



## DNA-based Image Security Algorithm Using Imperialist Competitive Algorithm

---

Amir Mosavi

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

March 5, 2020

# DNA-based Image Security Algorithm Using Imperialist Competitive Algorithm

Amir Mosavi<sup>1,2,3,4</sup>

<sup>1</sup> School of the Built Environment, Oxford Brookes University, Oxford OX3 0BP, UK; a.mosavi@brookes.ac.uk

<sup>2</sup> Institute of Structural Mechanics, Bauhaus Universität Weimar, 99423 Weimar, Germany

<sup>3</sup> Department of Mathematics and Informatics, J. Selye University, 94501 Komarno, Slovakia

<sup>4</sup> Kalman Kando Faculty of Electrical Engineering, Obuda University, 1034 Budapest, Hungary

**ABSTRACT** Medical data should have been kept safe over an insecure network throughout the Internet against adversary attacks. This paper proposes a symmetric image encryption method using logistic map, Deoxyribonucleic acid (DNA) and Imperialist Competitive Algorithm (ICA). First, logistic map and DNA are used to create initial population of ICA through constructing specified number of encrypted images. Then, ICA optimizes encrypted images through iterative assimilation of selected images. However, a two-field decryption table has also been introduced for decryption process. The experimental results approve the high quality of the proposed encryption method by resisting variety of typical attacks.

**INDEX TERMS** Image encryption, Deoxyribonucleic acid, ICA, chaotic map

## I. INTRODUCTION

Image encryption is necessary to securely protect transmitted images from unauthorized access over the Internet [1]. So, it is important to make the image information unreadable. In image encryption, the original image which is known as plain image is encrypted to the cipher image using encryption methods. Basically, linear correlation of neighboring pixels are high in plain images and this makes the conventional encryption algorithms inefficient for proper encryption against third parties [1, 2].

Chaotic map functions have been widely used in recent encryption methods [3-7]. Chaotic maps generate series in [0,1] using a secret key in which the key impacts on the series directly. Moreover, the dynamic behavior of chaotic map functions results in continuous change in the system based on the current condition. This change is surely based on the feedbacks as intrinsic behavior of chaotic maps.

Deoxyribonucleic acid (DNA) are nucleic acids which are vital for any organism. Application of DNA is a new interesting trend in symmetric image encryption [8-12]. The security of DNA-based encryption methods were sufficiently high against well-known attacks in the field [12]. However, to improve the security of DNA-based methods evolutionary algorithms have also been added in encryption methods.

It was believed that application of evolutionary algorithms could generate more robust optimized cipher images [13-15]. Generally, studying the literature reveals that exploiting the dynamic behavior of chaotic maps as well as the concept of

DNA could generate a good solution for image encryption. In addition, the optimization power of evolutionary algorithms creates a robust symmetric image encryption method.

Enayatifar et al. proposed a hybrid method of chaotic maps and DNA for permutation and diffusion steps. In permutation step, the pixels of plain image were reallocated keeping the entropy unchanged. However, in diffusion step the gray level of pixels were changed. The security of proposed encryption algorithm was validated against differential attacks, brute-force attacks, and statistical attacks. The speed test also proved the acceptable performance of the proposed method by overlapping permutation and diffusion steps [16]. The proposed method achieved the final entropy of 7.9994 for Lena image of size  $512 \times 512$ . Moreover, the UACI and NPCR of the hybrid method was 0.336 and 0.996 respectively regarding Lena image of size  $512 \times 512$ .

However, Enayatifar et al. also proposed a hybrid model of logistic map, GA, and DNA sequence. The goal of the study was to find the best DNA mask for plain image encryption. Logistic map and DNA sequences were used to generate several DNA masks. Afterwards, GA identified the best DNA mask through iterative optimization in 3284 milliseconds with best UACI and NPCR of 0.337 and 0.997 respectively. The proposed method also reached the best entropy of 7.9997 in iteration 78. Obviously, It is clear that the utilization of GA could improve the security of the encryption algorithm [17].

Pujari et al. proposed a hybrid method of DNA sequence and Genetic Algorithm (GA). The proposed model composed

of two major phases namely, scrambling and substitution. In the first phase the image pixels were changed to minimize the correlation among adjacent pixels. Then, the gray level of pixels were converted to DNA sequences using DNA rules. However, the investigation of the results were not comprehensive [18].

Abdullah et al. proposed a robust encryption algorithm using GA and chaotic maps. First, a number of encrypted images were constructed using the plain image and the chaotic function as initial population of GA. Next, GA found the final encrypted image using iterative optimization of initial population based on entropy and correlation coefficient. The best entropy and diagonal correlation coefficient were 7.9978 and  $-0.0009$  for Lena image of size  $256 \times 256$  respectively [15].

Wu et al. proposed a novel 2D chaotic map called 2D-HSM using Henon map and Sine map. Next, the hybrid method of 2D-HSM and DNA approach was proposed in which 2D-HSM and DNA sequence were used in permutation and diffusion respectively. The proposed method achieved the entropy of 7.9976 for Lena image of size  $256 \times 256$  and 7.9974 for Boat image of size  $512 \times 512$ . The investigation of correlation coefficient and differential attacks showed that the proposed method is competitive against state of the arts [9].

It can be concluded that proper exploiting the evolutionary algorithm could improve the security of the encryption method with acceptable execution time. Thus, in this paper a novel encryption method based on DNA sequence and Imperialist Competitive Algorithm (ICA) has been proposed so that the initial population of ICA is constructed using DNA and logistic map function.

