher test images

Fingerprint	Plain image	Cipher image
Fingerprint 1	7.1265	7.9956
Fingerprint 2	6.7121	7.9833
Fingerprint 3	6.0453	7.9849
Fingerprint 4	6.3022	7.9844
Fingerprint 5	6.3322	7.9838

Table 11. Entropy results comparison

Image	Sreenivasan et al. [21]		Proposed method	
	Plain image	Cipher image	Plain image	Cipher image
Lena	7.4318	7.9968	7.4293	7.9964
Pepper	7.5700	7.9967	7.5819	7.9964

The average entropy of cipher images mentioned in Table 10 is 7.9863, which means efficient encryption has been provided by the exploited crypto-system. Table 11 represents the entropy results of the presented technique and the technique in the study [21], where satisfying entropy results were obtained compared to the other method.

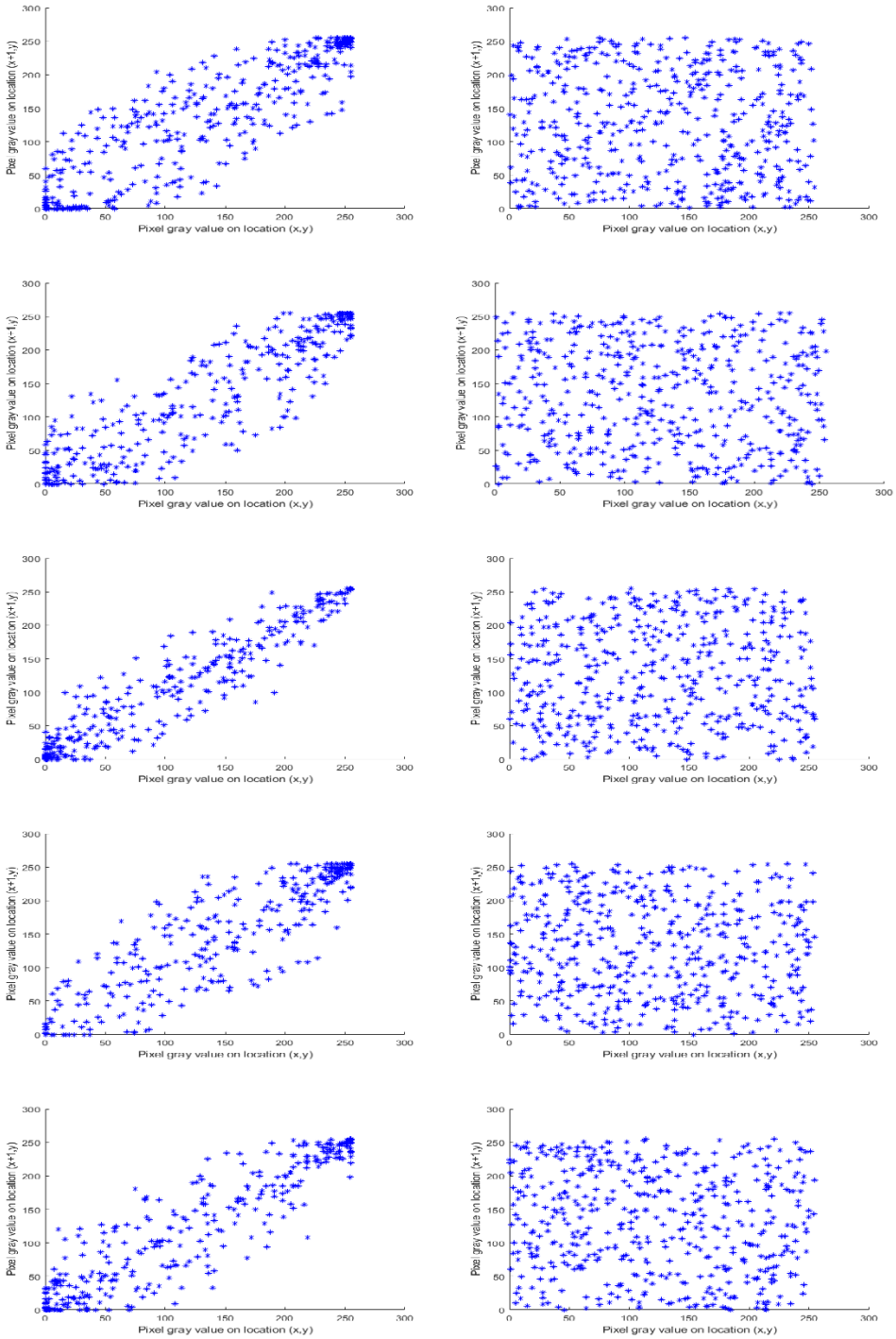

Figure 6. Correlation analysis of plain and cipher fingerprints

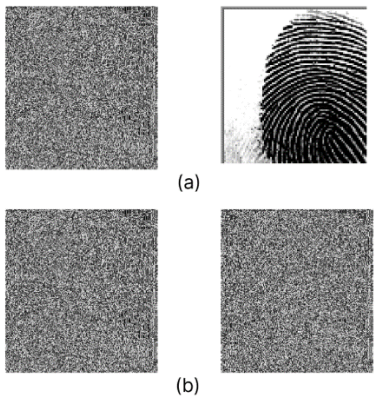

Figure 7. (a) Decryption using the right key, (b) decryption using the wrong

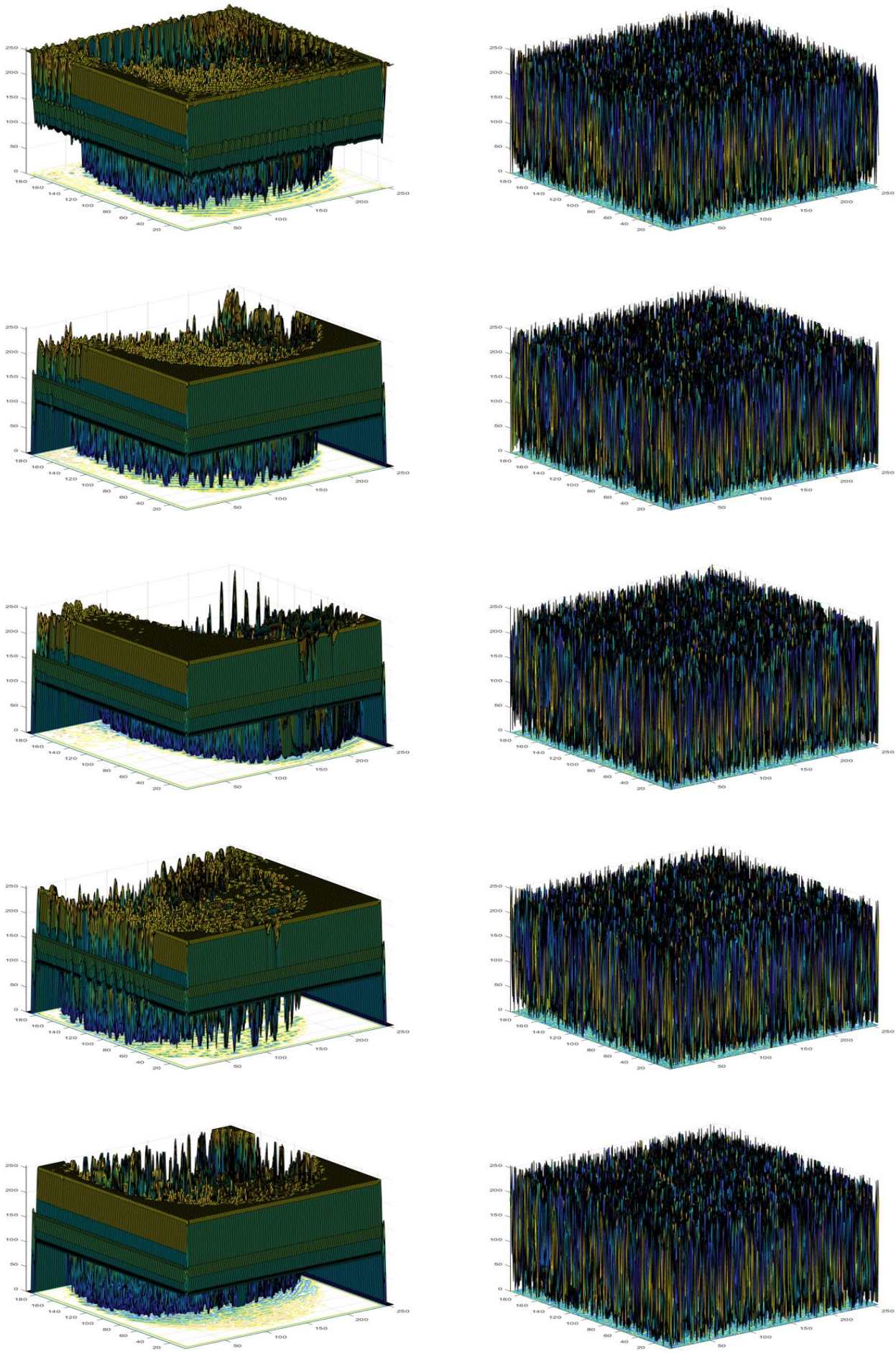

Figure 8. 3D histogram of plain and encrypted fingerprint images

5. CONCLUSION

This paper proposed a joint watermarking-encryption scheme for biometric fingerprint security improvement. The algorithm was based on inserting a secret into a host image, utilizing the least significant bits for the watermarking methodology, for the purpose of proving the authenticity and conformity of the fingerprint image. On the other hand, the goal behind encryption is to guarantee a secure transfer between