

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/352377382>

# Binary Image Encryption Based on Chaotic and DNA Encoding

Chapter · January 2021

DOI: 10.1007/978-981-16-0666-3\_23

CITATIONS

3

READS

247

3 authors:



**Sheimaa Hadi**

University of Babylon

3 PUBLICATIONS 3 CITATIONS

SEE PROFILE



**Suhad A. Ali**

University of Babylon

28 PUBLICATIONS 140 CITATIONS

SEE PROFILE



**Majid Jabbar Jawad**

The University of Babylon

25 PUBLICATIONS 54 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Robust Watermarking of Digital Vector Maps for Copyright Protection [View project](#)



Robust Watermarking of Digital Vector Maps for Copyright Protection [View project](#)

# Binary Image Encryption Based on Chaotic and DNA Encoding



Sheimaa A. Hadi, Suhad A. Ali, and Majid Jabbar Jawad

**Abstract** This paper proposed method for encrypting images depending on the chaotic system and the DNA coding. The encrypting operation is done with several procedures. In the first procedure, the image is divided into non-overlapped blocks of  $n \times n$  pixels. In the second procedure, the divide blocks are scrambled according to the desired key. In the third procedure, the quadratic chaotic system is used for generating a mask in order to scramble the pixels of the scrambled blocks. In the final procedure, the encrypting process based on DNA rules is used to encoding the scrambled image. Also, the decryption operation is done with several procedures. In the first procedure, the encrypted image is decrypted based on DNA rules. In the second procedure, the pixels of scrambled blocks are descrambled via quadratic chaotic system. Finally, the scrambled block is descrambled in order to get the decrypted image. More details about the proposed method are shown in the sections of the paper. The experimental results show that the proposed method satisfied the requirements of encryption.

**Keywords** Binary image · Image encryption · Image scrambling · Image diffusing · Chaotic system · DNA encoding

## 1 Introduction

After the tremendous development in communication technology and the extends of the popular of the Internet, the process of exchanging information by means of digital images over the Internet has become very easy, fast, and useful. Digital images such as medical, personal, or military are transferred through insecure channels. The transferred images may be attacked by hackers. By using a smart software, these images may be subjected to several illegal operations such as copying, modification, sabotage, or theft. So, it became necessary for founding a useful technique used for preserving the security of these images such as availability, confidentiality,

---

S. A. Hadi (✉) · S. A. Ali · M. J. Jawad  
Department of Computer Science, College of Science for Women, University of Babylon,  
Babylon, Iraq  
e-mail: [shaymaa.hadi@student.uobabylon.edu.iq](mailto:shaymaa.hadi@student.uobabylon.edu.iq)

and authenticity. A confidentiality requirement is the most security requirement in the security. One of the most important techniques used to protect information is encryption.

Encryption is the process of converting data into a structure that is not understood or unreadable by unauthorized individuals, before the process of transmitting it through insecure channel. The opposite of the encryption process is to return the data to a readable format called decryption [1]. There are many coding methods in use, and the most important of which are mathematical equation-based coding methods, which is called mathematical coding, elliptic coding, quantitative coding and chaotic coding, and DNA coding [2]. The chaotic coding method is one of the most important coding methods adopted because of its advantages. It is a nonlinear system, and the resulting sequence cannot be predicted it, as it is a sensitive system for the random and initial state. Chaotic coding systems are accomplished in two stages: diffusion and scrambling. Scrambling is a procedure of changing the positions of image pixels depending on key. Diffusion is a procedure of altering pixel values in the image. The resulting of the two processes is a new encoded image that differs from the original image [3]. DNA coding is one of the coding systems. The DNA is the carrier of genetic information from one generation to the next in living things. It consists of four main bases: A (adenine), T (thymine), C (cytosine), and G (guanine). These are used in the encryption process after encoding it into the form of [0, 1] [4]. The DNA coding is carried out by converting the pixels of the plain image to the DNA format using its basic rules for DNA. So, DNA produces an encoded image different from the plain image [5]. When chaotic coding is mixed with DNA coding, the advantages of both systems are exploiting. The mixing of DNA and chaotic coding produces a strong coding system that is resistant to differential attacks with a high entropy.

## 2 Related Work

In 2016, Houas [6] presented an algorithm for encrypting the binary images. It consists of many stages. The first stage reduces the amount of data needed to present the image. In the second stage, the image is partitioned into number of blocks, which is used in new images that have same size of the original image, and used to gain a key-image and encrypted images. The parameters that obtained from these stages treated as key-image for the encryption and decryption algorithm. The decryption algorithm is implemented by the subtraction between every key-image and encrypted image, then adding them in an image to resulting the original image.

In 2017, Chai [7] presented an algorithm that applies the rules of DNA and chaotic systems. The algorithm is implemented in three steps; the first step is to compute the system parameters of the two-dimensional logistic sine map completely, the initial values, and the one-dimensional chaotic system. The second step is to produce a DNA coding and decoding matrix using the chaotic system to encode the plain image according to the DNA rules. Thirdly, switching a row at the level of the nucleic acid

and a column on the DNA matrix of the original image, and then execute the XOR DNA to the DNA matrix using the DNA rules. The DNA rules are obtained from combining two one-dimensional chaotic systems.

