

Received July 23, 2020, accepted August 5, 2020, date of publication August 11, 2020, date of current version August 24, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3015687

A New Fuzzy-DNA Image Encryption and Steganography Technique

SAID E. EL-KHAMY¹, (Life Fellow, IEEE), NOHA O. KORANY¹,
AND AMIRA G. MOHAMED², (Student Member, IEEE)

¹Electrical Engineering Department, Faculty of Engineering, Alexandria University, Alexandria 11865, Egypt

²Electrical Engineering Department, Alexandria Higher Institute of Engineering and Technology, Alexandria 11865, Egypt


Corresponding author: Amira G. Mohamed (eng_amira90@yahoo.com)

ABSTRACT Image encryption and steganography techniques are receiving a lot of interest and investigations due to their high importance in multimedia communication systems. A novel highly efficient image encryption and steganography technique are presented in this paper. For the first time, the proposed technique uses hybrid DNA encoding and Choquet's Fuzzy Integral sequences. At first, a confused version of the image, using a simple chaotic map, is encoded using DNA's bases. Four coded images are generated using the four DNA bases, namely AT, CG, GC, and TA. Parallel to that, a Choquet's fuzzy Integral sequence is generated and DNA encoded similarly to obtain four pseudo-random sequences. Secondly, the resulting four fuzzy/DNA sequences are used to diffuse the four DNA encoded images using the complementary DNA XOR rule, according to certain control code. Finally, the wavelet fusion algorithm is then used to fuse the resulting four fuzzy-DNA encoded images, to get the encrypted image. For added security, a new steganography approach is used. In particular, the encrypted image is divided into four sub-images, each of which is hidden in a different carrier image selected from a known group of carrier images according to a given key. The simulation results and security analysis confirmed the efficiency of the proposed image encryption algorithm as well as the steganography approach used for enhanced security. Ten different images with a size of 256×256 are used to test the proposed method. The results show that the proposed algorithm has a higher key sensitivity. The pixel correlation coefficient values are very small (between $5.3220e-04$ and 0.0011 horizontally, between $8.7670e-04$ and 0.0022 vertically and between 0.0002 and 0.0045 diagonally). Furthermore, the measured information entropy of the encrypted images is between 7.9970 and 7.9979 which are very close to the ideal value of 8 . Additionally, the measured unified average changing intensity and number of pixels change rate values take the values between 33.46 and 33.39 and between 99.61 and 99.64 , respectively, which are again closed to the ideal values. The steganography test shows that the hidden encrypted images are almost invisible at high values of SNR and are characterized by good NCC values under different types of attacks. The performance of the new proposed algorithm is proved to overcome many other previously published image encryption techniques.

INDEX TERMS Image encryption, steganography, Choquet fuzzy integral, DNA technique, DWT fusion, chaotic maps.

I. INTRODUCTION

There has been a quantum leap in the last few years in the fields of digital communication and networking technologies. Huge amounts of data have been shared and communicated through open networks. This trend is not expected to stop anytime in the future, so it is important to find different

The associate editor coordinating the review of this manuscript and approving it for publication was Ismail Butun .

methods to secure data transferred over the different networks. Many domains have been created and used for data protection, including steganography, and watermarking. They depend on using media to hide information. For instance, cryptography is used to safeguard written messages, whereas a cipher (the coded equivalent of a message) is created from the original plaintext. An encryption algorithm is used for this process. To decrypt a message, the recipient needs to have a secret key to convert the cipher back into the original text.

To encrypt data, many methods have been employed. This includes DES or Data Encryption Standard, SDES or Simplified Data Encryption Standard, AES or Advanced Encryption Standard. However, images possess certain features that make all these methods inappropriate for their encryption, i.e., strong connection between the various pixels and high recurrence [1]–[5].

With the development of the fuzzy integral, it was found that it would be quite beneficial in image encryption, due to its many benefits, including its ease of use, high security, high speed, and high sensitivity [6]–[8]. Fuzzy integral is used to integrate all fuzzy sets. This is the opposite of ordinary definitions of a fuzzy integral. It can integrate fuzzy sets to the used fuzzy measure space. However, these sets have to not be united by an estimate. The fuzzy integral expresses a finite set that requires a fuzzy measure. Fuzzy rules are needed for the function of fuzzy measures. A Choquet fuzzy integral (CFI) is the output of these rules, achieved through the defuzzification process [9]–[11].

Many scientific fields, including Mathematics, computer science, and chemistry have been using DNA's biological structure since Adelman's work on the issue. This structure is used when attempting to encrypt storage spaces, especially large ones, as well as enormous parallelism, and ultra-low power consumption. There have been many DNA-dependent schemes, which have been studied with success recently. They mostly rely on the dynamic rule of ranges, which is used as a secret key for building. When encoding, the rules of DNA can be applied in one of two methods. The first is that every single pixel of an image, having an 8-bit gray value, is turned into a sequence of four DNA codes. This way the complexity of the image is reduced when it is encrypted. The second is that a cipher image is generated out of the plain encoded image, as per certain rules related to DNA [5].

If someone is trying to hide certain secret data in a cover media, this would be called steganography. This act mainly depends on human imperceptibility, in case of images and inaudibility, when the information being hidden is audible. A stego file is the result of a file that includes hidden information, using one of the following strategies: Least Significant Bit (LSB), Discrete Cosine Transform, (DCT) and Discrete Wavelet Transform (DWT) [12]–[15]. Even though both cryptography and steganography provide good security, there have been attempts to merge them into one method that has good not only good concealment but also high security.

Choquet's fuzzy integral is highly sensitive, complex, and nonlinear, properties that provide high security. Thus, it is used to encrypt images, which will be described in this paper. Seven steps are applied to use the algorithm described in this paper. **First**, a binary sequence of 8-bit in length is generated out of the original images. **Second**, a simple chaotic map is used to shuffle the binary stream. **Third**, DNA's complementary rule is used to encode the shuffled image. **Fourth**, according to DNA's four types of nitrogenous bases, four images are extracted from the encoded and shuffled image. They are AT, CG, GC, and TA. This is a new concept.

Fifth, the DNA random sequences are used to diffuse each of the four blocks that each image is split into. The previously random sequences described are generated from the Choquet fuzzy integral (CFI). This takes place while using a control code. A key made of two components is of dependence by the CFI. The components are used to create the initial condition of the CFI. These two components are the external secret key of the finite length and a secret image, which can be a signature, a stamp, or something different. This parameter is employed to enhance the security level. Both components are diffused together, creating the primary condition and parameters of the CFI. The NIST random test package was used to test the generated sequences and the results obtained were quite positive. However, these results proved that a single bit of change in the PN key produces uncorrelated sequences, which are very different; making sequence generation highly sensitive to any alteration in the image or PN key [16]. **Sixth**, an encrypted image is produced through the fusion of the resulting images by DWT. As for the **seventh** step, it works on improving the security of the suggested technique. This takes place through the division of the encrypted image into four sub-images. These are hidden in a carrier or a set of images, through steganography. **Finally**, different tests are used to check the security of this process. They include the following techniques tested under various attacks: histogram, entropy, the correlation between adjacent pixels, key sensitivity and differential attack analysis as well as the steganography with the imperceptibility and the robustness tests, under different attacks.

As for the remainder of the paper, it consist of the following: Related work in section II, a brief report on fuzzy measure and the Choquet fuzzy integral is described in section III, a description of the biological characteristics of DNA in section IV, the proposed cryptosystem in section V, the results of the study in section VI, security testing of the proposed system in section VII, the steganography test in section VIII, and the conclusion of the study in section IX.

II. RELATED WORK

This section will take a look at some of the previously studied aspects of image encryption. It will also demonstrate a merge between the methods of cryptography and steganography. In a previous study, an image was encrypted using the phase-truncated short-time fractional Fourier transform, as well as the hyper-chaotic system [17]. PTSTFRFT is different from coding done through traditional phase truncation in that it was combined with wave-based permutation. This is done in order to construct the EU or the encryption unit, used to code sub-images. In this encoding, the amplitude information is recombined with the confusing phase information. Another study suggested using the three dimensions of a chaotic map to encrypt color images. The map produces three numbers diffused through RGB channels of the image [18]. The next step was to divide the image into 4×4 parts. Then each of these parts' location is changed and is also divided into 16×16 blocks. Each of these blocks is then permuted using different

keys of a certain map. When all blocks have been permuted, the encrypted image is created. A different study proposed using an approach that uses compressed sensing as well as multi-image cross pixel scrambling to encrypt a color image. According to the tricolor theory, the image is divided into three sub-images, which are then processed sparsely using the discrete wavelet transform. To see these images, different Gaussian random matrices are used [19]. It was proposed to encrypt image using a generated random key stream and self-processing [6]. CFI produces pseudo-random sequences, for example a 128-bit key was used to produce the parameters of CFI. Following this step, each half of an image's data was used to shuffle the other half of the image and vice-versa. In study [7], it was proposed to perform the encryption of an RGB color image by using CFI based key stream generator. CFI yielded a certain output that was used to shift the bits of the three gray-level components randomly. Then, a coupling of the generated key stream and the three components of RGB color pixels was performed to encrypt the permuted components. In study [20], the following process took place: information to be hidden was encrypted using the Elliptic Curve Cryptography algorithm; then, the LSB Inversion algorithm was used to insert the encrypted data into a cover object. Several modes of attack were used to test the security of this method. These modes included visual, histogram, and chi-square attacks. In study [1], it was suggested to apply the LSB of the chaos-based audio steganography and the one-time pad of the cryptography method. To encrypt data, a key for one-time pad was used, it was made of a sequence of PWLCM. To hide a certain message, a random sequence was generated from the logistic map. The encrypted data was hidden in the host audio samples in some random positions of the LSB through indices of the ordered generated sequence. Cryptography and steganography were combined into one algorithm and shown [21]. The new steganography algorithm was used to encrypt and hide the data in an image, which was then divided into four level blocks. Depending on a key, the data will be hidden in the four diagonal sub-block values.

III. FUZZY MEASURE AND CHOQUET FUZZY INTEGRAL

A nonlinear aggregation tool is made from the combination the Choquet fuzzy integral and the fuzzy measure to produce a sequence of high security [10], [16], [22]. This paper tests this approach. CFI has certain characteristics, summarized as follows:

A. FUZZY MEASURE

There are different classes of fuzzy measures; they include probability (a subset of classical measures), plausibility, necessity, possibility, and belief measures. The following equations mark the method of determining a fuzzy measure [23], [24]:

$$F(A_1) = g_1 \tag{1}$$

$$F(A_i) = g_i + F(A_{i-1}) + \lambda g_i F(A_{i-1}), \quad 1 < i < n \tag{2}$$

where the membership grade is g_i and $F(A_i)$ is the fuzzy measure over the corresponding membership grades.