communication peers. The advanced encryption standard was used in its CBC mode for this process. The choice of the technical materials was made due to the advantages provided. The experimental results show the efficiency of the proposed technique in terms of imperceptibility and similarity compared with the original host image. Furthermore, low computational complexity and high resistance were supplied thanks to the AES strength and sensitivity to minimal manipulations. Moreover, the comparison showed that the suggested scheme's results exceeded those of various recent methods, which proves the method's effectiveness. In the future, a robust watermarking technique will be adopted, and more focus will be put on the exploited crypto-system in order to reduce complexity and adapt the technique to users' day-to-day application fields.

ACKNOWLEDGMENT

This work was supported by Directorate General for Scientific Research and Technological Development (DGRSDT).

REFERENCES

[1] Jiang, W., Wang, X., Song, X., Liu, Q., Liu, X. (2020). Tracking your browser with high-performance browser fingerprint recognition model. China Communications, 17(3): 168-175. https://doi.org/10.23919/JCC.2020.03.014

[2] Jain, A.K., Ross, A., Prabhakar, S. (2004). An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1): 4-20. https://doi.org/10.1109/TCSVT.2003.818349

[3] Yogesh, P.R., Devane, S.R. (2018). Primordial fingerprinting techniques from the perspective of digital forensic requirements. In 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, pp. 1-6. https://doi.org/10.1109/ICCCNT.2018.8494064