In 2019, Luo [8] proposed a coding algorithm based on modifying the scheme of linear chaotic Henon system to a nonlinear scheme and tested its efficiency and robustness by applying a set of methods such as histogram, balance, and linear complexity. This system resulted in random sequences that are used to implement the coding process, which goes through three steps: confusion, re-installation, and deployment.

In 2020, Mohamed [9] proposed an algorithm for encrypting color image. The algorithm employs a confusion process based on a hybrid chaotic map, and it is implemented by dividing each channel of color images into number of clusters and creates global scramble over all image. Finally, the pixel scrambling is applied in each cluster, to form high encrypted image. Then, it employs the rationale of human mitochondrial genome mDNA to spread confused pixel values.

In 2020, Athira [10] introduced an encryption technique based on combination of Arnold transform and DNA encoding base. The image is mixed by utilizing Arnold transform, and then DNA encoding bases are applied for the encryption purpose. At the last phase of encryption, chaotic mapping is applied to change the pixel value and break the correlation between pixels in the image.

### 3 Preliminaries of Chaotic Map

In the past, where mostly studied on chaos theories, a large number of various types of mathematical models are concluded and investigated. Chaotic maps generation can be a simple or complex control system. Chaotic maps exhibit the behaviors of a chaotic system. There are some well-known maps such as logistic map, tent map, quadratic map, and others. Mathematically, any chaotic map can be defined as in Eq. (1) [11]:

$$x_{n+1} = f(x_n), \quad n = 1, 2, \dots, n \quad (1)$$

where  $x_n$  is called the state of iteration  $n$  and the function  $f$  is mapping the state  $x_n - 1$  to the next state  $x_n$ . In this thesis, we used and concentrated on quadratic map. Quadratic map equation can be defined as in Eq. (2) [11]:

$$x_{n+1} = r - (x_n)^2 \quad (2)$$

where  $n$  represents the iterations number and  $r$  is the parameter of chaotic.

The quadratic map is satisfying the conditions of a system to be chaotic because it is nonlinear, deterministic, and sensitive to the initial value of  $x_0$ .

**Table 1** Encoding of DNA rules

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

## 4 Preliminaries of DNA Encoding

### 4.1 DNA Computing Rules

The DNA consists from four base: A (adenine), T (thymine), C (cytosine), and G (guanine), and these bases are converted to binary coding according to Table 1 [12].

### 4.2 XOR Operation for DNA Sequences

The XOR operation is applied to the rules for DNA mentioned in Table 1 in the same way as it applies it to the binary numbers. The XOR are reflexive operation, meaning when it is applied between two rules and obtain the resulting rule, it is possible to apply a XOR between the result and one of the coefficients of the first XOR operation to obtain the second parameter. For that reason, it is used in encryption methods. To clarify, if we apply the XOR operation between the sequence [ATTC] and the sequence [GTAC], then the result will be [GATA] as shown in Table 2. When we reverse the operation and apply the XOR between the sequence [GATA] and the sequence [GTAC], then the result will be [ATTC] [12].

## 5 The Proposed System

The proposed method consists of two main stages, namely encryption and decryption. The details of them are listed as follows:

**Table 2** DNA-XOR operation

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

### 5.1 Encryption Stage

This stage consists of several steps. Figure 1 shows the general steps of encryption process.

#### 5.1.1 Binary Image Scrambling Operation

To increase the strength of the encryption method, two scrambling operations for the binary image are done:

##### 1. Block Scrambling

In this process, the binary image is divided into a set of non-overlapped blocks of  $n * n$  pixels. After that, the blocks are repositioned using key (position key) to generate scrambled image based on the following equations:

$$Nb1 = (Key * lenw) \tag{3}$$

$$Nb2 = \text{mod}(Nb1, Nb) + 1 \tag{4}$$

where Key is a key of a prime number used for blocks scrambling, Nb is total number of blocks, lenw is accouter [from 1 to Nb], and Nb2 is the block number where Nb1 is stored in it.

Figure 2 shows scrambling operation for binary image of size 4\*4 pixels.