B. SUGENO λ MEASURE

A very similar type of measure to probability is the Sugeno measure. It is a very specific type of fuzzy measure that deals with $g(A \cup B)$ state of probability reconstruct. The value of λ measures represents the variance between the Sugeno measure and the previously mentioned state $\lambda \in [-1, \infty]$ is a real-valued parameter, which can be calculated using the following equation [25]:

$$1 + \lambda = \prod_{i=1}^n (1 + \lambda g_i) \tag{3}$$

C. CHOQUET FUZZY INTEGRAL

To calculate the Choquet fuzzy integral, one must depend on the Sugeno λ and the fuzzy measures. The CFI is more complex and nonlinear. The following equation is used in the calculation of the CFI [11]:

$$CFI = \int h dg = \sum_{i=1}^n [h(x_i) - h(x_{i-1})] F(A_i) \tag{4}$$

where h is the initial input of the Choquet fuzzy integral.

IV. BIOLOGICAL BACKGROUND OF DNA

The human body is composed mainly of DNA or deoxyribonucleic Acid. It marks the storage space for human genetic information, which contains information about each's person's growth, development and procreation. One molecule of DNA carries an extremely large amount of information in its consolidated structure. It is a polymer of nucleotides made essentially of four nitrogenous bases. Two of them are the two-ringed purines, Guanine (*G*) and Adenine (*A*), and the other two are the single-ringed pyrimidine, Cytosine (*C*) and Thymine (*T*) [5].

A. DNA SEQUENCE ENCRYPTION

A string of DNA contains the four basic nucleotides arranged in sequence. The letters G, C, A, and T, represent Guanine, Cytosine, Adenine and Thymine, respectively, where the first two are complementary, as well as the last two. One and zero are also complementary in the binary system. The same applies to 01 and 10 and also 11 and 00. Thus, the 24 schemes shown in Table 1 DNA coding, as per the standards of complementation of DNA coupling.

TABLE 1. The encoding rules for DNA sequences.

Bases	Rule 0	Rule 1	Rule 2	Rule 3	Rule 4	Rule 5	Rule 6	Rule 7
A	00	00	01	10	10	01	11	11
G	10	01	00	00	11	11	01	10
C	01	10	11	11	00	00	10	01
T	11	00	11	10	01	10	00	00

Certain mathematical and biological computation are introduced to enable the use of DNA in cryptography. These include exclusive and XOR. The binary formation is used

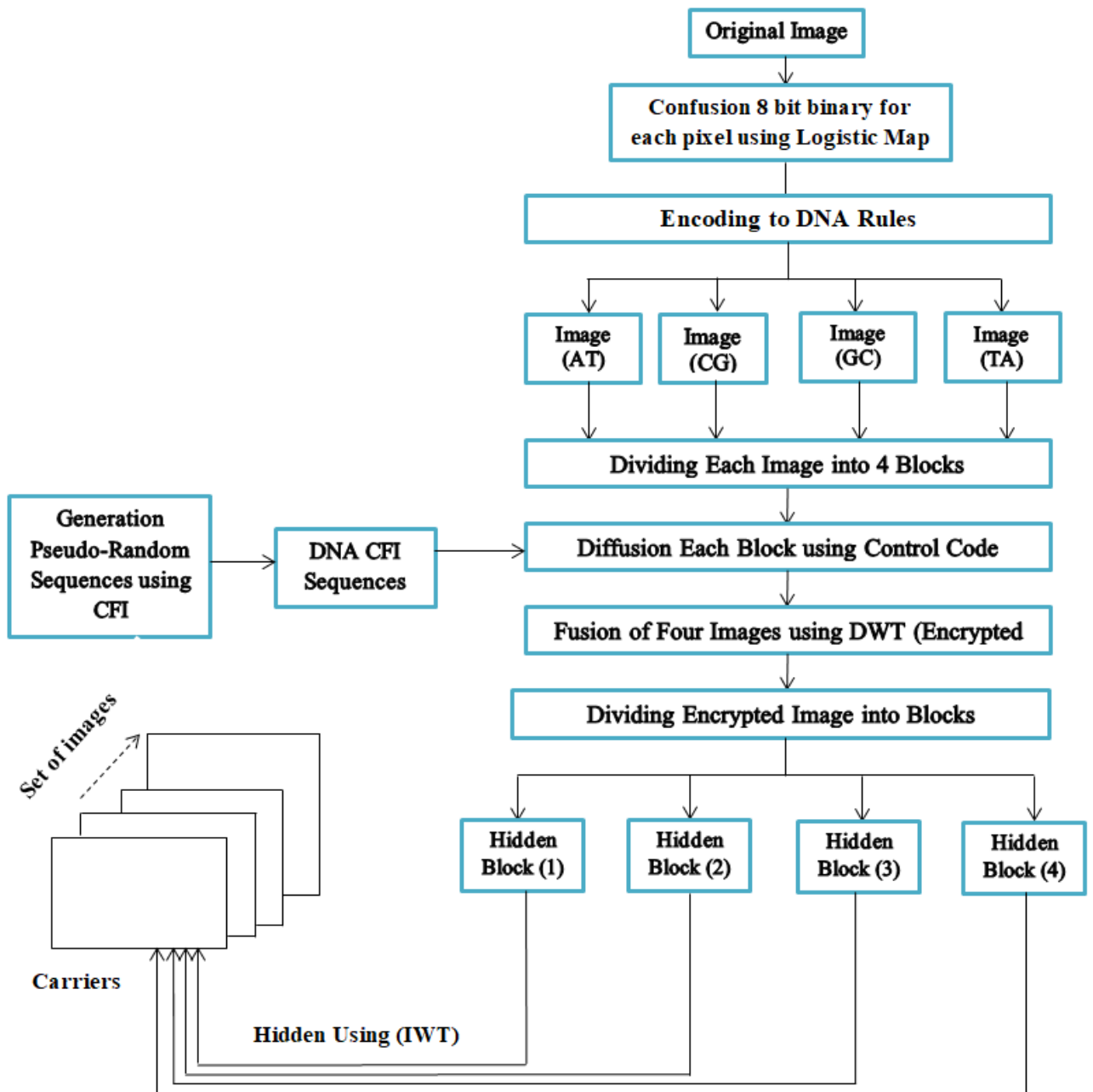


FIGURE 1. Block diagram of the proposed algorithm.

in sequencing DNA according to the XOR operations. Eight types of DNA XOR rules are available and represent the eight types of encoding rules. Rule 2, seen in Table 2, is used for the sake of this paper.

V. THE PROPOSED CRYPTOSYSTEM

This part of the paper describes the algorithm used to encrypt images, which will later be hidden in a group of images. In step one, CFI is used to generate pseudo-random sequences which our work was presented in [16]. In step two, a simple chaotic map is used to confuse one version of the image,

TABLE 2. DNA XOR operations using Rule 2.

	A	C	G	T
A	A	C	G	T
C	C	A	T	G
G	G	T	A	C
T	T	G	C	A

which results in coded using DNA, according to the four nitrogenous bases. This image is divided into four images, as per the AT, CG, GC, and TA bases of DNA. At the same time, DNA bases are also used to encode the random

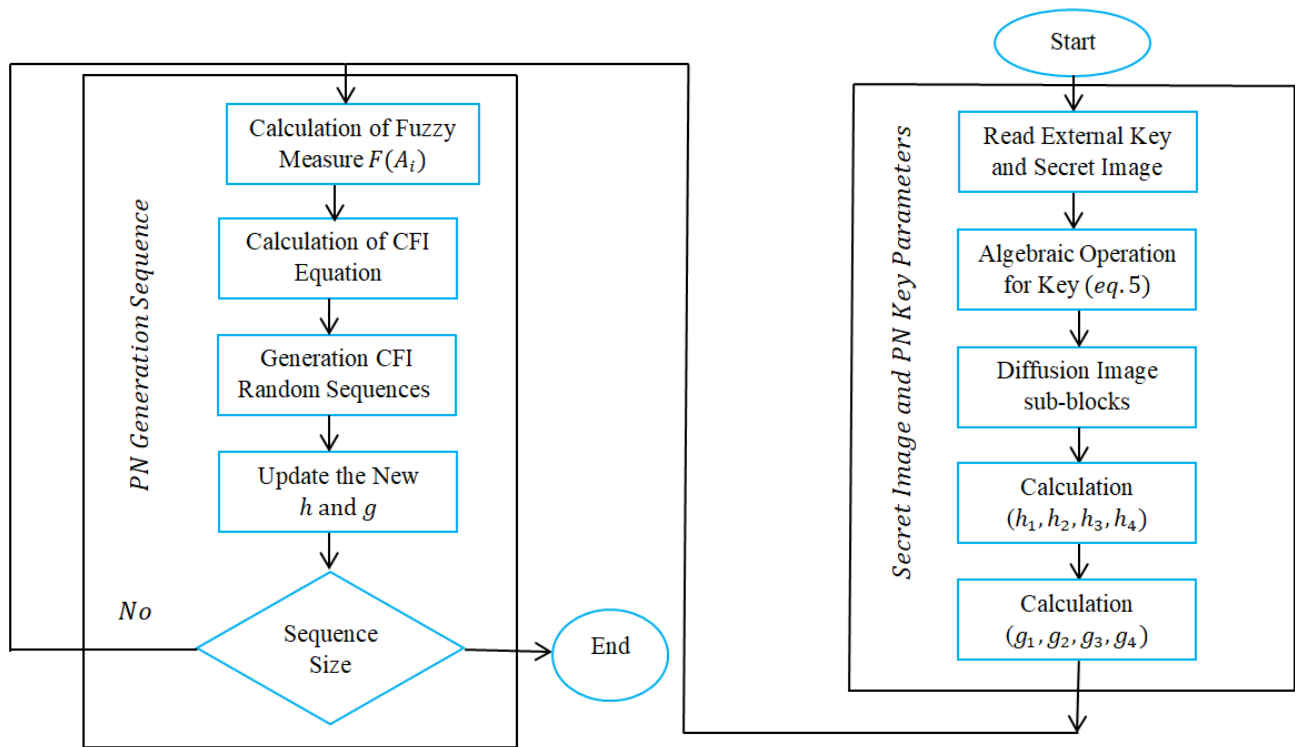


FIGURE 2. Generation of pseudo-random sequences.

sequences of Choquet Fuzzy Integral. Out of the encoded images, four blocks arise as a result of splitting. Then, the diffusion of the pixels of each block and random DNA fuzzy sequences is carried out using the XOR DNA complementary rule by applying a control code. To construct an encrypted image, the four blocks are combined using DWT. The final step of this process is hiding the four sub-images split from the encrypted image into a carrier using IWT. This step is undertaken to increase the security of the process. Figure 1 shows the structure of the suggested encryption. For more details regarding the steps taken, following are more illustrations:

Step 1:

The pseudo-random sequence from CFI utilized for encryption is shown in Figure 2 with a brief description of its generation. The external key and the secret image are used to calculate the initial input of the CFI, h_1, h_2, h_3, h_4 . At the key level, the image can be any type of file, including signatures, icons, etc.