[4] Hsu, L.Y., Hu, H.T., Chou, H.H. (2022). A high-capacity QRD-based blind color image watermarking algorithm incorporated with AI technologies. Expert Systems with Applications, 199: 117134. https://doi.org/10.1016/j.eswa.2022.117134

[5] Swain, M., Swain, D. (2022). An effective watermarking technique using BTC and SVD for image authentication and quality recovery. Integration, 83: 12-23. https://doi.org/10.1016/j.vlsi.2021.11.004

[6] Sha, Y., Sun, B., Cheng, X., Mou, J., Wang, L. (2022). Cross-plane colour image encryption scheme based on BST model and chaotic map. The European Physical Journal Special Topics, 231: 3249-3263. https://doi.org/10.1140/epjs/s11734-022-00566-x

[7] Niu, P.P., Wang, L., Wang, F., Yang, H.Y., Wang, X.Y. (2022). Fast quaternion log-polar radial harmonic fourier moments for color image zero-watermarking. Journal of Mathematical Imaging and Vision, 64(5): 537-568. https://doi.org/10.1007/s10851-022-01084-0

[8] Anand, A., Singh, A.K. (2022). Hybrid nature-inspired optimization and encryption-based watermarking for e-healthcare. IEEE Transactions on Computational Social Systems, 1-8. https://doi.org/10.1109/TCSS.2022.3140862

[9] Kasim, Ö. (2022). Secure medical image encryption with Walsh–Hadamard transform and lightweight cryptography algorithm. Medical & Biological Engineering & Computing, 60(6): 1585-1594. https://doi.org/10.1007/s11517-022-02565-5