##### 2. Diffusion by Quadratic Chaotic System

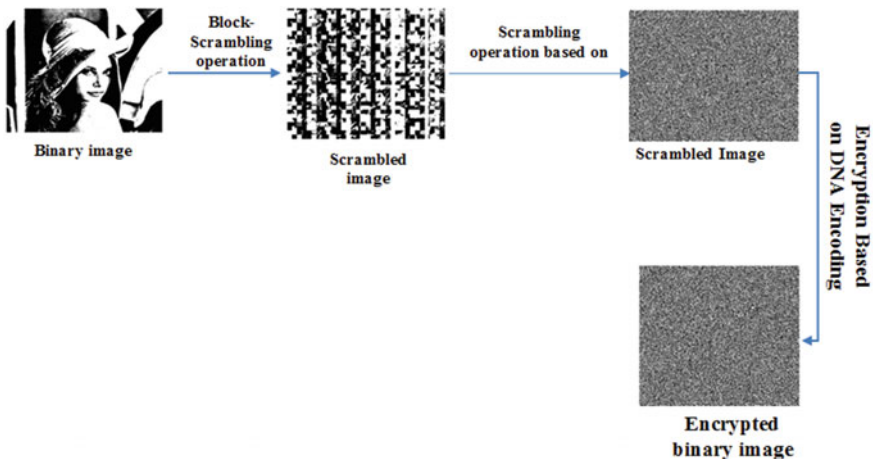


Fig. 1 General steps of encryption process

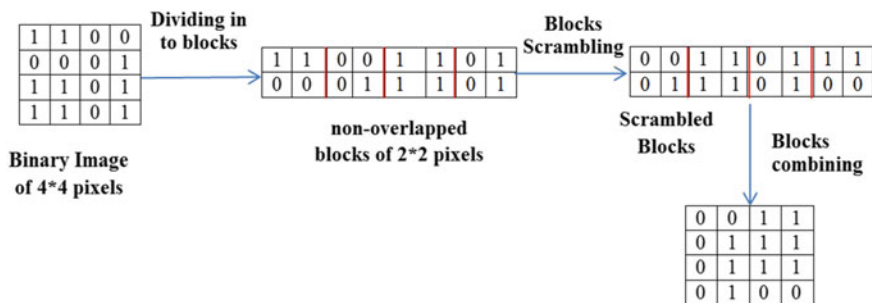


Fig. 2 Binary image scrambling operation

In this operation, the input 2D binary image is converted into 1D vector ( $vec\_Img$ ). Then, a chaotic sequence ( $Seq$ ) with length equal to ( $vec\_Img$ ) is generated according to the standard quadratic chaotic system Eq. (5)

$$Seq_{n+1} = r - (Seq_n)^2 \quad (5)$$

where  $r$  is the chaotic parameter and  $n$  is the number of iterations.

The generated chaotic sequence ( $Seq$ ) is sorted in ascending (or descending) order. After that, the bit location of image is changed according to corresponding indices ( $loc$ ) of the sorted sequence. Finally, the result is the (Diffused-Vector) is converted into 2D image (Diffused-Image). Equations (6) and (7) show how the diffusing operation is done:

$$[Sorted\_Seq, loc] = sort(Seq) \quad (6)$$

$$\begin{aligned} Scrambled\_Vector(i) &= image(loc(i)), \\ \text{for } i &= 1 \dots length(image) \end{aligned} \quad (7)$$

where  $loc$  the arrangement of the elements of ( $Seq$ ) into ( $Sorted\_Seq$ ). Figure 3 shows the example of binary image diffusing.

### 5.1.2 Generating mask

The generated chaotic sequence ( $Seq$ ) is used to build the binary mask which is used later in the encryption process. Firstly, the mask sequence element ( $Mask\_seq$ ) is generated for each image pixel according to the following equation:

$$\begin{aligned} Mask\_seq(i) &= \lfloor [Seq(i)] \rfloor \times 255 \\ \text{for } i &= 1 \dots length(image) \end{aligned} \quad (8)$$

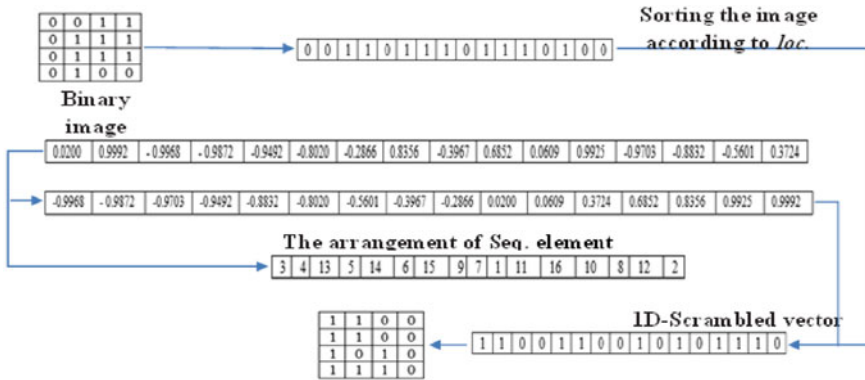


Fig. 3 Binary image scrambling

Secondly, convert the Mask\_seq elements to binary range [0, 1] by thresholding according to Eq. (9) to obtain binary mask (Mask) which is used in the next steps.

$$Mask(i) = \begin{cases} 1 & \text{if } Mask_{seq(i)} \geq T \\ 0 & \text{otherwise} \end{cases}, \tag{9}$$

where  $T$  is threshold which is set by the user.