- The 128-bit secret key is made of session keys, $(K_1, K_2, \dots, K_{16})$, i.e., 8-bit long blocks.
- The following equations are used to calculate the Key parameter A, B, C, D :

$$A = (K_1 \oplus K_2 \oplus K_3 \oplus K_4) \tag{5}$$

$$B = (K_5 \oplus K_6 \oplus K_7 \oplus K_8) \tag{6}$$

$$C = (K_9 \oplus K_{10} \oplus K_{11} \oplus K_{12}) \tag{7}$$

$$D = (K_{13} \oplus K_{14} \oplus K_{15} \oplus K_{16}) \tag{8}$$

$$K = \sum_{i=1}^{i=16} (K_i) \tag{9}$$

- The image used has a size of 256×256 and its gray level matrix is inserted.
- It is then divided into blocks of 2×2 , the result are four values of $I(s)$, using XOR for each of the gray levels within each block.
- The initial inputs can be calculated as the following equations:

$$h_1 = ((A + K) \text{ mod } 256) \oplus I(1) \tag{10}$$

$$h_2 = ((B + K) \text{ mod } 256) \oplus I(2) \tag{11}$$

$$h_3 = ((C + K) \text{ mod } 256) \oplus I(3) \tag{12}$$

$$h_4 = ((D + K) \text{ mod } 256) \oplus I(4) \tag{13}$$

where $I(1), I(2), I(3)$, and $I(4)$ are the diffused values for each block by using XOR and K is the sum of blocks for the secret key.

- Eq.(14) is then used to calculate membership grades g from h [26].
- Following this step λ is calculated using Eq. (3). Its value is then substituted in Eq.(2) to obtain the fuzzy measure $F(A_i)$.

$$g_i = \frac{1}{1 + h_i} \tag{14}$$

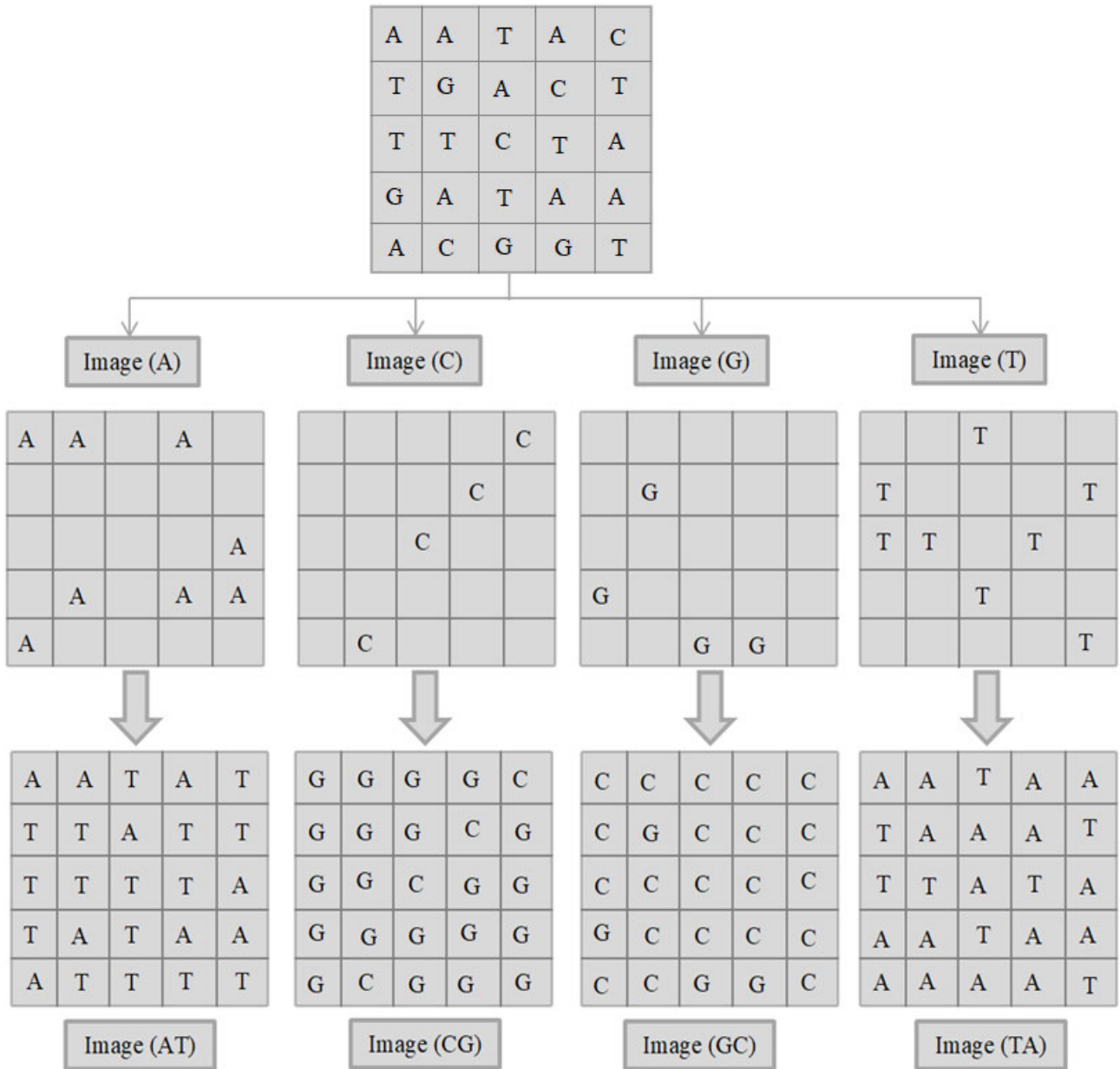


FIGURE 3. Description of the extraction of the four DNA images.

- The initial inputs h_1, h_2, h_3, h_4 as well as the fuzzy measure $F(A_i)$ are used to calculate the CFI through the use of Eq. (4).
- Finally, The secure random sequences from the fuzzy integral value CFI as follows:

$$C_j = (ARS(int(CFI \text{ mod } 1) \times 10^{14}, S)) \text{ mod } 256 \quad (15)$$

In the previous equation, ARS represents the arithmetic right shift for the binary sequence, as for the normalized fraction value, it is represented by $(CFI \text{ mod } 1)$. As S assumes values from 0 to 7, a different four random sequences (C_1, C_2, C_3, C_4) can be generated. The length of the sequence is reached after repeating the previous steps. Thus, the initial

input values are updated as such:

$$h_j = C_j \text{ mod } 256, \quad j = 1, 2, 3, 4 \quad (16)$$

Step 2:

In this step, 8-bit binary sequences are issued out of each pixel of the plain image, which are then shuffled with the help of a logistic map. These systems are a form of chaotic systems. They have the following characteristics: control parameters (λ), an initial condition of (X_0), and an output of (X). As for the input variables, they are expressed as:

$$x_{n+1} = \lambda x_n (1 - x_n) \quad (17)$$

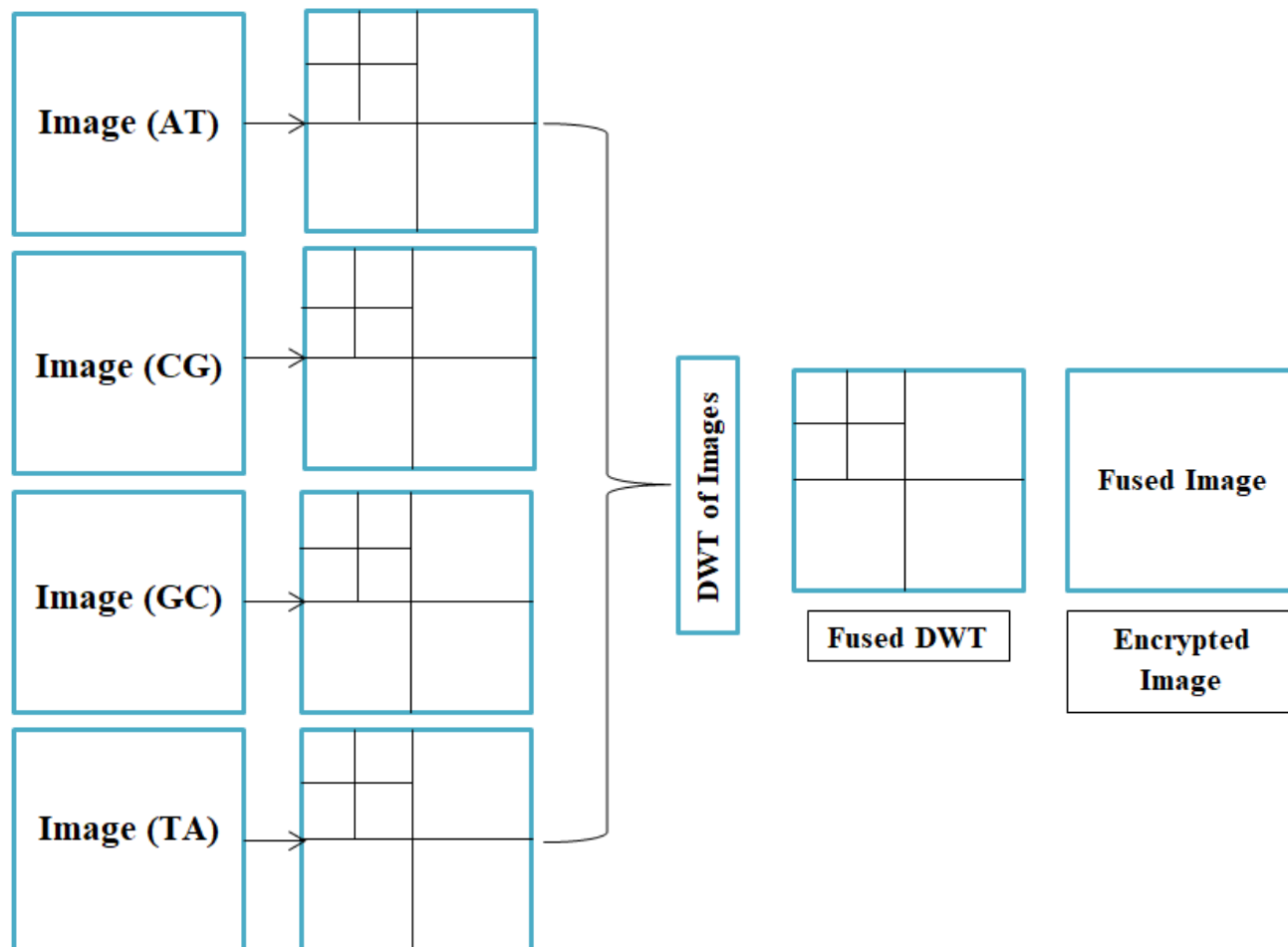


FIGURE 4. Description of the fusion image using DWT.

where the chaotic parameter is λ and the number of iterations is n . $\lambda \in [0, 4]$, $x \in [0, 1]$ in which the chaotic attitude is realized when $\lambda \in [3.57, 4]$.