[10] Haddad, S., Coatrieux, G., Moreau-Gaudry, A., Cozic, M. (2020). Joint watermarking-encryption-JPEG-LS for medical image reliability control in encrypted and compressed domains. IEEE Transactions on Information Forensics and Security, 15: 2556-2569. https://doi.org/10.1109/TIFS.2020.2972159

[11] Aminuddin, A., Ernawan, F. (2022). AuSR1: Authentication and self-recovery using a new image inpainting technique with LSB shifting in fragile image watermarking. Journal of King Saud University-Computer and Information Sciences, 34(8): 5822-5840. https://doi.org/10.1016/j.jksuci.2022.02.009

[12] Mata-Mendoza, D., Cedillo-Hernandez, M., Garcia-Ugalde, F., Cedillo-Hernandez, A., Nakano-Miyatake, M., Perez-Meana, H. (2022). Secured telemedicine of medical imaging based on dual robust watermarking. The Visual Computer, 38(6): 2073-2090. https://doi.org/10.1007/s00371-021-02267-3

[13] Garg, P., Jain, A.K. (2020). An invisible based watermarking technique for biometric image authentication. Materials Today: Proceedings. https://doi.org/10.1016/j.matpr.2020.11.141

[14] Shankar, A., Kannammal, A. (2021). A hybrid of watermark scheme with encryption to improve security of medical images. In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, pp. 226-233. https://doi.org/10.1109/ICICV50876.2021.9388616

[15] Moad, M.S., Kafi, M.R., Khaldi, A. (2022). A wavelet based medical image watermarking scheme for secure transmission in telemedicine applications. Microprocessors and Microsystems, 90: 104490. https://doi.org/10.1016/j.micpro.2022.104490

[16] Kamble, A., Agrawal, S.S. (2019). Wavelet based digital image watermarking algorithm using fractal images. In 2019 3rd International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp. 1220-1224. https://doi.org/10.1109/ICECA.2019.8822029

[17] Geetha, R., Geetha, S. (2020). Embedding electronic patient information in clinical images: an improved and efficient reversible data hiding technique. Multimedia Tools and Applications, 79(19-20): 12869-12890. https://doi.org/10.1007/s11042-019-08484-2

[18] Benseddik, M.L., Zebbiche, K., Azzaz, M.S., Sadoudi, S. (2021). Efficient interpolation-based reversible watermarking for protecting fingerprint images. In 2021 International Conference on Networking and Advanced