### 5.1.3 DNA Encoding of Diffused Image and Generated Mask

Cryptography has adopted DNA cryptography as a new method of the coding process. In the proposed method, the DNA encoding is applied on the diffused image and generated mask through several steps. Firstly, the diffused image (Diffused-Image) that resulted from the two scrambling processes is divided into two matrices (Even, Odd). Odd matrix contains the pixels in the odd rows positions, and the even matrix contains the pixels in the even rows positions. Also, the generated mask is splitting into two matrices, one has the elements of the odd position rows, and the other has the elements of the even position rows. Secondly, the odd and even image matrices are converted into 1D vector. Finally, the odd (mask, image) vectors are encoded by rule (1) of DNA rules and save the result in 1D array (ODNAMask, ODNAimg). Also, the even (mask, image) vectors are encoded by rule (3) of DNA rules and save the result in arrays (EDNAMask, EDNAimg). Figure 4 shows example of encoding diffused and generated mask.



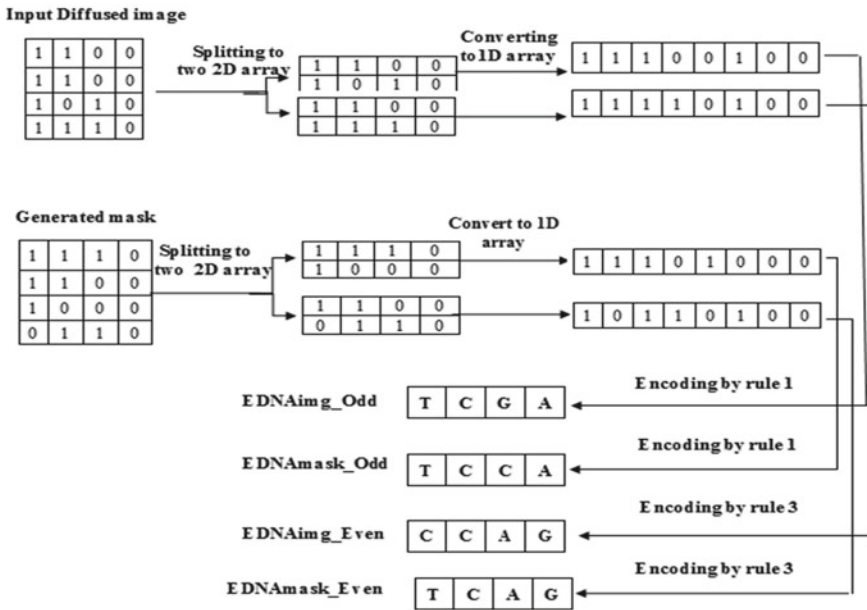


Fig. 4 DNA encoding between diffusing image and generated mask

### 5.1.4 DNA-XOR Operation

In this stage, the DNA-XOR operation in Table 2 is applied between the encoded even and odd image arrays and even and odd mask arrays. Firstly, the XOR operation is carried out between the encoded odd image array and the encoded odd mask (ODNA-mask, ODNAimg). The result is saved in an array. Secondly, the XOR operation is carried out between the encoded even array and the encoded even mask (EDNA-mask, EDNAimg). The result is saved in the other array. Thirdly, resulted (decoded) matrices from two XOR operations are reconstructed into two 2D matrices. Finally, the two matrices are combining to form the encrypted image. Figure 5 shows an example on applying DNA-XOR operation.

The encryption algorithm is listed as follows:

Input:

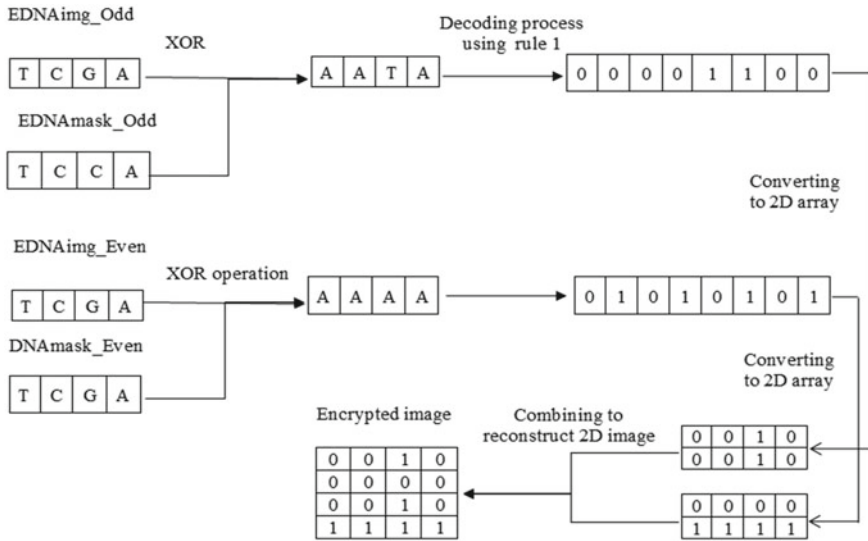
The original binary image I

Position Key PK

Chaotic Key CK

Output: encrypted image

Step 1: Start



**Fig. 5** DNA-XOR operation

- Step 2: dividing I into no overlapped  $n \times n$  pixels
- Step 3: Scramble the position of each block according to Eqs. (3) and (4) by using Position Key (PK)
- Step 4: Use Chaotic Key (CK) to generate random vector with the size of image based on quadratic chaotic system according to Eq. (6)
- Step 5: Diffuse the resulting from step 2 by using the generated random vector in step (4)
- Step 6: Generate a mask according to Eq. (7) using the generated random vector in step (4)
- Step 7: convert mask to 2D matrix M
- Step 8: divide M in to two groups namely C and D. C for odd rows position pixels and D for even rows position pixels
- Step 9: convert C and D to two 1D array C1 and D1
- Step 10: divide scrambled image in to two groups A and B, A for odd rows position pixels, D for even rows position pixels
- Step 11: convert A and B to 1D array A1 and B1
- Step 12: encode A1 and C1 by rule 1 of DNA rules that showed in Table 1 to result in A2 and C2
- Step 13: encode B1 and D1 by rule 3 of DNA rule that showed in Table 1 to result in B2 and D2
- Step 14: apply XOR operation on A2 and C2, and on B1 and D1 according to Table 2.
- Step 15: decoding resulting from step 12, to obtain the results D1, D2
- Step 16: convert D1 and D2 from two 1D array to two 2D array

Step 17: combining the two 2D arrays these generated from step 14 to reconstruct the encrypted binary image

End

The encryption process is shown in Fig. 6.

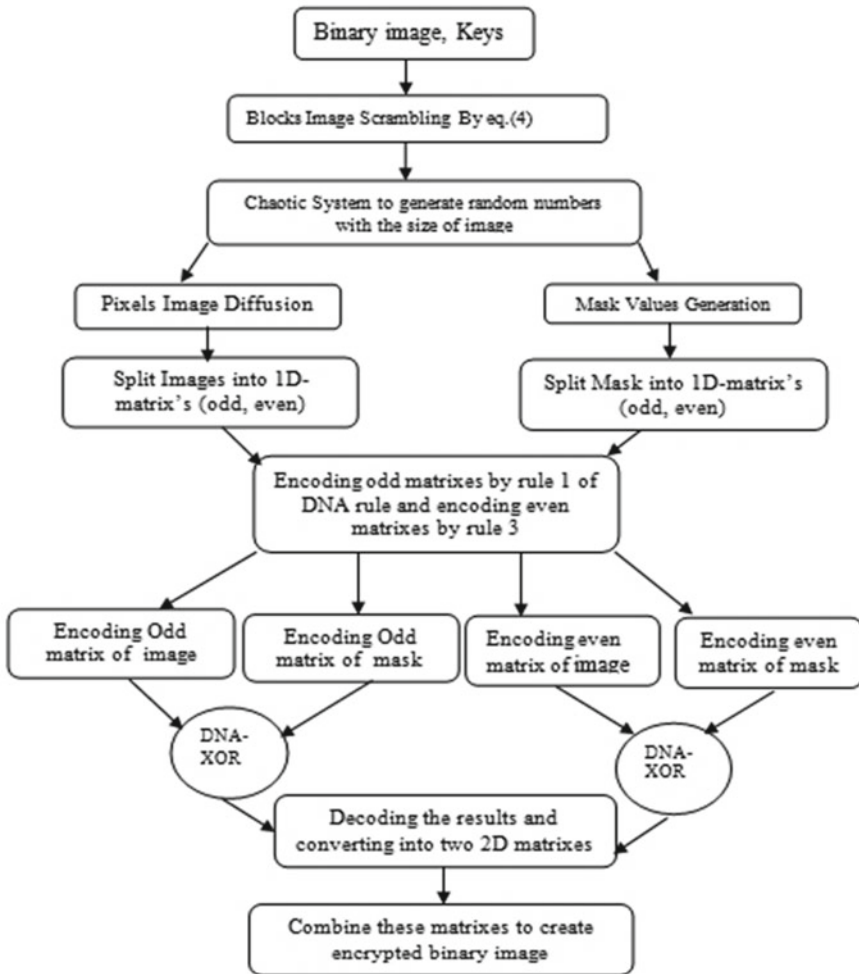


Fig. 6 Encryption processes

### 5.2 Decryption Process

The decryption process is the inverse operation of the encryption process. Figure 7 shows the proposed decryption process.

The decryption algorithm is listed as follows:

Input:

The Encryption binary image E

Position Key PK

Chaotic Key C K

Output: Decrypted binary image

Step 1: Start

Step 2: Use Chaotic Key (C K) to generate random vector with the size of image based on quadratic chaotic system according to Eq. (6).

Step 3: Generate a mask (M) according to Eq. (7) by using the generated random vector in Step (2).

Step 4: dividing M in to two groups. One for odd position pixels (C) and other for even position pixels (D).

Step 5: convert C, D to two 1D array C1 and D2, respectively.

Step 6: dividing E into two arrays according to odd and even rows pixel positions A, B, respectively.

Step 7: converting A, B to 1D arrays A1, B1.

Step 8: applying XOR operation between A1 and C1, and between B1 encoded and D1 to result X1, X2.

Step 9: decode the resulting from Step 8 X1, X2.

Step 10: converting X1, X2 from 1D array to 2D array .

Step 11: combine arrays generated from Step 10 to reconstruct the image L1.