Step 3:

- Table 1 shows the DNA-inspired, according to which the image is encoded. For the purpose of this research, when DNA’s nitrogenous bases are transformed into the binary system, A means 00, C means 01, G means 10, and T means 11. The length of the DNA-inspired sequence for each pixel is four. For example, the first pixel, which has a value of 220, is transformed into the following binary code [11011100]. This pixel can be DNA encoded as such TCTA, whereas A, C, G, T indicate 00, 01, 10, 11, respectively.
- The four images (A, C, G, and T), each represented by one of the nitrogenous bases, are extracted from the image which was encoded and permuted. The empty spaces of each image are replaced by its complement. For instance, the empty spaces of image (A) are replaced with its complement (T), image (C) with its complement (G), and so on.

- The four images are renamed to (AT, CG, GC, and TA). This step is illustrated in Figure 3. Also, the generated fuzzy sequences from the first step are coded using DNA.

Step 4:

- In the next step, four blocks are obtained from the division of each of the DNA images. A different random fuzzy sequence is used to XOR each of the blocks.
- For each of the blocks, a random sequence is selected from a control code with four different sequences. For example, when image AT is divided into four blocks.
- The four random sequences are selected by the control code to encrypt each of the blocks, where (C_1) encrypts the fourth block, (C_2) encrypts the third block, (C_3) encrypts the first block, and (C_4) encrypts the second block. This takes place for each image.
- After that, every DNA image is converted into a binary based on Table 1. Then, each element is transformed into a decimal number.

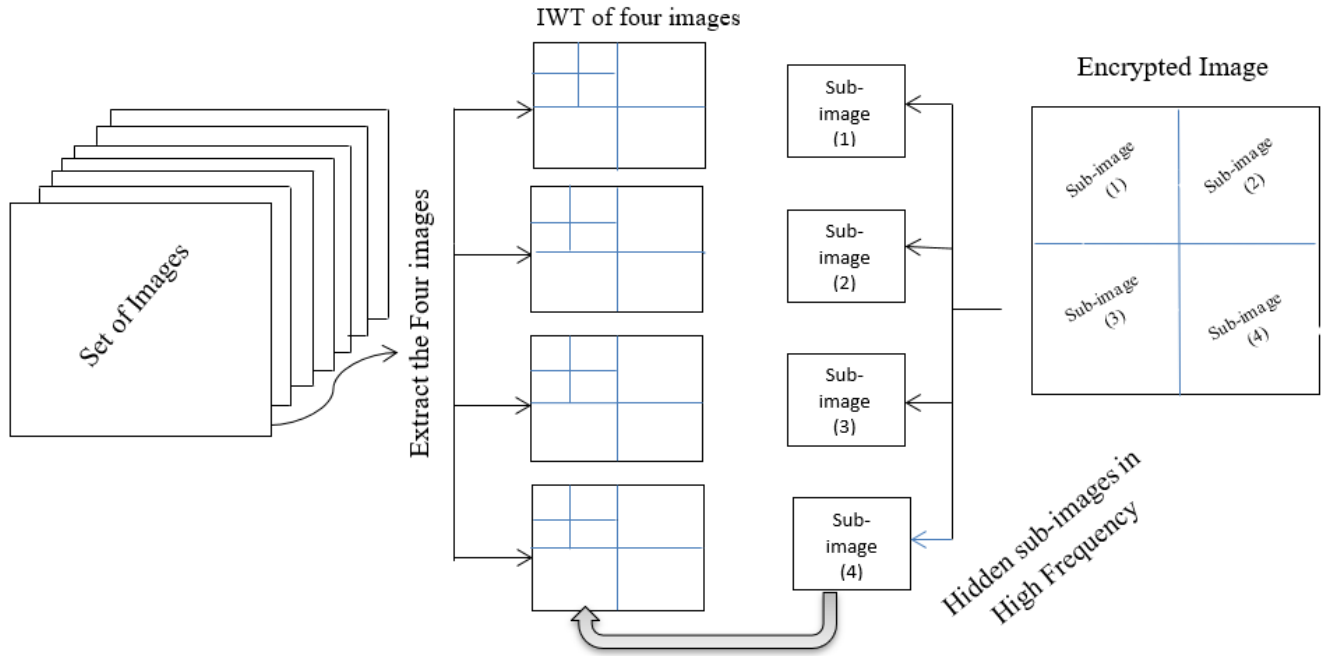


FIGURE 5. Description of embedding the secret image.

- DWT (Discrete Wavelet Transform) is used to combine the four registered inputs that were encrypted. Figure 4 shows image fusion and how it is carried out.

Step 5:

“After the encryption process described in the previous step, the encrypted image is hidden into a group of carriers imaged using the integer wavelet transform (IWT) technique [14], [15]. IWT is selected as it is a more efficient approach than DWT. The coefficients in IWT are represented by finite precision integer numbers which allow for lossless encoding. This transform maps integers to integers, whereas in the case of DWT, if the input consists of integers (as in the case of images), the resulting output no longer consists of integers. Thus, the perfect reconstruction of the original image becomes difficult.

In the adopted steganography technique, the encrypted image is divided into four sub-images, each of which is hidden in a different carrier image selected from a known group of carrier images according to a given key. Each of the carrier, or cover, images is transformed using the second level of IWT to obtain four sub-bands (LL2, HL2, LH2 and HH2). The secret data, representing one quadrant of the encrypted image is embedded in the high-frequency coefficients (HH2 sub-band) of the IWT of the corresponding carrier image.”

- Steps to Embed an image

- 1- Reading the set of images.
- 2- Selecting the four images and applying one level wavelet transform to each image.
- 3- Reading the secret image.

- 4- Dividing the secret image into four blocks.

5- Embedding each block in the high-frequency coefficients produced from Integer Wavelet Transform in the chosen locations of details coefficients as shown in Figure 5.

- Steps of Image Extraction

A set of images is sent to the receiver. To extract the four images, a password is needed, and the previously described steps are done in reverse order. Figure 6 shows how the extraction process is accomplished. The following steps are used:

- 1- Inserting password for extraction the four images which the four blocks are hidden in it;
- 2- Applying the integer wavelet transform to each image;
- 3- Extracting the four sub-images;
- 4- Decrypting the sub-images using the DNA rules and the fuzzy integral to obtain the final image.

VI. EXPERIMENTAL RESULTS

To apply the new algorithm, MATLAB R2015 is used for computer simulation with gray scale images size 256×256 . Two stages make the components of the new algorithm. Figure 7 shows the first stage which makes up the encryption process and Figure 8 shows the second stage which is the steganography process.

VII. SECURITY ANALYSIS OF IMAGE ENCRYPTION

To ensure the security of the encrypted image, a performance analysis is applied. This includes security against brute-force attacks. Details of the security analysis are described in this section. This analysis includes the following aspects:

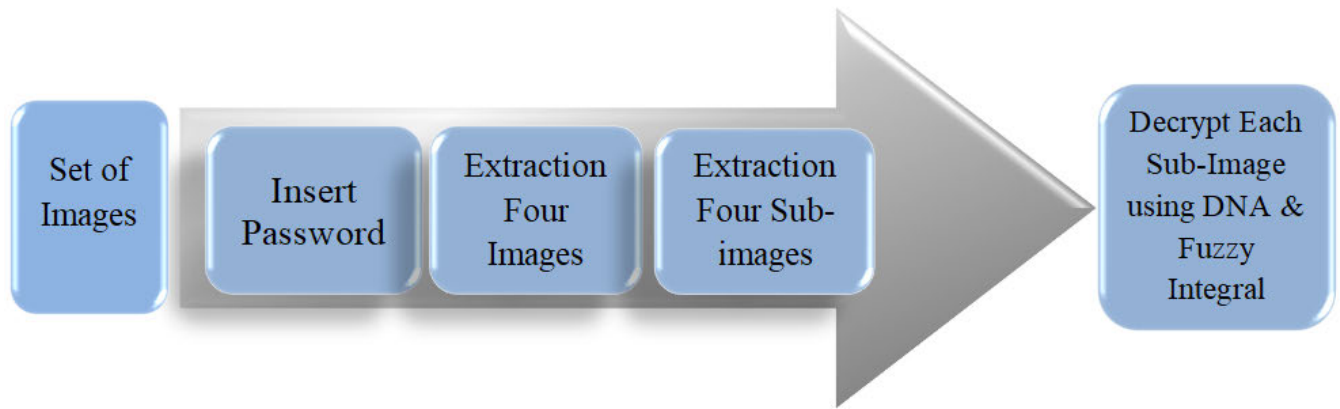


FIGURE 6. Description of the extraction of the secret image.

correlation tests between two adjacent pixels, information entropy, key sensitivity, histogram, and differential attack, including the mean square error, the unified average changing intensity and the number of pixel change rate are demonstrated [27]–[29].

A. DIFFERENTIAL ATTACK

To find out the relationship between the original image and the encrypted one, attackers resort to changing one pixel in the original image. This type of attack, the differential attack, would lose its effect if a minimal change in the original image would lead to a significant change in the encrypted one. Three different measures testing the effect of a single-pixel variation on the encrypted image are employed in this paper [30].

1) AVALANCHE EFFECT

In the case of the avalanche effect, a major change in the encrypted image is obtained from the modification of the encryption key or a change in the original image. The avalanche effect happens when 50% of the bits of the encrypted image are changed from just a single-bit change in the original one. To test for the avalanche effect, the modified bit should be determined from the keys. If MSE is ≥ 30 dB, then there is a major variation between the two images. MSE can be calculated using Eq.(18) [30]–[32]:

$$MSE = \frac{1}{M * N} \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [C_1(i, j) - C_2(i, j)]^2 \quad (18)$$

If C_1 and C_2 are two encrypted images, which differ by one bit in the key used in their encryption. Table 3 shows the results of MSE by changing one bit in the key. It is shown that the values MSE of the proposed algorithm are greater than 30 dB, which proves that the proposed algorithm is sensitive to the variation of the key.

2) NUMBER OF PIXEL CHANGE RATE (NPCR)

NPCR, calculated using Eq.(19), marks the percentage of pixels changed in the cipher image corresponding to the pixel

TABLE 3. Avalanche effect.