The rest of this paper is as follows. In Section II basic concepts of Logistic Map, Deoxyribonucleic acid sequence, and Imperialist Competitive Algorithm (ICA) are described. In Section III the proposed method is identified. Section VI demonstrated the results and further analysis of ICA. Finally, the paper is concluded in Section V.

## II. PRELIMINARIES

Section II describes major concepts which have been used in the proposed method namely, logistic map, Deoxyribonucleic acid (DNA), and Imperialist Competitive Algorithm (ICA).

### A. LOGISTIC MAP

Logistic map is a nonlinear polynomial dynamic equation which can produce incredibly chaotic results [5]. Mathematically, logistic map (function) can be shown using Equation 1 in which  $R$  is generally selected in  $[0,4]$  which is assumed 3.99 in this research. Moreover,  $x_n$  is a random number in  $[0,1]$ . The dynamic behavior of the logistic map

function for  $R = 3.99$  and  $X_n = 0.3$  regarding 500 iterations is shown in Figure 1.

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

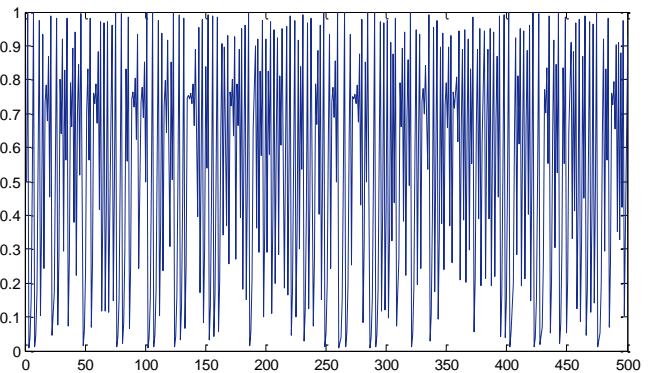


FIGURE. 1. Logistic map for  $R = 3.99$  and  $X_0 = 0.3$  regarding 500 iteration

### B. DEOXYRIBONUCLEIC ACID SEQUENCE

Deoxyribonucleic acid (DNA) is a double-stranded chains of nucleic acids namely, cytosine (C), guanine (G), adenine (A) and thymine (T) [12]. According to the base pairing rules as shown in Figure 2 A bounds with T, and C bounds with G to form a double-stranded DNA which is a basic idea of passing hereditary information between generations. Thus, the binary coding rules for nucleic acids can be derived so that each nucleic acid is considered as a two-bit digit with 8 distinguished possibilities as shown in Table 1. Thus, assuming four consecutive nucleic acids of ACCG in Figure 2 results in 8 different binary representations using rules of Table 1. In addition, XOR operation can also be defined on DNA genetic codes based on Table 2. Hence, XOR of rules 1 and rule 2 in Figure 2 results in an 8-digit binary sequence (00111111). The binary sequence could be converted to the relevant DNA sequence according to Table 2.

TABLE I  
BINARY CODING RULES FOR DNA SEQUENCES

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

TABLE II  
XOR OPERATOR FOR DNA NUCLEIC ACIDS

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

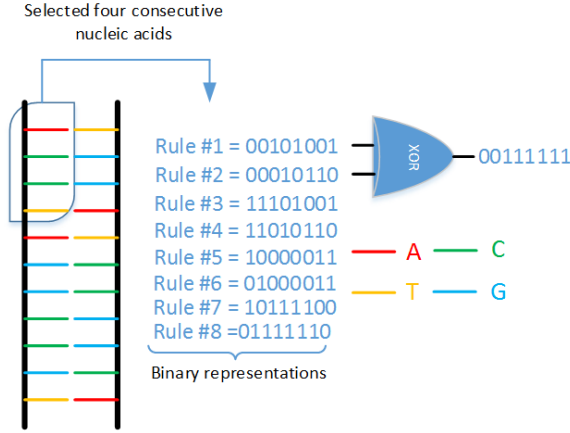


FIGURE 2. Binary representation of ACCG and XOR of Rule 1 and Rule 2

### C. IMPERIALIST COMPETITIVE ALGORITHM

Imperialist Competitive Algorithm (ICA) is an effective optimization algorithm which is widely applicable in various domain of engineering [19-21]. Generally, ICA starts by defining initial population so that each individual is called a country. The countries with the best fitness are usually selected as imperialists while the rest form the colonies of these imperialists. Each imperialist with its relevant colonies is called an empire. Afterwards, the colonies in each empire move toward the relevant imperialist using assimilation operator. However, to avoid local optima the properties of each colony may change randomly using revolution operator.