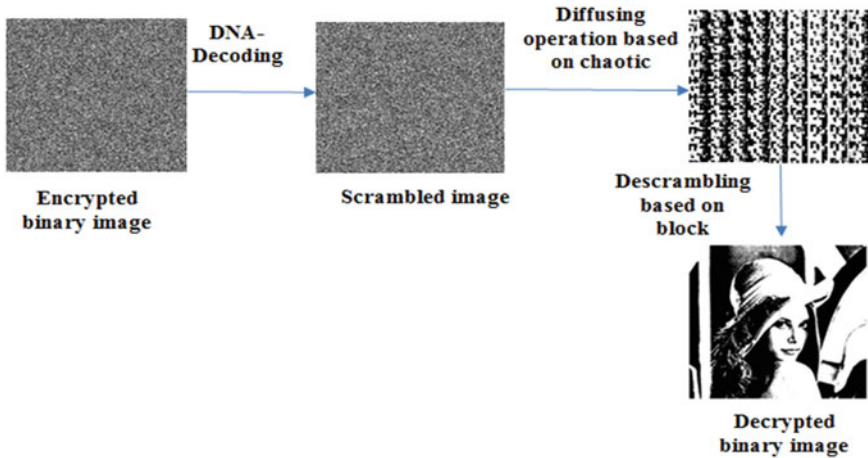


Fig. 7 Proposed decryption process

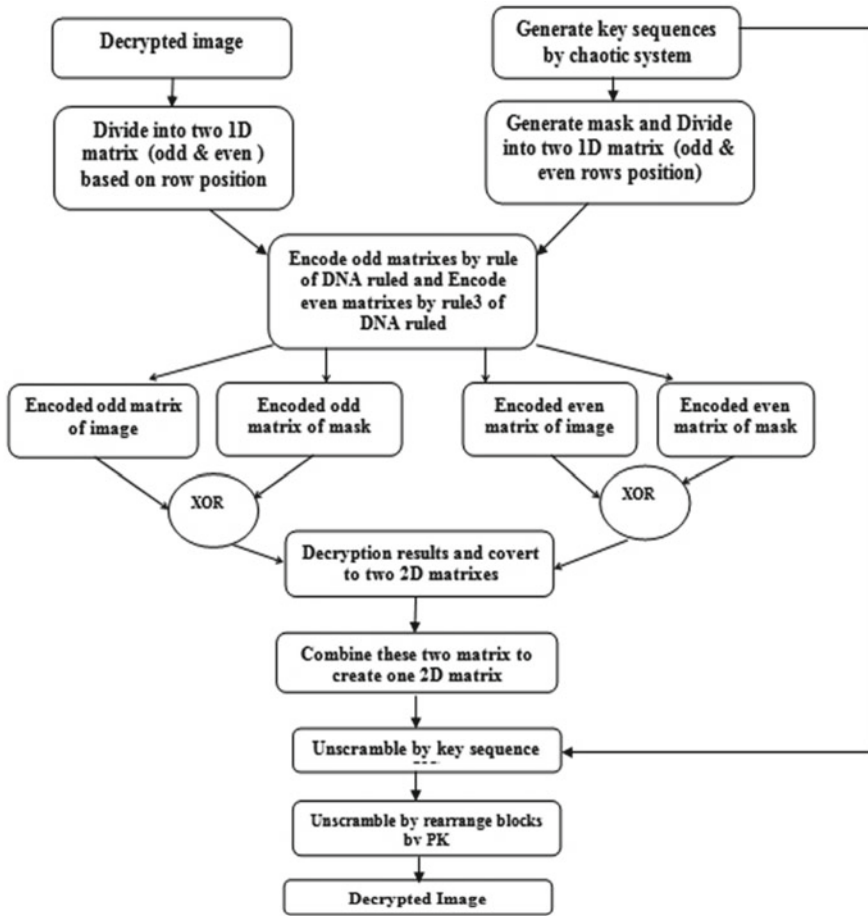


Fig. 8 Proposed decryption system

Step 12: use CK to descramble L1 to result L2

Step 10: dividing L2 in to no overlap  $n \times n$  pixels.

Step 11: descramble blocks resulting from Step 10 by using PK to obtain the original image.

The decryption proposed system is shown in Fig. 8.

## 6 The Experimental Results

The experiments are conducted on different PK standard images with different characteristics such as more details and large areas with the same color. These binary images of

size  $512 \times 512$  are ‘Lena,’ ‘Baboon,’ ‘Cameraman,’ ‘House,’ and ‘Pirate’ as shown in Fig. 9 the original tests images and with corresponding permuted encrypted images by proposed algorithm. As it is noticed that the encrypted image is similar to noise image, there is no relationship with the original image.

To assess the effectiveness of proposed cryptography algorithm, some performance measurements are used.