Systems (ICNAS), Annaba, Algeria, pp. 1-6. https://doi.org/10.1109/ICNAS53565.2021.9628987
[19] Zhang, Y. (2018). The unified image encryption algorithm based on chaos and cubic S-Box. Information Sciences, 450: 361-377. https://doi.org/10.1016/j.ins.2018.03.055
[20] Rachmawanto, E.H., De Rosal, I.M.S., Sari, C.A., Santoso, H.A., Rafrastara, F.A., Sugiarto, E. (2019). Block-based arnold chaotic map for image encryption. In 2019 International Conference on Information and Communications Technology (ICOIACT), Yogyakarta, Indonesia, pp. 174-178. https://doi.org/10.1109/ICOIACT46704.2019.8938443
[21] Sreenivasan, M., Sidhardhan, A., Priya, V.M., Thanikaiselvan, V. (2019). 5D combined chaotic system for image encryption with DNA encoding and scrambling. In 2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN), Vellore, India, pp. 1-6. https://doi.org/10.1109/ViTECoN.2019.8899479
[22] Gollagi, S.G., Srividya, R., Kumar, G.S., Pareek, P.K. (2021). A new method of secure image encryption by using enhanced RSA algorithm. In 2021 International Conference on Forensics, Analytics, Big Data, Security (FABS), Bengaluru, India, pp. 1-5. https://doi.org/10.1109/FABS52071.2021.9702550
[23] Almuhammadi, S., Al-Hejri, I. (2017). A comparative analysis of AES common modes of operation. In 2017 IEEE 30th Canadian conference on electrical and computer engineering (CCECE), Windsor, ON, Canada, pp. 1-4. https://doi.org/10.1109/CCECE.2017.7946655
[24] Hu, Q., Fan, X., Zhang, Q. (2019). An effective differential power attack method for advanced encryption standard. In 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), Guilin, China, pp. 58-61. https://doi.org/10.1109/CyberC.2019.00019
[25] Daemen, J., Rijmen, V. (1999). Rijndael/AES. Encyclopedia of Cryptography and Security, 520-524.
[26] National Institute of Standards and Technology. Advanced encryption standard (AES). CSRC, 26-Nov-2001. https://csrc.nist.gov/publications/detail/fips/197/final, accessed on 27 Apr., 2022
[27] Assafli, H.T., Hashim, I.A. (2020). Security enhancement of AES-CBC and its performance evaluation using the Avalanche effect. In 2020 3rd International Conference on Engineering Technology and its Applications (IICETA), Najaf, Iraq, pp. 7-11. https://doi.org/10.1109/IICETA50496.2020.9318803
[28] Vaidehi, M., Rabi, B.J. (2014). Design and analysis of AES-CBC mode for high security applications. In Second International Conference on Current Trends in Engineering and Technology-ICCTET 2014, Coimbatore, India, pp. 499-502. https://doi.org/10.1109/ICCTET.2014.6966347
[29] Artiles, J.A., Chaves, D.P., Pimentel, C. (2019). Image encryption using block cipher and chaotic sequences. Signal Processing: Image Communication, 79: 24-31. https://doi.org/10.1016/j.image.2019.08.014
[30] Pillai, A., Vasanthi, S.M., Kadikar, R., Amutha, B. (2018). Encryption analysis of AES-cipher block chaining performance in crypto-wall ransomware and SDN based mitigation. International Journal of Engineering & Technology, 7(2.24): 47-54.
[31] Savitri, N., Johan, A.W.S.B., Firnanda Al Islama, A., Utaminingrum, F. (2019). Efficient technique image encryption with cipher block chaining and gingerbreadman map. In 2019 International Conference on Sustainable Information Engineering and Technology (SIET), Lombok, Indonesia, pp. 116-119. https://doi.org/10.1109/SIET48054.2019.8986084
[32] Shehu, Y.I., Ruiz-Garcia, A., Palade, V., James, A. (2018). Sokoto coventry fingerprint dataset. arXiv preprint arXiv:1807.10609. https://doi.org/10.48550/arXiv.1807.10609
[33] Naffouti, S.E., Kricha, A., Sakly, A. (2022). A sophisticated and provably grayscale image watermarking system using DWT-SVD domain. The Visual Computer, 1-21. https://doi.org/10.1007/s00371-022-02587-y
[34] Wang, H., Ho, A.T., Li, S. (2014). A novel image restoration scheme based on structured side information and its application to image watermarking. Signal Processing: Image Communication, 29(7): 773-787. https://doi.org/10.1016/j.image.2014.05.001
[35] Patro, K.A.K., Acharya, B. (2019). An efficient colour image encryption scheme based on 1-D chaotic maps. Journal of Information Security and Applications, 46: 23-41. https://doi.org/10.1016/j.jisa.2019.02.006
[36] Tanveer, M., Shah, T., Rehman, A., Ali, A., Siddiqui, G.F., Saba, T., Tariq, U. (2021). Multi-images encryption scheme based on 3d chaotic map and substitution box. IEEE Access, 9: 73924-73937. https://doi.org/10.1109/ACCESS.2021.3081362
[37] Yao, F.F., Yin, Y.L. (2005). Design and analysis of password-based key derivation functions. In: Menezes, A. (eds) Topics in Cryptology – CT-RSA 2005. CT-RSA 2005. Lecture Notes in Computer Science, vol 3376. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-30574-3_17
[38] Hasnat, A., Barman, D., Mandal, S.N. (2016). A novel image encryption algorithm using pixel shuffling and pixel intensity reversal. In 2016 International Conference on Emerging Technological Trends (ICETT), Kollam, India, pp. 1-6. https://doi.org/10.1109/ICETT.2016.7873740
[39] Daoui, A., Karmouni, H., Sayyouri, M., Qjidaa, H. (2022). Robust image encryption and zero-watermarking scheme using SCA and modified logistic map. Expert Systems with Applications, 190: 116193. https://doi.org/10.1016/j.eswa.2021.116193
[40] Nazir, H., Bajwa, I.S., Abdullah, S., Kazmi, R., Samiullah, M. (2022). A color image encryption scheme combining hyperchaos and genetic codes. IEEE Access, 10: 14480-14495. https://doi.org/10.1109/ACCESS.2022.3143096