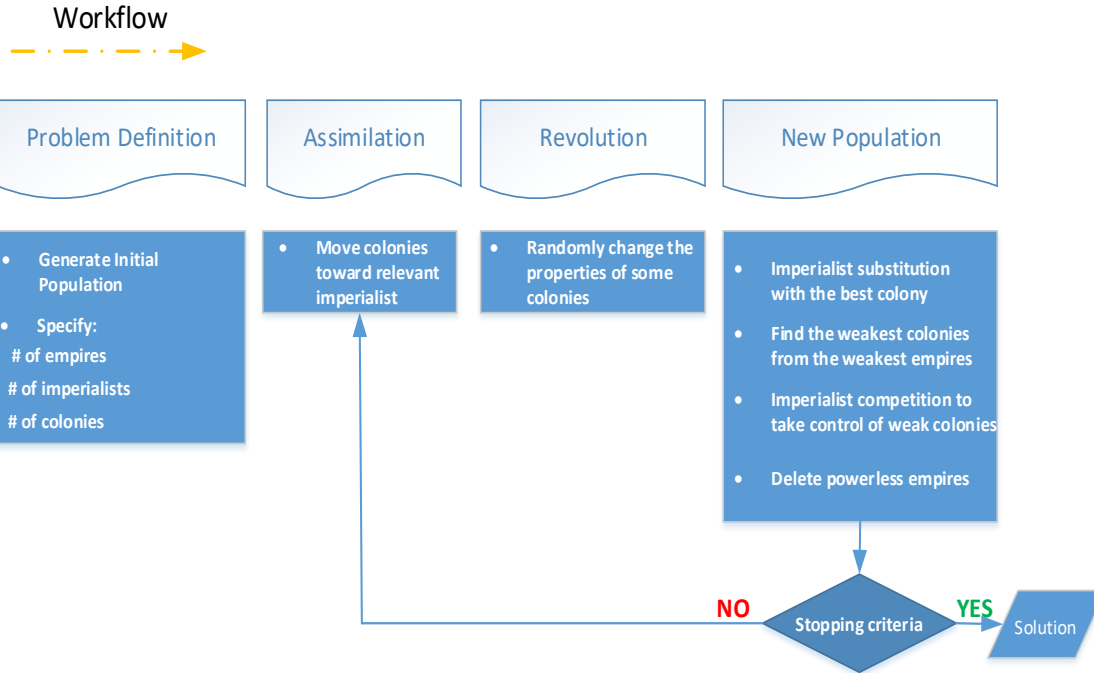


FIGURE 3. Workflow of ICA

### B. INITIAL POPULATION GENERATION

The proposed method has two steps. First, initial population of Imperialist Competitive Algorithm (ICA) are generated as mentioned earlier. Then, ICA optimizes the solutions

Moreover, the total power of each empire is defined as the power of the imperialist as well as the percentage of the mean power of its relevant colonies. After assimilation and revolution, the best colonies are found for possible substitution with related imperialist. Next, the imperialists compete for colonies of weak empires using roulette wheel process. The empires with no colonies will be deleted. The stopping criteria is existence of one empire and deletion of others. The above steps can be summarized as Figure 3.

### III. PROPOSED METHOD

Prior to start the proposed method, the 128-bit key should be generated as the initial key. Next, the main two steps of the proposed method begin so that initial population of ICA (initial number of cipher images) should have been generated using DNA and chaotic map as a logistic map function firstly. Then, ICA optimizes the solutions through assimilation secondly.

#### A. INITIAL KEY GENERATION

Initially, the 128-bit key should be introduced to generate the first element of the logistic map ( $x_0$ ) as shown in Equation 2.

$$x_0 = \frac{k_{15,0}^{127} + k_{15,1}^{126} + \dots + k_{8,0}^{63} + \dots + k_{0,6}^1 + k_{0,7}^0}{2^{128}} \quad (2)$$

Where  $K_i$  is the 8-bit character and  $K_{i,j}$  is jth bit from ith character respectively.

iteratively to converge to final solution which here is the optimal cipher-image as stated in Section III. Hence, the process of generating initial population of the ICA is explained in the following. Initially, the plain-image should have been

converted to the binary format. Meanwhile, a 128-bit key is used to generate  $x_0$  in the chaotic map. Then, chaotic map will generate series of elements according to Equation 1 in which each four successive elements can be considered as a tuple so that the first element is used to generate a random number in  $[0,255]$  and the other three elements are used to generate random numbers in  $[1,8]$ . Next, the random number in  $[0,255]$  is converted to the corresponding binary format which represents a key. Likewise, three random numbers in  $[1,8]$  are used to specify the corresponding rule numbers for generating the DNA of the relevant key, DNA of the relevant pixel in the plain-image, and converting the DNA XOR image to the relevant binary format. Afterwards, the binary DNA pixel is converted to the relevant decimal format and is embedded to the cipher-image. Similarly, the entire pixels within the plain-

image should have been converted to the corresponding pixels in the cipher-image. Since, initial population of ICA incorporates specified number of solutions, specified number of cipher-images should have also been generated using the plain-image accordingly. In addition, each image in initial population should have a unique integer identifier so that each identifier denotes the number of images in order of generation which is further invoked in decryption table generation. Figure 4 shows the process of generating a cipher-image from the plain-image.

### C. ICA STEP

The initial population from Section III are used in optimization process of ICA. The ICA follows the conventional ICA. However, the assimilation process differs noticeably which has been explained in the following.