Algorithms	Images (256 × 256)	Mean Square Error (dB)
Ours	Lena	40.8409
	Airplane	40.4164
	Boat	40.8749
	Cameraman	40.8213
	Peppers	40.9365
	Tree	40.0048
	Truck	40.6574
	Girl	40.7734
	Baboon	40.7912

variation of the original image [30], [33], [34]:

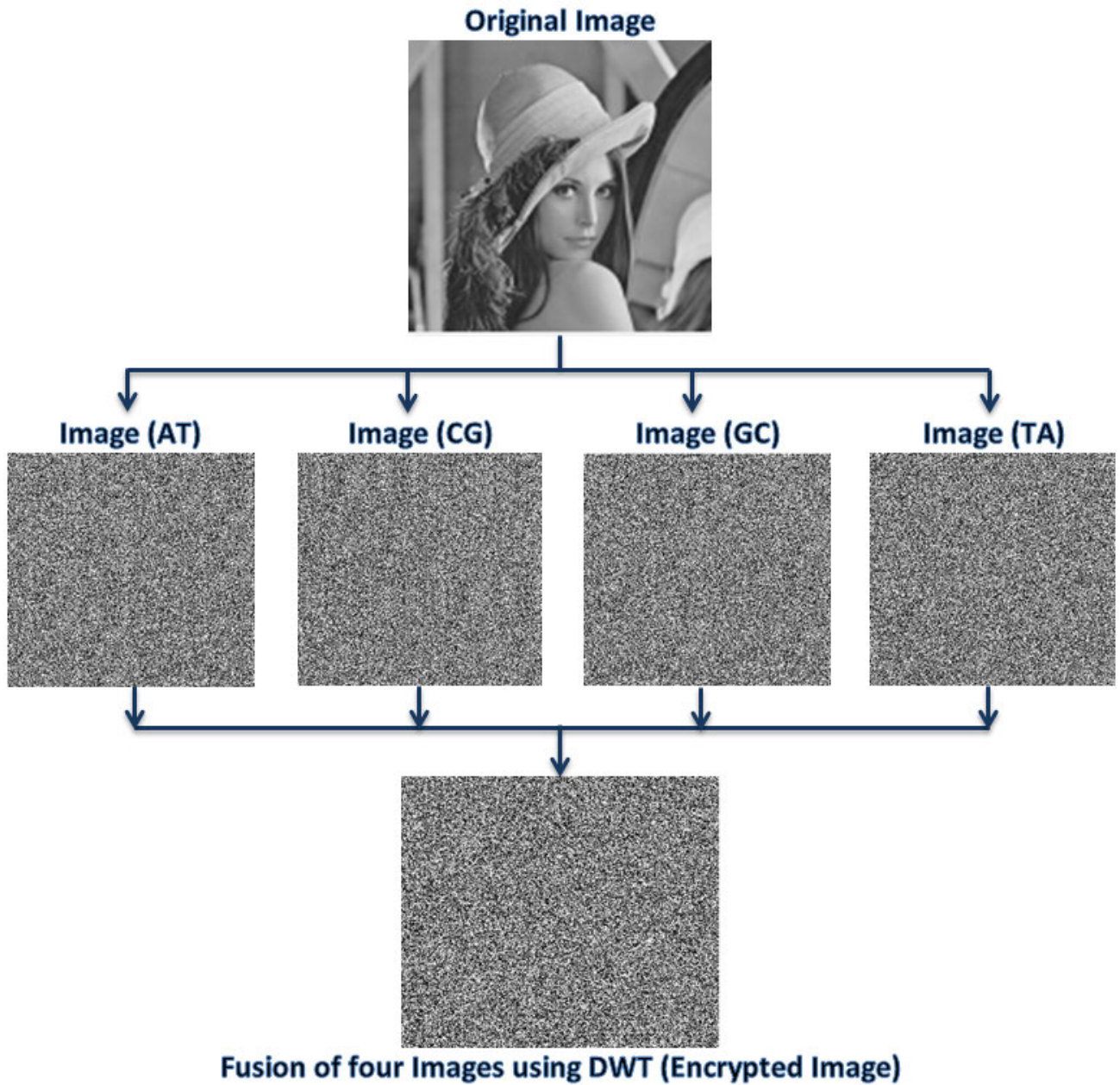
$$NPCR = \frac{\sum_{i,j} D(i, j)}{M * N} * 100 \% \quad (19)$$

3) UNIFIED AVERAGE CHANGING INTENSITY (UACI)

The average intensity of variation between two images is calculated using UACI, this takes place when a major variation in the encrypted image takes place as a small variation in the original image happens. It is calculated using Eq.(20) [30], [33], [34]:

$$UACI = \frac{\sum_{i,j} E_1(i, j) - E_2(i, j)}{255 * M * N} * 100 \% \quad (20)$$

where M and N represent the length and width of the image, respectively, $E_1(i, j)$ and $E_2(i, j)$ represent the corresponding cipher image pixel values before and after the plain image variation, respectively. The UACI and NPCR values are shown in Table 4, it can be shown that the NPCR results are close to ideal value 99.6094% and the UACI results are close to ideal value 33.4635 %, which displays that the proposed algorithm is highly sensitive to little variations of the plain image and then can resist differential attack. The NPCR and UACI decryption metrics have also been calculated. The values of NPCR and UACI have been estimated to be Zero, as after the decryption procedure, the decrypted image and the original image are identical with no missing packets or changes between them.



□

FIGURE 7. Encryption process.

B. CORRELATION COEFFICIENT

The quality of encryption of a cryptosystem can be measured through the calculation of the correlation coefficient. Thus, this calculation is considered useful in the analysis of the performance of the encryption. The correlation coefficient marks the relation between any two variables. This coefficient reaches zero or is very close to it when the original image and the encrypted one are different. The correlation coefficient is calculated for various positions of the encrypted, as well as the original images. They are the horizontal, the vertical, and the diagonal positions. The formula below is used to calculate

the correlation coefficient [30], [41], [42]:

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)} * \sqrt{D(y)}} \tag{21}$$

where r_{xy} is the correlation coefficient and COV is the covariance between pixels (x) and (y), where (x) and (y) are the gray scale values of two pixels in the same place in the plaintext and cipher-text images, respectively. D(x) is the variance and E(x) is the mean. Multi images encrypted with the proposed algorithm's correlation distribution can be seen in Table 5, which shows that the performance of this algorithm

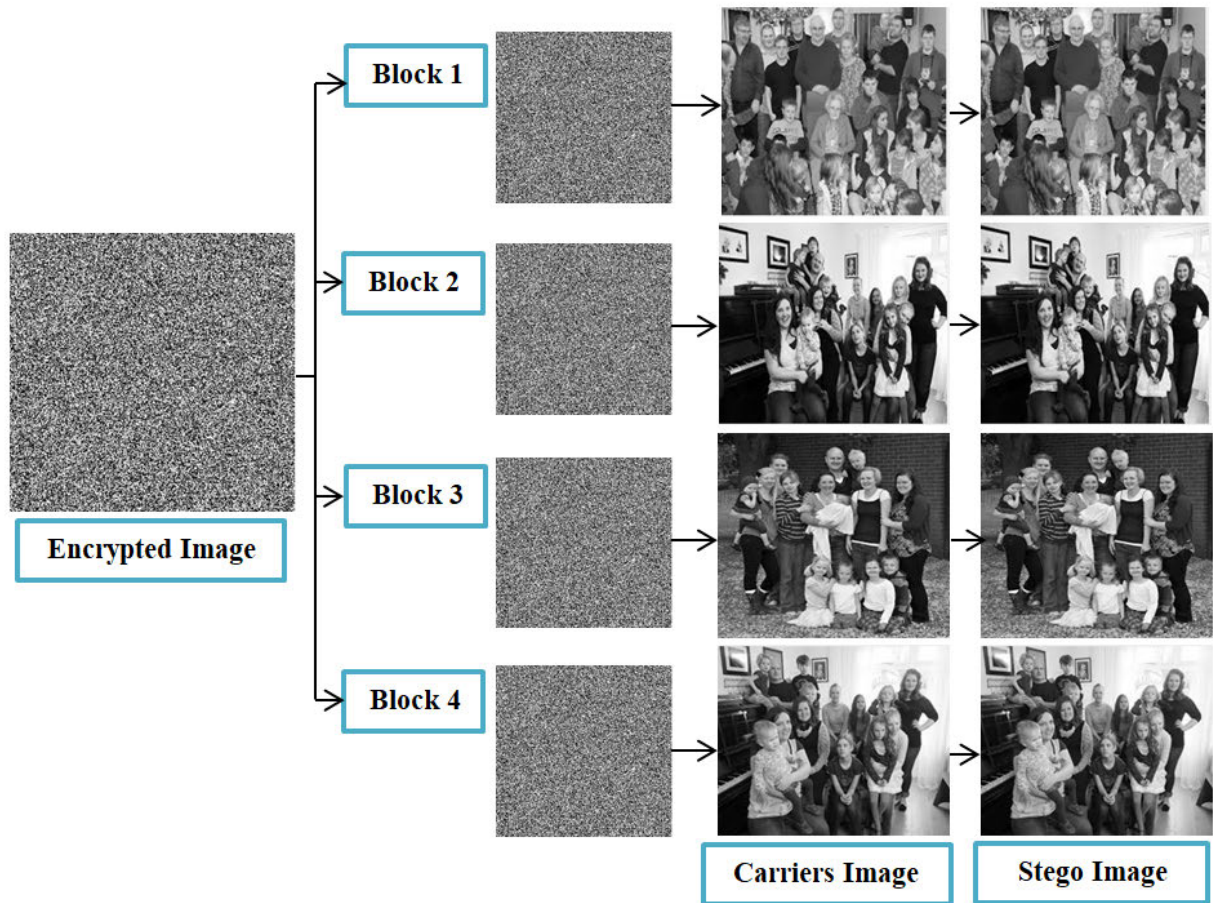


FIGURE 8. The steganography approach.

TABLE 4. NPCR & UACI.

Algorithms	Images (256 × 256)	NPCR	UACI
Ours	Lena	99.61	33.46
	Airplane	99.62	33.43
	Boat	99.65	33.42
	Cameraman	99.63	33.44
	Peppers	99.63	33.46
	Tree	99.64	33.42
	Truck	99.60	33.46
	Girl	99.61	33.45
	Baboon	99.61	33.44
	All Black	99.56	33.39
Ref [35]	Baboon	99.55	33.61
Ref [36]	Peppers	99.62	33.37
Ref [37]	Cameraman	99.63	33.48
Ref [38]	Pepper	99.62	33.63
Ref [39]	Airplane	99.59	33.12
Ref [40]	Lena	99.50	33.09

compared to other references. The correlation coefficients of the proposed algorithm are closer to 0 than the other algorithms. It denotes that the proposed algorithm can effectively decrease the correlation of adjacent pixels in a cipher image.

C. ENTROPY INFORMATION ANALYSIS

Entropy is used to describe the texture of an image. It is a statistical measure of randomness. A source that emits

256 symbols has an entropy of 8. Entropy (E) is calculated using the following formula [46], [47]:

$$E = \sum_{i=1}^{N-1} P(X_i) \log_2 P(X_i) \tag{22}$$

where N is the total number of symbol (X) and P(X_i) is the probability of occurrence of symbol(X_i). The entropy should be close to 8 for encrypted image. Table 6 shows the entropy values for the encrypted image, as well as other references. The entropy of the proposed algorithm is very close to the ideal value 8. Our proposed algorithm has better 4 results in overall, better 2 results in Ref [36], [37]. It is denoted that the proposed algorithm realizes the best results, which means the encrypted images of our algorithm has a random pixel value distribution.

D. PEAK SIGNAL-TO-NOISE RATIO (PSNR)

The peak signal-to-noise ratio is applied to measure the quality of the encryption technique. PSNR indicates the variation in pixel values between the original image and the encrypted image [32]. PSNR can be calculated as the following formula:

$$PSNR = 10 \log_{10} \left[\frac{M * N * 255^2}{\sum_{i=0}^{N-1} \sum_{j=0}^{M-1} [P(i, j) - C(i, j)]^2} \right] \tag{23}$$

TABLE 5. Correlation coefficient between two adjacent pixels in the original and encrypted images.