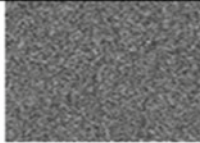


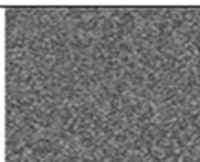


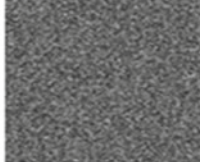


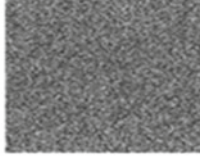


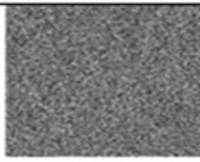

Original Image	Encrypted Image	Decrypted Image
 Lena		
 Baboon		
 Cameraman		
 House		
 Pirate		

Fig. 9 Results of encryption process

**Table 3** Entropy of original images and its encrypted images

Image name	Lena	Baboon	Cameraman	House	Pirate
Entropy	0.9999	0.99998	0.99919	0.99961	0.9995

## 6.1 Entropy

Entropy refers to the amount of information contains in a data set, and it exhibits how the gray values are dispensed in the image. The value of entropy is always positive, and the higher the entropy value, the more it indicates that the amount of information carried by the variable is high. The entropy can be calculated by Eq. (10).

$$H(S) = - \sum_{i=0}^{n-1} P(S_i) \log_2 P(S_i) \quad (10)$$

where  $S_i$  represents gray scale,  $P(S_i)$  is probability of ( $S_i$ ), and  $n$  is the number of gray scale. The entropy of binary image is (1) or close to it, and the entropy of test binary images for proposed system is shown in Table 3.

It can be noted that the entropy of the encrypted image information for all test images is very nearby to (1) and that the suggested algorithm has a greater dominance.

## 6.2 Correlation Coefficient (CC)

The correlation coefficient (CC) is one of the most important statistical measures. The value of it shows the difference between the plain and encrypted image. When the value of the correlation coefficient approaches to (1), this means that the correlation between the two images is very high. Consequently, the encryption system will be vulnerable against attacks. Meanwhile, when the value of the correlation coefficient approaches to (0), this means that the correlation between the two images is very low. Consequently, the encryption system will be robust against attacks. The CC is evaluated according Eq. (11).

$$CC = \frac{\sum_m \sum_n (A_{mn} - A') * (B_{mn} - B')}{\sqrt{\sum_m \sum_n (A_{mn} - A')^2 * (B_{mn} - B')^2}} \quad (11)$$

where  $A'$  and  $B'$  are the average of original image and encryption image, respectively, and the (CC) of the tested images is shown in Table 4.

It can be noted that the correlation value is less than (0). This correlation is critically weakened and for ciphered images viewing a robust randomness. This indicates that the effectiveness of image encryption is good and higher security level.

**Table 4** Correlation of original images and its encrypted images

Image name	Lena	Baboon	Camera man	House	Pirate
Correlat-ion	-0.0013	0.00154	-6.92872	0.00123	-0.0010

**Table 5** Avalanche effect (AE) of original images and its encrypted images

Image name	Lena	Baboon	Camera man	House	Pirate
AE	0.5006	0.4992	0.5032	0.5012	0.5023

### 6.3 *Avalanche Effect (AE)*

The avalanche effect (AE) represents the percentage to measure the efficiency of the propagation method used in the encoding system. If the value of the avalanche effect is high, this means that the random spread of the bits is strong and that any change occurs in one of the bits of the input image (the original image) causes a large change in the bits of the resulting image (the encoded image). The avalanche effect (AE) is evaluated by Eq. (12).

$$AE = \frac{\sum_{i=1}^M \sum_{j=1}^N [C(i, j) - C'(i, j)]^2}{M * N} \tag{12}$$

where  $C$  and  $C'$  are to plain image and encryption image, respectively, and  $M$  and  $N$  are the row and column of image. Table 5 shows the AE of the tested images.

Table 5 illustrates that the lowest value for AE is (0.4992) for the tested images. That means the randomization diffusion is large and almost half of the bits differ between these encoded and plain images. This shows high robustness of the proposed system.

### 6.4 *NPCR and UACI*

The number of variable pixel rate (NPCR) and uniform variable intensity average (UACI) are used to estimate the strength of the encoded image against various raids. Usually in digital images, the values of (NPCR) and (UACI) are equaled. The (NPCR) and (UACI) can be calculate by applying Eqs. (13) and (15), respectively.

$$NPCR = \frac{D(i, j)}{W * H} * 100\% \tag{13}$$

where  $W$  and  $H$  are row and column for image, respectively, and  $D$  is calculated based on the following formula:



**Table 6** NPCR and UACI of original images and its encrypted images

Image name	Lena	Baboon	Camera man	House	Pirate
NPCR and UACI	50.0682	49.9286	50.3242	50.3242	50.2330

$$D(i, j) = \begin{cases} 1 & \text{if original}_{\text{image}(i,j)} = \text{decryption}_{\text{image}} \\ 0 & \text{otherwise} \end{cases} \quad (14)$$