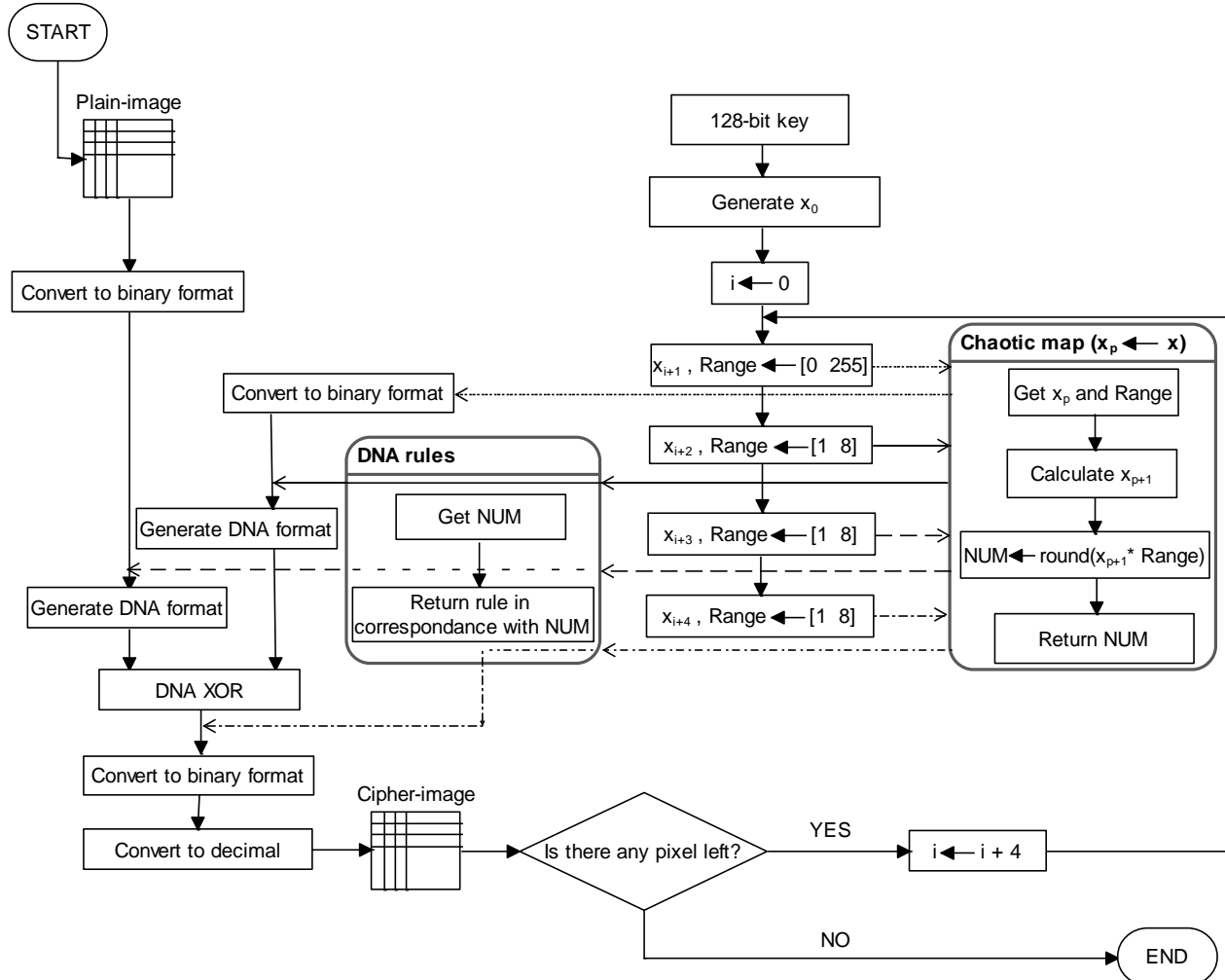


FIGURE 4. One cipher-image generation for initial population of ICA

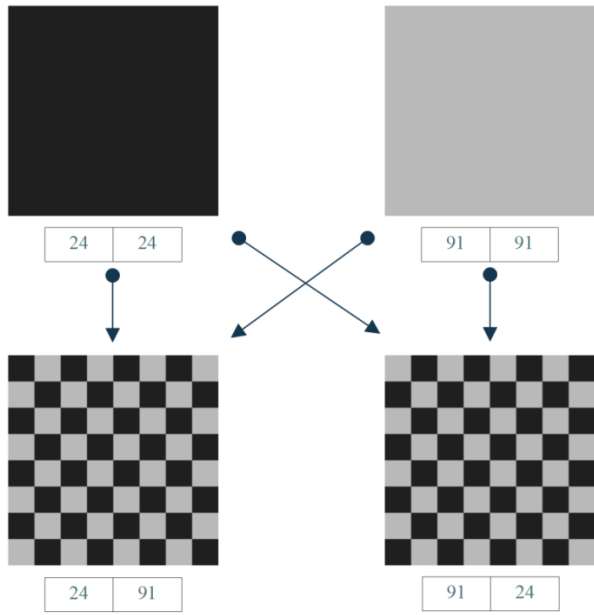


FIGURE 5. Assimilation process

The assimilation process generates two checkered offspring images from parents in which each offspring incorporates alternative pixels of parents. Regarding the first offspring, if the sum of row number and column number is even the first parent's corresponding pixel is transferred to the relevant position in the offspring. In contrast, if the sum of row number and column number in the offspring is odd, the corresponding pixel from the second parent is transferred to relevant position

in the offspring. Finally the pixels in the second offspring should have also been transferred from the parents in reverse order with respect to the first offspring. Afterwards, a decryption table of two fields should have been updated for each recently generated offspring. The decryption table includes the parents' identifier for each offspring. Figure 5 illustrates the assimilation process as well as the decryption table. Furthermore, Table 3 shows the pseudo code of proposed ICA.

#### IV. EXPERIMENTAL RESULTS

The robustness of the proposed method has been investigated on ten standard images of medical optical images including the smallest size of  $225 \times 225$  to the biggest size of  $696 \times 876$  in Figure 6. The implementation has been carried on with Python 3 on a PC with the following platform (including hardware specifications and operating systems):

- Intel Core i7, 2.3 GHz CPU
- 8 GB memory
- 500 GB hard disk
- Windows 8 professional operating system.

In order to assess the stability of the proposed encryption method, the impacts of well-known attacks have been investigated on the cipher image including in Sections IV to 4.4.