Algorithms	Images (256 × 256)	Correlation Coefficient					
		Horizontal		Vertical		Diagonal	
		Plain	Encrypted	Plain	Encrypted	Plain	Encrypted
Ours	Lena	0.9853	5.3220e-04	0.9791	8.7670e-04	0.9402	0.0002
	Airplane	0.9166	1.2627e-04	0.9931	8.1190e-04	0.9621	0.0003
	Boat	0.9268	3.8595e-04	0.9452	0.0003	0.9152	0.0008
	Cameraman	0.9335	0.0002	0.9592	2.8897e-04	0.9452	0.0012
	Peppers	0.9634	0.0003	0.9704	0.0011	0.9014	0.0023
	Tree	0.9645	0.0014	0.9451	0.0004	0.9312	0.0032
	Truck	0.8955	0.0013	0.9477	0.0016	0.8745	0.0023
	Girl	0.9740	0.0003	0.9657	0.0006	0.9216	0.0014
	Baboon	0.8736	0.0011	0.8261	0.0021	0.8132	0.0032
	All Black	NA	0.0014	NA	0.0012	NA	0.0025
	All White	NA	0.0011	NA	0.0022	NA	0.0045
Ref [43]	Lena	0.9761	-0.0058	0.98862	-0.0068	0.9561	-0.0103
Ref [31]	Peppers	0.9807	-0.0028	0.9752	-0.0039	0.9636	-0.0024
Ref [44]	Cameraman	0.933480	0.002941	0.959220	-0.000775	0.908660	-0.001903
Ref [45]	Lena	0.9718	0.0045	0.9865	0.0018	0.9620	-0.0058
Ref [39]	Airplane	0.9702	-0.0019	0.9687	-0.0067	0.9454	0.0161
Ref [41]	Lena	0.9794	0.0214	0.9646	0.0465	0.9535	-0.0090
Ref [42]	Lena	0.93063	0.00773	0.95945	-0.01103	0.90711	0.00153

TABLE 6. Entropy information analysis.

Algorithms	Images (256 × 256)	Information Entropy Analysis
Ours	Lena	7.9973
	Airplane	7.9972
	Boat	7.9979
	Cameraman	7.9971
	Peppers	7.9977
	Tree	7.9976
	Truck	7.9975
	Girl	7.9974
	Baboon	7.9972
	All Black	7.9970
	Ref [35]	Baboon
Ref [36]	Peppers	7.9976
Ref [37]	Cameraman	7.9972
Ref [38]	Pepper	7.9978
Ref [46]	Boat	7.9789
Ref [47]	Lena	7.9965

TABLE 7. Peak signal to noise ratio.

Algorithms	Images (256 × 256)	Peak Signal to Noise Ratio
Ours	Lena	8.4124
	Cameraman	9.1405
	Peppers	9.4374
	Airplane	8.6867
	Boat	8.4373
	Tree	9.3829
	Truck	9.5234
	Girl	9.9582
Baboon	9.3772	

where M and N represent the length and width of the image, respectively. $P(i, j)$ represents the pixel value of an original image, and $C(i, j)$ represents the pixel value of the cipher image. The encryption quality is better when PSNR is low. Table 7 shows the result of PSNR between original and cipher images.

E. HISTOGRAM ANALYSIS

The histogram marks the distribution of pixels in their gray scale values. A good encryption algorithm is confirmed, when

TABLE 8. Encryption time consumption [unit:sec].

Algorithms	Images (256 × 256)	Encryption Time (unit:sec)
Ours	Lena	0.9924245
	Baboon	0.9078264
	Cameraman	0.8992656
	Boat	0.8908977
	Airplane	0.9131487
	Pepper	0.9147926
Ref [31]	Lena	1.170844
Ref [36]	pepper	0.95
Ref [48]	Lena	1.164

pixels are distributed uniformly in the encrypted image [29]. Figure 9 shows a step by step histogram for the image encryption proposed. The histogram of original and encrypted images is illustrated in Figure 10.

F. KEY SENSITIVITY ANALYSIS

It is important to note changes in the encryption key and see how sensitive the process is to such changes. High sensitivity means that a single bit of change in this key may lead to a totally different result. In general, fuzzy integral is extremely sensitive to changes in system initial parameters. That is to say that an unnoticeable change in the encryption key results in differences between the decrypted and the original images. In Figure 11, there are three images, the original one, a decrypted one with the correct encryption key, and a decrypted one with the wrong key. It can be said that the algorithm was highly sensitive to the key since a small change has resulted in a very different image and the original one was never reached with such a key [28].

G. SPEED ANALYSIS

The speed of the algorithm is estimated in a system that has a 3.0 GHz processor with 8GB RAM, MATLAB R2015b, and Windows 10 operating system. The encryption time of the proposed algorithm for various images is

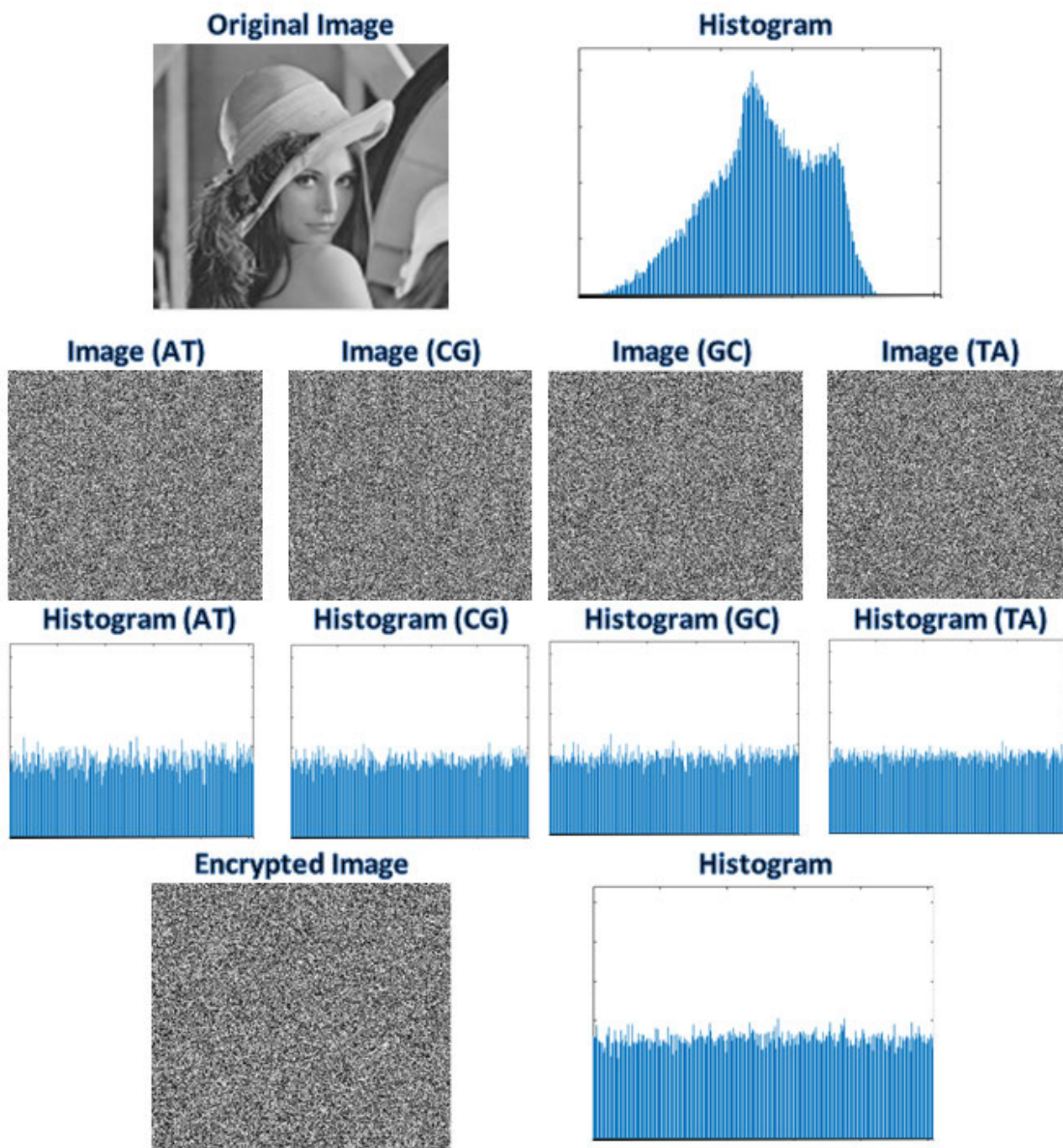


FIGURE 9. Histogram analysis.

shown in Table 8 and compared with different algorithms. Decryption time consumption is listed in Table 9.

VIII. STEGANOGRAPHY TESTS

In the encryption process described in this paper, it was suggested that after the encryption of the image is done, four sub-images would be extracted from the said image and hidden in a set of images using the IWT method. This process is done to improve the security level. To test whether this desired effect was accomplished or not, two metrics were applied under

TABLE 9. Decryption time consumption [unit:sec].

Algorithms	Images (256 × 256)	Decryption Time (unit:sec)
Ours	Lena	2.1833291
	Baboon	1.9972180
	Cameraman	1.9638721
	Boat	1.8705817
	Airplane	2.0089271
	Pepper	2.01254372

different attacks, namely the imperceptibility and robustness tests [2], [14], [15].