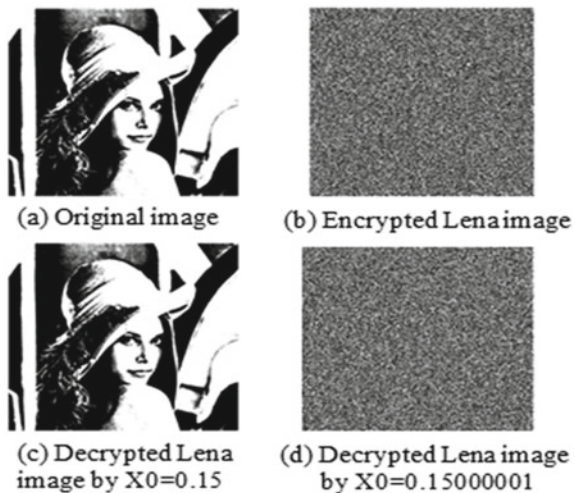
$$\text{UACI} = \frac{1}{W * H} \left[ \sum_{i,j} \frac{W(i, j) - W'(i, j)}{2^L - 1} \right] \quad (15)$$

where  $W$  and  $H$  are row and column for image, respectively, and  $L$  is the number of gray levels. Table 6 shows the value of each after testing a set of binary images by proposed system.

### 6.5 Key Sensitivity Analysis

It is considered as one of an important measurement that used to evaluate the encryption systems. It is used to determine the sensitive of the encryption system to very slightest modification in secret key that used in encryption and decryption process [12]. In the proposed system, the secret key value is ( $x_0 = 0.15$ ) that it used to encrypt (Lena) image, as show in Fig. 10b, then we modified the secret key to ( $x_0 = 0.15000001$ ) and used it to decryption the image result from encryption Lena image, shown in Fig. 10d. Obviously, decoding by slightly modifying the secret key

**Fig. 10** Sensitivity of encryption process to the secret key



presented us with a completely different image from the original image. That means the proposed system is very sensitive to any slightest modification in secret key.

## 7 Conclusions and Suggestions for Futures Works

This paper proposed a robust encryption and decryption method. In order to increase the security layer, more than one method is used to scramble the image before doing the encryption operation. Later, the encryption operation is done with DNA encoding. The decryption is done in the opposite operation of the encryption. According to the experimental results, the proposed method satisfies the requirements of image security.

The suggestions for future works can be shown as follows:

1. Studying the ability of applying a method to select the best DNA rule for encoding using evolutionary approach.
2. Studying the ability of applying the proposed method in another image types such as gray and color.
3. Studying the ability of combining the proposed method with another security mechanisms such as steganography or watermarking in order to increase the security layer of transmitted the digital media through unsecure channel.

**Acknowledgements** This work was supported by Department of Computer Science, College of Science for Women, University of Babylon, Babylon, Iraq.

## References

1. Venkat PK, Magesh S (2017) A survey on encryption algorithms using modern techniques. *Int J Pure Appl Math* 117(16):673–678
2. Popli M, Gagandeep (2019) DNA cryptography: a novel approach for data security using flower pollination algorithm. In: *International conference on sustainable computing in science, technology & management*, pp 1–10
3. Dwivedi N, Gupta RK, Agarwal S (2016) Image encryption using curved scrambling and diffusion. *Int J Eng Technol* 8(6):2990–2991. <https://doi.org/10.21817/ijet/2016/v8i6/160806262>
4. Nandy N, Banerjee D, Pradhan C (2018) Color image encryption using DNA based cryptography. *Int J Inf Technol*. <https://doi.org/10.1007/s41870-018-0100-9>
5. Paul S, Dasgupta P, Naskar PK, Chaudhuri A (2017) Secured image encryption scheme based on DNA encoding and chaotic map. *Int Inf Eng Technol Assoc* 4(2):70–75. <https://doi.org/10.18280/rces.040206>
6. Houas A, Mokhtari Z, Melkemi KE, Boussaad A (2016) A novel binary image encryption algorithm based on diffuse representation. *Int J Eng Sci Technol* 19(4). <https://doi.org/10.1016/j.jestch.2016.06.013>

7. Chai X, Gan Z, Yuan K (2017) A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural Comput Appl*, 219–237. <https://doi.org/10.1007/s00521-017-2993-9>
8. Luo H, Ge B (2019) Image encryption based on Henon chaotic system with nonlinear term. *Multimedia Tools Appl*, 34323–34352. <https://doi.org/10.1007/s11042-019-08072-4>
9. Mohamed HG, ElKamchouchi DH, Moussa KH (2020) A novel color image encryption algorithm based on hyperchaotic maps and mitochondrial DNA sequences. *Entropy* 22(2). <https://doi.org/10.3390/e22020158>.
10. Athira A, Basu P (2020) A novel technique for image encryption using transform based scrambling and DNA based multi chaotic encoding scheme. In: *AIP Conference Proceedings*, vol 2222. <https://doi.org/10.1063/5.0004250>
11. Ramadan N, Ahmed HEH, Elkhamy SE, El-samie FEA (2016) Chaos-based image encryption using an improved quadratic Chaotic map. *Am J Signal Process* 6(1):1–13
12. Guesmi R, Farah MAB, Kachouri A, Samet M (2015) A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2. *Nonlinear Dyn* 83:1123–1136. <https://doi.org/10.1007/s11071-015-2392-7>