TABLE 3  
PSEUDO-CODE OF THE PROPOSED METHOD

---

<b>Input :</b>	<i>Initial countries</i>
<b>Output :</b>	<i>Optimum Cipher-Image</i>

---

1. *countries*  $\leftarrow$  Null array of size "number of countries"
2. **FOR**  $i \leftarrow 1$  to number of countries
3.     *countries*[ $i$ ]  $\leftarrow$  create a country using Figure 3
4. **END FOR**
5. Create empires using *countries*
6. Determining 5 percent of more powerful *countries* as imperialist
7. Imperialist absorb colonies among remaining *countries* regarding to their power
8. **WHILE** just one empire will remain **DO**
9.     Do assimilation part regarding Figure 4
10.    Apply revolution part on the 10 percent of each empire population
11.    **IF** power (most powerful colony in each empire) > power (corresponding imperialist) **THEN**
12.        Exchanging the most powerful colony and imperialist position
13.    **END IF**
14.    Do imperialists competition for seizing the weakest colony in the weakest empire
15. **END WHILE**

---

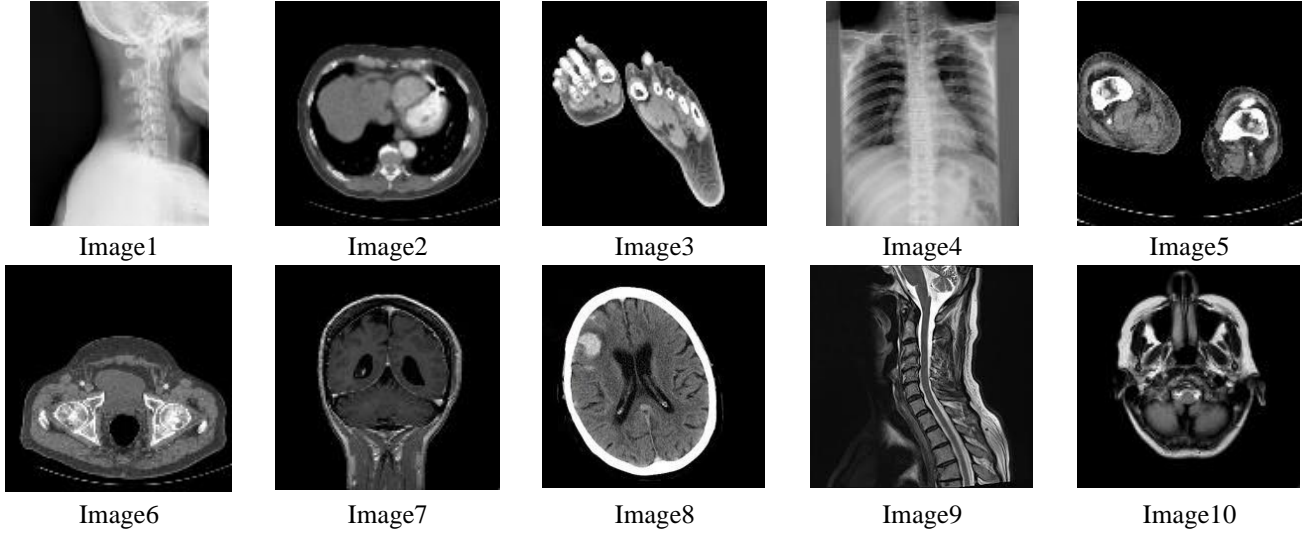


FIGURE 6. Standard images

### A. ENTROPY

A good cipher-image should have uniform distribution of the gray levels. Entropy of any image is calculated through Equation 3 which is 8 ideally.  $P(s_i)$  in Equation 3 denotes the probability of occurrence regarding  $s_i$ . The average entropy of the cipher images are calculated after 30 repetitions of the algorithm in Table 4. The entropy results approve the stability of the proposed method.

$$E(s) = \sum_{i=0}^{2^M-1} P(s_i) \log_2 \frac{1}{P(s_i)} \quad (3)$$

### B. STATISTICAL ATTACKS

Statistical attacks calculate the correlation of neighborhood pixels firstly. Second, the histogram analyses of the benchmark images are provided.

#### 1) CORRELATION COEFFICIENT ANALYSIS

The linear correlation of neighboring pixels in a robust encryption method should remain minimum. Thus, the ideal correlation coefficient is 0 in  $[-1, +1]$  in which the extreme points denote the perfect negative and positive correlation. The correlation coefficient of any two neighboring pixels is calculated using the covariance and variance of  $x$  and  $y$  variables based on Equation 4.

$$r_{xy} = \frac{|cov(x, y)|}{\sqrt{V(x)} \times \sqrt{V(y)}} \quad (4)$$

Basically, covariance of two gray levels in adjacent pixels of  $x$  and  $y$  is calculated using Equations. 5, 6 in which  $E(x)$  and  $E(y)$  are the mathematical expectations of  $x$  and  $y$  variables and  $V(x)$  and  $V(y)$  are the respective variances which can be calculated using Equation 7.

$$cov(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \quad (5)$$

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (6)$$

$$V(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \quad (7)$$

Table 5 demonstrates the average correlation coefficients for 8000 pairs of adjacent pixels of cipher images vertically, horizontally, and diagonally.


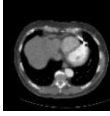


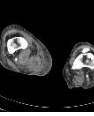
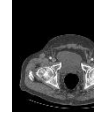
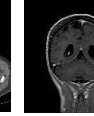
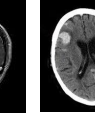
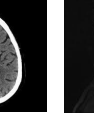

Figure 7 shows linear relationships of vertical, horizontal and diagonal adjacent pixels in Image4 plain and cipher image respectively. The experiments have been conducted on 8000 pairs of adjacent pixels. The correlation in the left section of Figure 6 is high against the right side which is minimum.