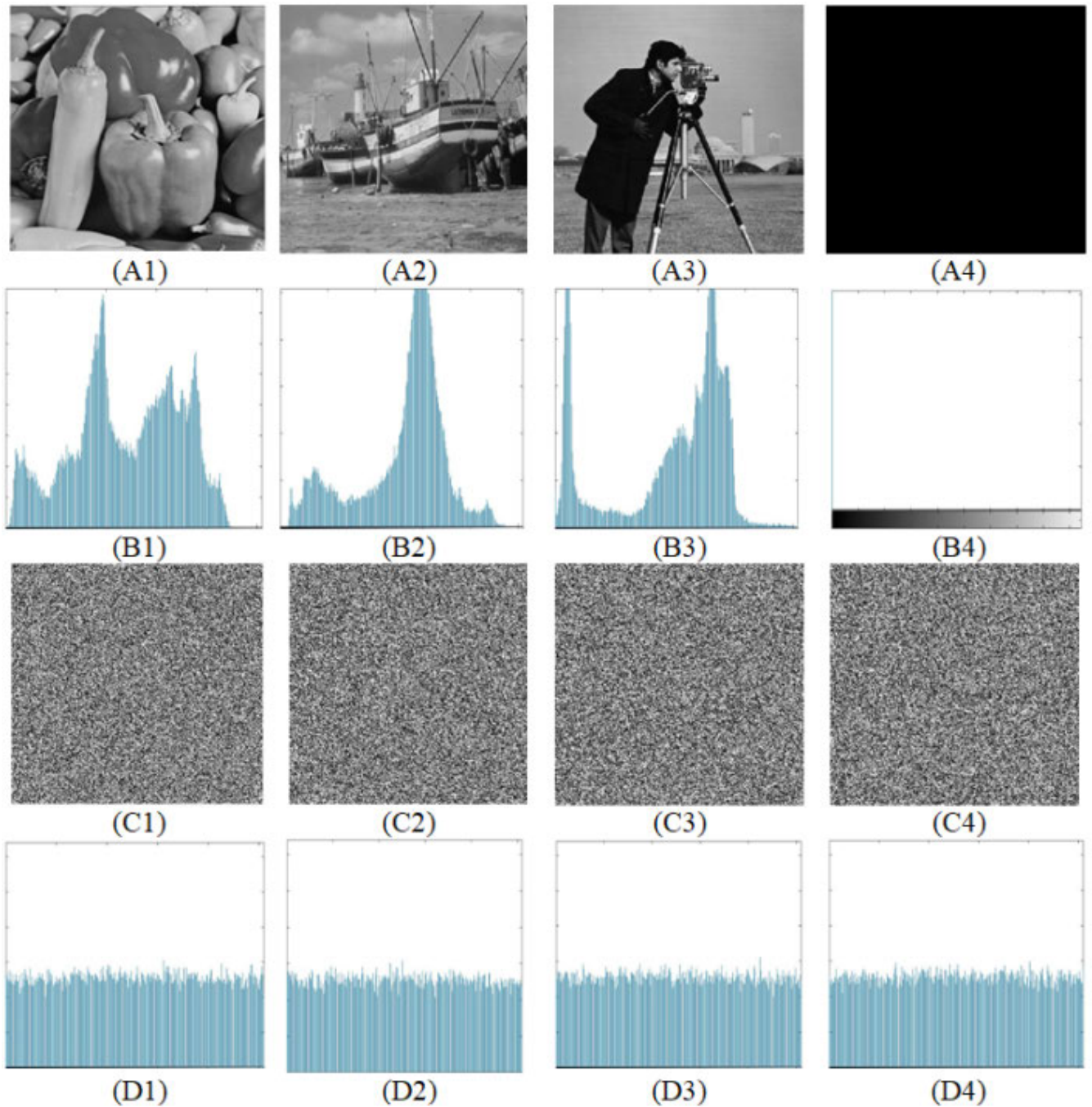


FIGURE 10. Histogram of original and encrypted images; (A1) - (A4) The original images; (B1) - (B4) The histogram of original images; (C1) - (C4) The encrypted images; (D1) - (D4) The histogram of encrypted images.

A. IMPERCEPTIBILITY TEST

Imperceptibility looks at the quality of the image and how it was affected following encryption, as well as how good the sub-images were hidden and whether the viewer could see them. To test this, the signal-to-noise ratio (PSNR) is applied. This ratio serves in the evaluation of the similarities between the original image (x) and the stego-image (y). PSNR can be calculated using the following equation.

$$PSNR = 10 \log_{10} \left(\frac{Max((i, j))^2}{MSE} \right) \tag{24}$$

$$MSE = \frac{1}{M * N} \sum_{i=1}^L \sum_{j=1}^W [x(i, j) - y(i, j)]^2 \tag{25}$$

where L and W are the size of the image (length and width) and MSE is the mean square error between the two images. When the results of the PSNR are high, this means that imperceptibility was good and that the similarities between the two images are high. For each stego image, Table 10 shows the values of its PSNR.

Encrypted Image

Decrypted Image

Decrypted Images after a One-Bit Change in the Main Key

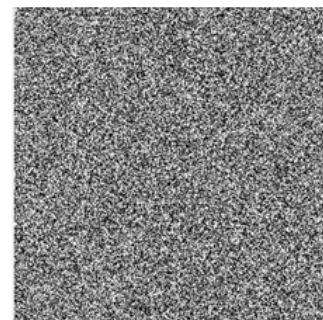
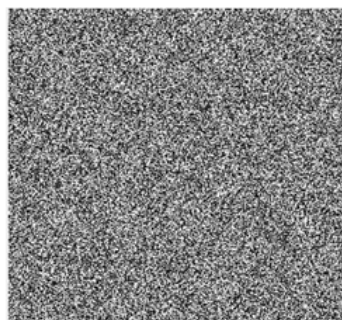


FIGURE 11. Key sensitivity analysis.

TABLE 10. PSNR of four stego image.

Images	PSNR (dB)
Stego-image (1)	42.1824
Stego-image (2)	42.5703
Stego-image (3)	42.4666
Stego-image (4)	42.2313

TABLE 11. SSIM between cover image and stego image.

Images	SSIM
Image (1)	0.9789
Image (2)	0.9798
Image (3)	0.9795
Image (4)	0.9791

B. STRUCTURE SIMILARITY INDEX ANALYSIS OF STEGANOGRAPHIC RESULTS (SSIM)

SSIM is utilized to measure the similarity between the cover image and stego image. The values of SSIM lie between 0 and 1. SSIM is better when the result is larger [49], [50]. It can be calculated as formula:

$$SSIM = \frac{(2 \mu_c \mu_s + C_1) (2 \sigma_{cs} + C_2)}{(\mu_c^2 + \mu_s^2 + C_1) (\sigma_c^2 + \sigma_s^2 + C_2)} \quad (26)$$

where C_1 and C_2 are two constants. c is the cover image and s is the stego image. Furthermore, μ, σ are the average and the standard deviation respectively. Table 11 shows the values of its SSIM.

C. ROBUSTNESS TEST

Several types of attacks were used to test the algorithm, including median and mean, salt and pepper noise, cropping, Gaussian noise, rotation, and shearing. The similarities between the original image and the stego one were tested using the normalized correlation coefficient (NCC), which is considered one of the best means of testing the relation between two functions. Eq.27 is used to calculate the NCC. Table 12 shows the NCC values under different types of attacks. These values were high proving the effectiveness of the algorithm and its resistance to different attacks. NCC values were high and the higher the values, the robustness of the encryption process against any attack. NCC usually varies

TABLE 12. Normalized correlation coefficient (NCC).

Attacks	Stego (1)	Stego (2)	Stego (3)	Stego (4)
Mean Filter	0.9556	0.9672	0.9564	0.9492
Median Filter	0.9864	0.9939	0.9926	0.9815
Shearing	0.8778	0.8937	0.8510	0.8769
Rotation	0.7595	0.8091	0.7636	0.7819
Cropping	0.9117	0.9637	0.9080	0.8450
Salt, Pepper Noise	0.9860	0.9834	0.9805	0.9824
Gaussian Noise	0.0.9721	0.9626	0.9551	0.9525

between 0 and 1 and the closer it is to 1, the more robust the algorithm is.

$$NCC = \frac{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (I_c(i, j) I_s(i, j))}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (I_c(i, j))^2} \quad (27)$$

IX. CONCLUSION

Our proposed new scheme in this paper is inspired by the increasing performance of Image encryption and steganography techniques in modern multimedia communication systems. Our new highly stochastic and secure image encryption technique is based on the use of the DNA’s dynamic range rule, as well as the complex and nonlinear properties of fuzzy integrals. In summary, four images are extracted from the original image, according to the nitrogenous bases of DNA (AT, CG, GC, and TA). Then each DNA image is diffused using a fuzzy sequence. After that, DWT is used to fuse these images. For increasing security, a new steganography approach is used. In particular, the encrypted image is split into four sub-images, each of which is hidden in a different carrier image selected from a known group of carrier images according to a given key. Each selected carrier image will have one-quarter of the encrypted image hidden into it. The performance analysis is carried out to test the security properties of the proposed scheme. The results prove the robustness of the new algorithm against most types of attacks. From the encryption point of view and standards, it is a very stochastic algorithm that has low correlation coefficients (close to the ideal value of zero) and quite sensitive to changes in the encryption key and has good entropy. Also, the steganography

test proved that hidden encrypted images are almost invisible at high PSNR and have good NCC values under different types of attacks. The robustness of the new proposed algorithm and the promising results of its different security tests make it suitable for digital image encryption for future multimedia communication systems.

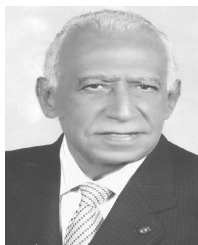
X. FUTURE WORK

Inspired by a recommendation of one of the anonymous reviewers, we plan to extend our work in a future paper that is concerned with the security problems of the proposed fuzzy-DNA encryption algorithms. In this future work we will examine any possible flaws that could affect the proposed encryption algorithms. As suggested by that reviewer, we can use determined steps and identified flowchart to represent the flaws and solve the problems that could affect the security of the system after encryption as described in [51].