TABLE 4  
AVERAGE ENTROPY AFTER 30 REPETITIONS

Entropy	7.9998	7.9995	7.9995	7.9997	7.9994	7.9994	7.9979	7.9974	7.9973	7.9984
Size	696×876	512×512	512×512	696×799	512×512	512×512	256×256	225×225	225×225	288×288



TABLE 5  
AVERAGE CORRELATION COEFFICIENT AFTER 30 REPETITIONS

										
Vertical	0.0055	0.0018	0.0074	0.0057	0.0105	0.0040	0.0036	0.0160	0.0172	0.0046
Horizontal	0.0115	0.0113	0.0070	0.0089	0.0179	0.0127	0.0141	0.0082	0.0051	0.0011
Diagonal	0.0053	0.0050	0.0211	0.0070	0.0007	0.0074	0.0154	0.0082	0.0025	0.0015

2) HISTOGRAM ANALYSIS

The uniform distribution of gray levels in the cipher image results in a uniform histogram. Figure 8 shows the histograms

of Image2 prior to and after encrypting the plain image using proposed method. The experiments reveal that the frequency of gray level pixels has a uniform distribution throughout the cipher image.

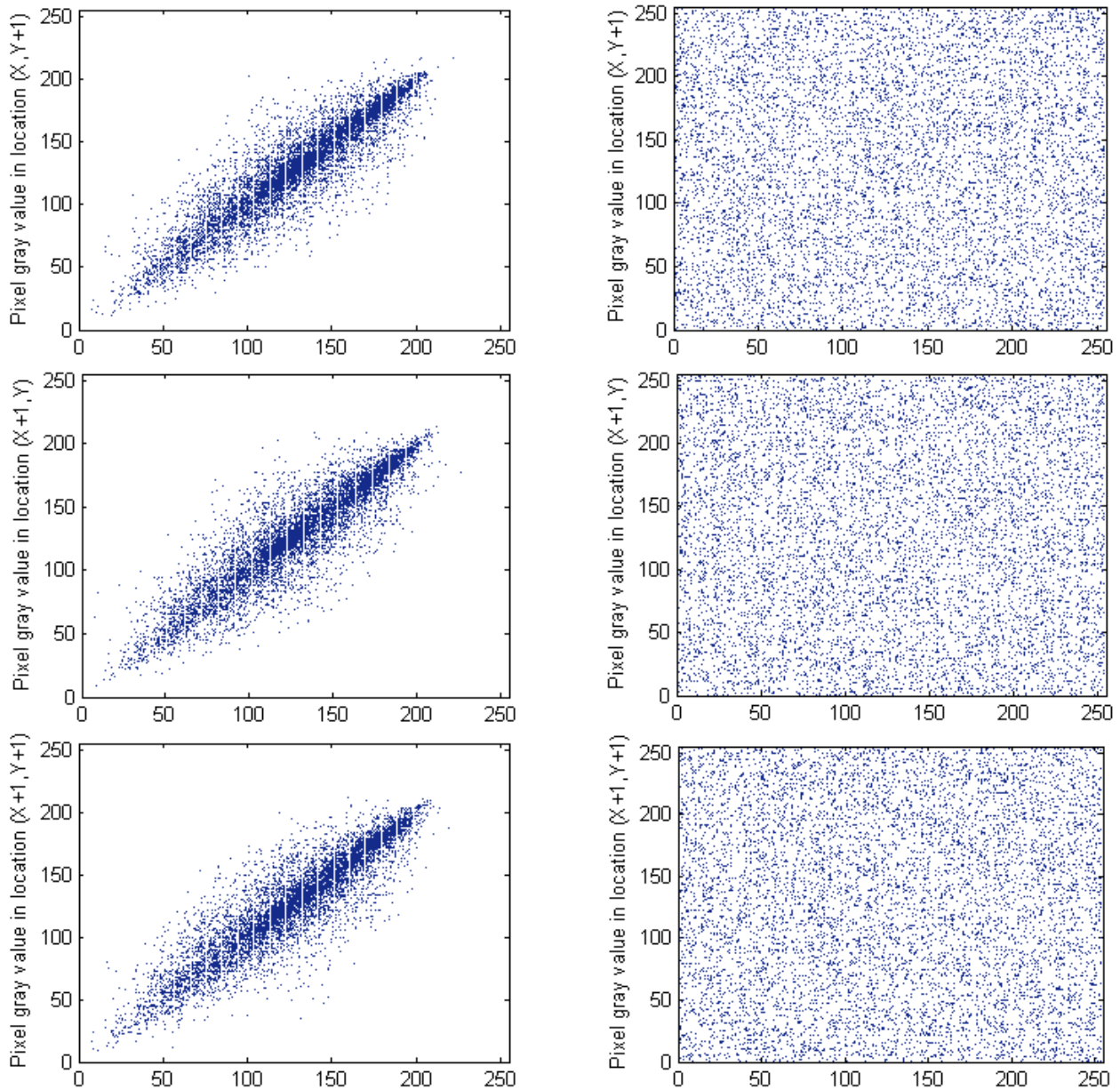


FIGURE 7. Image4's linear relationship of adjacent pixels in plain and cipher image



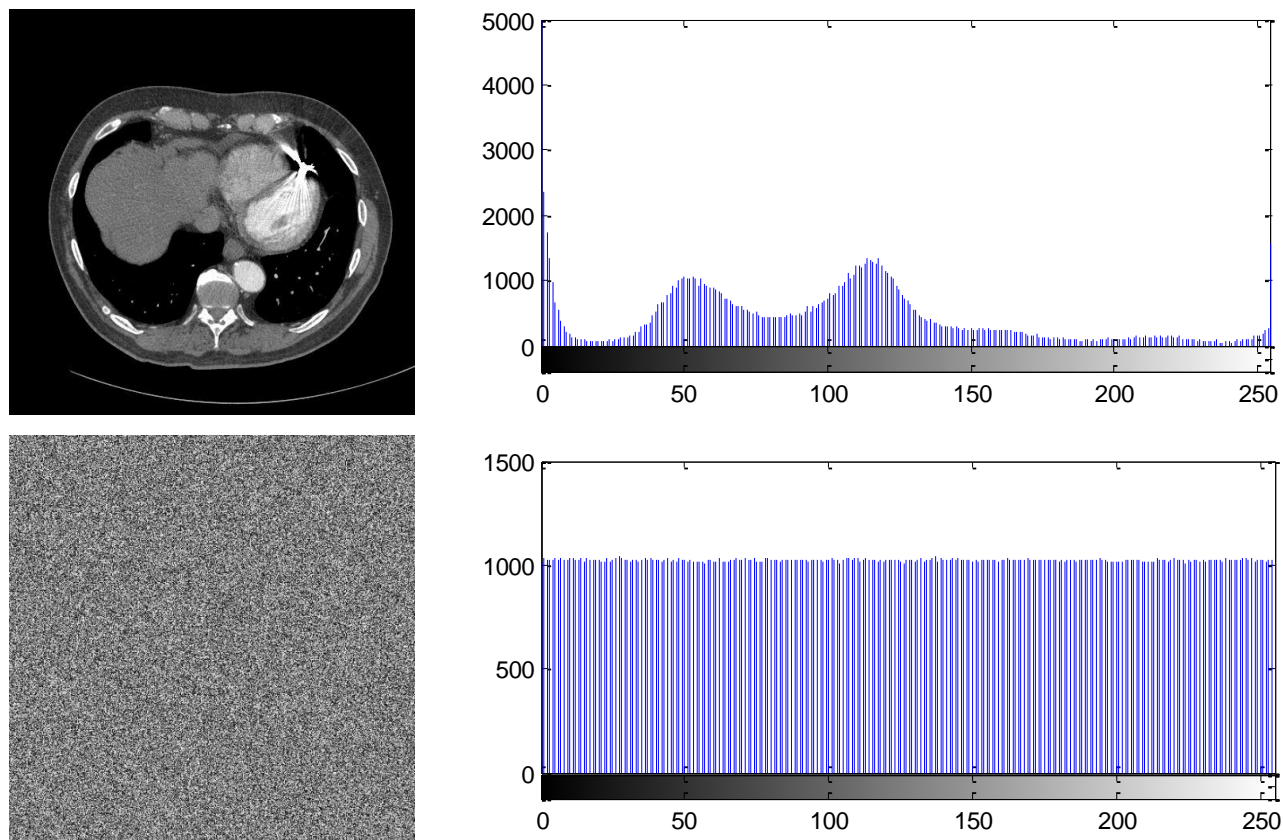


FIGURE 8. From left to right in each row: Plain image, Histogram of plain-image, Cipher image, Histogram of cipher-image regarding Image2

**C. BRUTE-FORCE ATTACK**

Secret key sensitivity and the size of the secret key space are well-known brute-force attacks evaluated on the proposed encryption method.

1) *KEY SENSITIVITY ANALYSIS*

A strong image encryption method should be sensitive to even a trivial alteration in initial value so that a completely new cipher image should have been created. Thus, Image1 with the size of  $696 \times 876$  (Figure6) is encrypted with a secret key of size 128-bit initially. Next, the same image is encrypted via the same secret key with slight variation of the bit value regarding the randomly selected bit. Figures 9b and 9c. show cipher images from the initial and altered secret key

respectively. Figure 9d clearly shows the number of identical gray levels (specified in white color) in both cipher images are trivial. In addition, Table 6 also shows the percentage differences between two cipher-images. All in all, Figure 9d confirms the high sensitivity of proposed method against key sensitivity analysis.

2) *KEY SPACE ANALYSIS*

The encryption key should not be exposable to any third party besides the sender and receiver. Thus, the key space should be sufficiently large to deactivate any attack from the third parties. The secret key space of  $2^{128}$  (calculated from the 128-bit key used to create  $X_0$ ) confirms the resistance of the proposed encryption method against any attacks.