REFERENCES

- [1] S. M. Alwabhani and H. T. Elshoush, "Chaos-based audio steganography and cryptography using LSB method and one-time pad," in *Proc. SAI Intell. Syst. Conf. (IntelliSys)*, 2016, pp. 755–768.
- [2] S. E. El-Khamy, N. O. Korany, and M. H. El-Sherif, "Highly secured image hiding technique in stereo audio signal based on complete complementary codes," *Multimedia Tools Appl.*, vol. 78, no. 24, pp. 34373–34395, 2019.
- [3] D. D. Bloisi and L. Iocchi, "Image based steganography and cryptography," *VISAPP*, vol. 1, no. 1, pp. 127–134, 2007.
- [4] A. A. AL-Shaaby and T. AIKharobi, "Cryptography and steganography: New approach," *Trans. Netw. Commun.*, vol. 5, no. 6, p. 25, Dec. 2017.
- [5] J. Chen, Z.-L. Zhu, L.-B. Zhang, Y. Zhang, and B.-Q. Yang, "Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption," *Signal Process.*, vol. 142, pp. 340–353, Jan. 2018.
- [6] S. M. Seyedzadeh and S. Mirzakhaki, "Image encryption scheme based on Choquet fuzzy integral with pseudo-random keystream generator," in *Proc. Int. Symp. Artif. Intell. Signal Process. (AISP)*, Jun. 2011, pp. 101–106.
- [7] S. M. Seyedzadeh, B. Norouzi, and S. Mirzakhaki, "RGB color image encryption based on choquet fuzzy integral," *J. Syst. Softw.*, vol. 97, pp. 128–139, Nov. 2014.
- [8] Y. Hashemi, "Design a new image encryption using fuzzy integral permutation with coupled chaotic maps," *Int. J. Res. Comput. Sci.*, vol. 3, no. 1, p. 27, 2013.
- [9] A. Dvořák and M. Holčápek, "Fuzzy measures and integrals defined on algebras of fuzzy subsets over complete residuated lattices," *Inf. Sci.*, vol. 185, no. 1, pp. 205–229, Feb. 2012.
- [10] D. Ralescu and G. Adams, "The fuzzy integral," *J. Math. Anal. Appl.*, vol. 75, no. 2, pp. 562–570, 1980.
- [11] H. Liu, X. Wang, and A. Kadir, "Color image encryption using Choquet fuzzy integral and hyper chaotic system," *Optik Int. J. Light Electron Opt.*, vol. 124, no. 18, pp. 3527–3533, Sep. 2013.
- [12] S. Gupta and N. Dhanda, "Audio steganography using discrete wavelet transformation (DWT) & discrete cosine transformation (DCT)," *IOSR J. Comput. Eng.*, vol. 17, no. 2, pp. 2278–2661, 2015.
- [13] X. Liao, Q.-Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," *J. Vis. Commun. Image Represent.*, vol. 22, no. 1, pp. 1–8, Jan. 2011.
- [14] R. El Safy, H. Zayed, and A. El Dessouki, "An adaptive steganographic technique based on integer wavelet transform," in *Proc. Int. Conf. Netw. Media Converg.*, 2009, pp. 111–117.
- [15] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," *J. Syst. Eng. Electron.*, vol. 29, no. 3, pp. 639–649, 2018.
- [16] S. E. El-Khamy and A. G. Mohamed, "Image keyed PN sequence generator and authentication technique based on Choquet fuzzy integral," in *Proc. 35th Nat. Radio Sci. Conf. (NRSC)*, Mar. 2018, pp. 293–299.
- [17] S.-S. Yu, N.-R. Zhou, L.-H. Gong, and Z. Nie, "Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system," *Opt. Lasers Eng.*, vol. 124, Jan. 2020, Art. no. 105816.
- [18] M. Y. Valandar, M. J. Barani, and P. Ayubi, "A fast color image encryption technique based on three dimensional chaotic map," *Optik*, vol. 193, Sep. 2019, Art. no. 162921.
- [19] S. Yao, L. Chen, and Y. Zhong, "An encryption system for color image based on compressive sensing," *Opt. Laser Technol.*, vol. 120, Dec. 2019, Art. no. 105703.
- [20] R. Shanthakumari and S. Malliga, "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm," *Multimedia Tools Appl.*, vol. 79, nos. 5–6, pp. 3975–3991, Feb. 2020.
- [21] P. Bharti and R. Soni, "A new approach of data hiding in images using cryptography and steganography," *Int. J. Comput. Appl.*, vol. 58, no. 18, pp. 1–5, Nov. 2012.
- [22] M. Grabisch, "The application of fuzzy integrals in multicriteria decision making," *Eur. J. Oper. Res.*, vol. 89, no. 3, pp. 445–456, Mar. 1996.
- [23] P. R. Halmos, *Measure Theory*, vol. 18. New York, NY, USA: Springer-Verlag, 1950.
- [24] H.-C. Liu, Y.-D. Jheng, W.-C. Lin, and G.-S. Chen, "A novel fuzzy measure and its Choquet integral regression model," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 3, Aug. 2007, pp. 1394–1398.
- [25] H. T. Nguyen, V. Kreinovich, J. Lorkowski, and S. Abu, "Why sugeno λ -measures," in *Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE)*, Aug. 2015, pp. 1–7.
- [26] S. Medasani, J. Kim, and R. Krishnapuram, "An overview of membership function generation techniques for pattern recognition," *Int. J. Approx. Reasoning*, vol. 19, nos. 3–4, pp. 391–417, Oct. 1998.
- [27] H. W. Safi and A. Y. Maghari, "Image encryption using double chaotic logistic map," in *Proc. Int. Conf. Promising Electron. Technol. (ICPET)*, Oct. 2017, pp. 66–70.
- [28] S. Somaraj and M. A. Hussain, "Performance and security analysis for image encryption using key image," *Indian J. Sci. Technol.*, vol. 8, no. 35, p. 1, Dec. 2015.
- [29] W. Xingyuan, Z. Junjian, and C. Guanghui, "An image encryption algorithm based on ZigZag transform and LL compound chaotic system," *Opt. Laser Technol.*, vol. 119, Nov. 2019, Art. no. 105581.
- [30] J. Ahmad, S. O. Hwang, and A. Ali, "An experimental comparison of chaotic and non-chaotic image encryption schemes," *Wireless Pers. Commun.*, vol. 84, no. 2, pp. 901–918, Sep. 2015.
- [31] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.
- [32] J. Ahmad and F. Ahmed, "Efficiency analysis and security evaluation of image encryption schemes," *Computing*, vol. 23, p. 25, Aug. 2012.
- [33] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Comput. Biol. Med.*, vol. 72, pp. 170–184, May 2016.
- [34] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Trans. Nanobiosci.*, vol. 16, no. 8, pp. 850–858, Dec. 2017.
- [35] X. Liu, D. Xiao, W. Huang, and C. Liu, "Quantum block image encryption based on arnold transform and sine chaotification model," *IEEE Access*, vol. 7, pp. 57188–57199, 2019.
- [36] X. Zhang, L. Wang, Z. Zhou, and Y. Niu, "A chaos-based image encryption technique utilizing hilbert curves and h-fractals," *IEEE Access*, vol. 7, pp. 74734–74746, 2019.
- [37] L. Liu, Y. Lei, and D. Wang, "A fast chaotic image encryption scheme with simultaneous permutation-diffusion operation," *IEEE Access*, vol. 8, pp. 27361–27374, 2020.
- [38] S. Sun, Y. Guo, and R. Wu, "A novel image encryption scheme based on 7D hyperchaotic system and row-column simultaneous swapping," *IEEE Access*, vol. 7, pp. 28539–28547, 2019.
- [39] S. Zhang and T. Gao, "An image encryption scheme based on dna coding and permutation of hyper-image," *Multimedia Tools Appl.*, vol. 75, no. 24, pp. 17157–17170, 2016.
- [40] A. S. Rajput and M. Sharma, "A novel image encryption and authentication scheme using chaotic maps," in *Advances in Intelligent Informatics (Advances in Intelligent Systems and Computing)*, vol. 320. Cham, Switzerland: Springer, 2015, pp. 277–286.
- [41] P. Zhen, G. Zhao, L. Min, and X. Jin, "Chaos-based image encryption scheme combining DNA coding and entropy," *Multimedia Tools Appl.*, vol. 75, no. 11, pp. 6303–6319, Jun. 2016.

- [42] J. Zhang, D. Hou, and H. Ren, "Image encryption algorithm based on dynamic dna coding and chen's hyperchaotic system," *Math. Problems Eng.*, vol. 2016, 2016.
- [43] R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux, and L. Luo, "A novel chaos-based symmetric image encryption using bit-pair level process," *IEEE Access*, vol. 7, pp. 99470–99480, 2019.
- [44] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.
- [45] Y.-Q. Zhang, J.-L. Hao, and X.-Y. Wang, "An efficient image encryption scheme based on s-boxes and fractional-order differential logistic map," *IEEE Access*, vol. 8, pp. 54175–54188, 2020.
- [46] M. Ahmad, M. Z. Alam, Z. Umayya, S. Khan, and F. Ahmad, "An image encryption approach using particle swarm optimization and chaotic map," *Int. J. Inf. Technol.*, vol. 10, no. 3, pp. 247–255, Sep. 2018.
- [47] M. Ahmad, A. Chopra, P. Jain, and S. Alam, "A chaotic substitution based image encryption using apa-transformation," in *Proc. 3rd Int. Conf. Frontiers Intell. Comput. Theory Appl. (FICTA)*. Cham, Switzerland: Springer, 2015, pp. 75–83.
- [48] R. Enayatifar, A. H. Abdullah, I. F. Isnin, A. Altameem, and M. Lee, "Image encryption using a synchronous permutation-diffusion technique," *Opt. Lasers Eng.*, vol. 90, pp. 146–154, Mar. 2017.
- [49] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin, "A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network," *IEEE Access*, vol. 8, pp. 25777–25788, 2020.
- [50] E. Z. Astuti, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and M. K. Sarker, "LSB-based bit flipping methods for color image steganography," *J. Phys. Conf. Ser.*, vol. 1501, Mar. 2020, Art. no. 012019.
- [51] Z. M. Z. Muhammad and F. Özkaynak, "Security problems of chaotic image encryption algorithms based on cryptanalysis driven design technique," *IEEE Access*, vol. 7, pp. 99945–99953, 2019.



SAID E. EL-KHAMY (Life Fellow, IEEE) received the B.Sc. (Hons.) and M.Sc. degrees from Alexandria University, Alexandria, Egypt, in 1965 and 1967, respectively, and the Ph.D. degree from the University of Massachusetts, Amherst, USA, in 1971.

He has been a Teaching Staff with the Department of Electrical Engineering, Faculty of Engineering, Alexandria University, since 1972, and was appointed as a full-time Professor, in 1982, and as the Chairman of the Electrical Engineering Department, from September 2000 to September 2003, where he is currently an Emeritus Professor. He has published about 400 scientific articles in national and international conferences and journals. His current research interests include wireless multimedia communications, wave propagation, smart antenna arrays, modern signal processing techniques, image processing, and security and watermarking techniques.

Dr. El-Khamy is a Fellow of the Electromagnetic Academy. He is the Founder and the past President of the IEEE Alexandria/Egypt Subsection and the past President of the Egypt's National Radio Science Committee of URSI. He has earned many national and international research awards, among which are the R.W.P. King Best Paper Award of the Antennas and Propagation Society of IEEE, in 1980, the Egypt's State Engineering Encouraging Research Award for two times, in 1980 and 1989, respectively, the Abdel-Hamid Schoman–Kingdom of Jordan Award for Engineering Research, in 1982, the State Scientific Excellence Award in Engineering Sciences for 2002, the Alexandria University Appreciation Award of Engineering Sciences for 2003, the State Appreciation Award of Engineering Sciences for 2004, and the IEEE Region 8 Volunteer Award for 2010. In 2016, he was honored by the Egypt's National Radio Science Committee of URSI and was selected as the Radio Science Recognized Figure of the year. Also, in 2016, he was announced to be "The Distinct Scientist of Alexandria University, in Engineering Sciences." He took part in the organization of many local and international conferences, including the yearly series of NRSC (URSI) conference series (1990–2019), ISCC'95, ISCC'97, ISSPIT'2000, MELECON'2002, and IEEE GCIoT'2019. He took part in many IEEE Region 8 activities as well as URSI general assemblies.



NOHA O. KORANY received the B.Sc.Eng. and Ph.D. degrees from Alexandria University, Egypt. She received a fellowship from Ruhr-University Bochum. She was a Member of Scientific Staff at the Institute of Communication-Acoustics, Ruhr-University Bochum, Germany, from 2002 to 2004. She is currently a Professor at Alexandria University. Her main research interest includes acoustics and communications.



AMIRA G. MOHAMED (Student Member, IEEE) received the B.S. degree in electronics and communication engineering from the Alexandria Higher Institute of Engineering and Technology (AIET), Alexandria, Egypt, in 2013, and the M.S. degree in electrical engineering from the Faculty of Engineering, Alexandria University, Alexandria, in 2017, where she is currently pursuing the Ph.D. degree in electrical engineering. She is also a Teaching Assistant with the Electronics and Communication Department, AIET. Her research interests include image processing, steganography, cryptography, and information security.

•••