TABLE 6  
THE IMPACT OF 1-BIT VARIATION OF THE SECRET KEY ON THE RESPECTIVE CIPHER-IMAGES IN PERCENTAGE

99.60 %	99.62 %	99.63 %	99.61 %	99.62 %	99.59 %	99.56 %	99.63 %	99.62 %	99.56 %

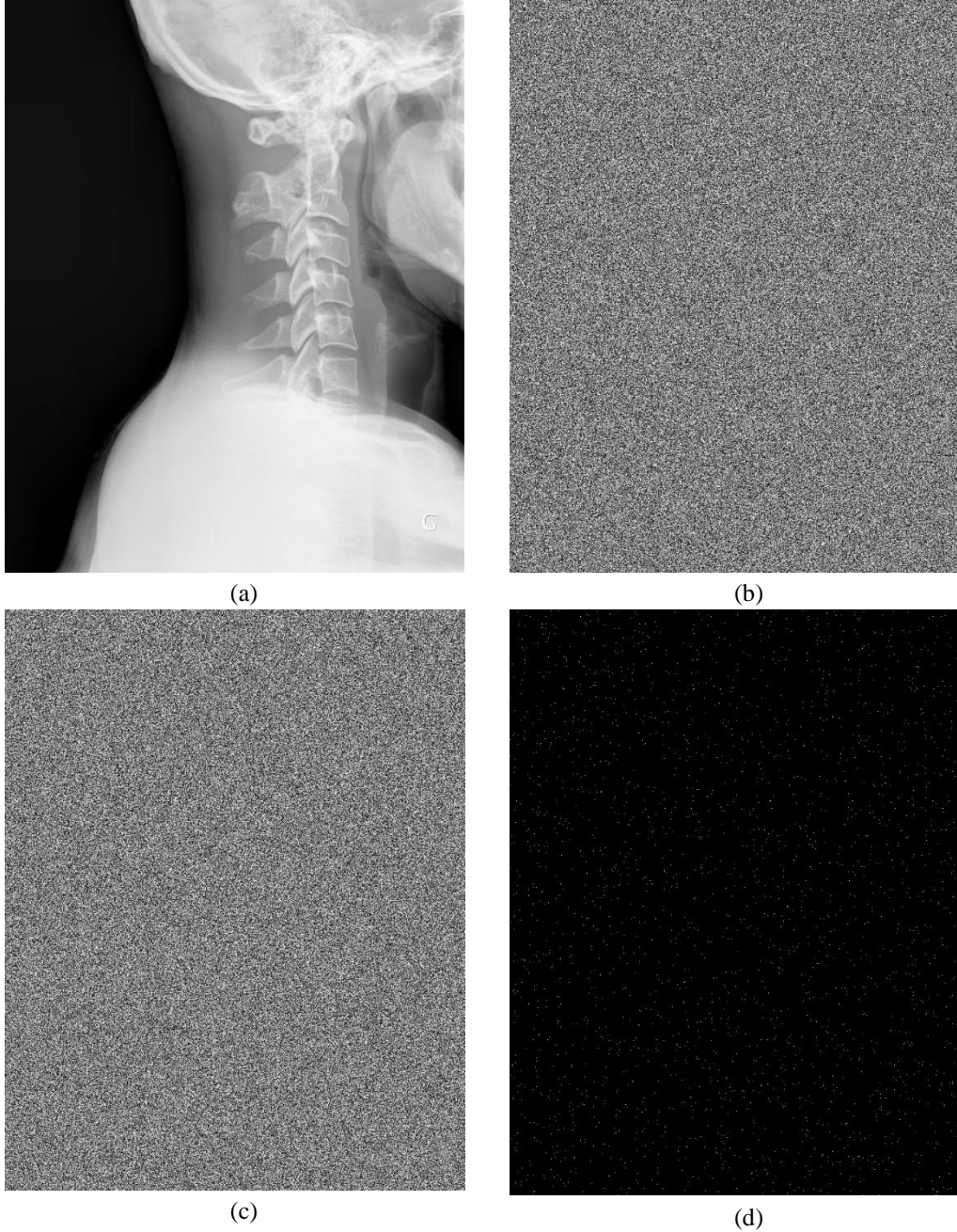


FIGURE 9. a) Plain-image b) Cipher-image with 128-bit secret key c) Cipher-image with the same key as Figure 8b with changing in the value of randomly selected bit d) difference between Figures 8b and 8c

#### D. DIFFERENTIAL ATTACKS

Differential attack grasps the opinion that a slight variation in the pixels of the plain image cause a significant change in the encrypted image. Thus, two measures are used to calculate differential attacks namely, number of pixels change rate (NPCR) and unified average changing intensity (UACI) as in Equation 8 and Equation 9:

$$\text{NPCR} = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i, j)}{M \times N} \times 100\% \quad (8)$$

$$\text{UACI} = \frac{\sum_{i=1}^M \sum_{j=1}^N |C_1(i, j) - C_2(i, j)|}{255 \times M \times N} \times 100\% \quad (9)$$

In which  $D(i, j)$  is calculated as follows in Equation 10:

$$D(i, j) = \begin{cases} 0 & \text{if } C_1(i, j) = C_2(i, j) \\ 1 & \text{if } C_1(i, j) \neq C_2(i, j) \end{cases} \quad (10)$$

$C_1$  and  $C_2$  are two distinguished cipher images with their relevant plain-images initiated from the same key and

different in one-bit. Basically, the greater NPCR/UACI score is, the more resistant the proposed encryption method is against differential attacks. Table 7 shows the average NPCR and UACI of  $C_1$  and  $C_2$  with the proposed encryption method of ten standard images.

**E. ICA ANALYSIS**

This section verifies and validates the embedded ICA within the proposed method through illustrating the relevant box plot of benchmark images and investigating the empire collaspation trend.

1) *BOX PLOT*

Box plots in Figure 10 illustrates the worst and best entropies obtained from 30 repetitions of the ICA so that the line inside the box shows the median of calculated entropies. Figure 10 approves that the entropies calculated using the embedded

ICA in the proposed method are logically distributed and the median splits the box reasonably in most of the cases except in Image3 and Image10 in which the median is closer to the worst entropy. All in all, the box plot illustrated in Figure 10 exhibits the acceptable convergence behavior of ICA and the validity of the results.

2) *EMPIRE COLLAPSATION TREND*

Table 8 shows the trend of empires collaspation through the successive iterations regarding Image4. First, empire 4 has been collapsed in iteration 28 with a relative entropy of 7.9961. Next, empire 1 is the second empire to be deleted including its weak colonies. Then, empires 3 and 5 are deleted in iterations of 65 and 102 respectively. Basically, empire 4 is the strongest empire through 138 iterations with the final entropy of 7.9997.

NPCR	0.996034	0.996085	0.996169	0.996085	0.996091	0.995981	0.996185	0.995911	0.995865	0.995949
UACI	0.334914	0.334647	0.335014	0.334612	0.33423	0.334803	0.334842	0.335446	0.335856	0.334961

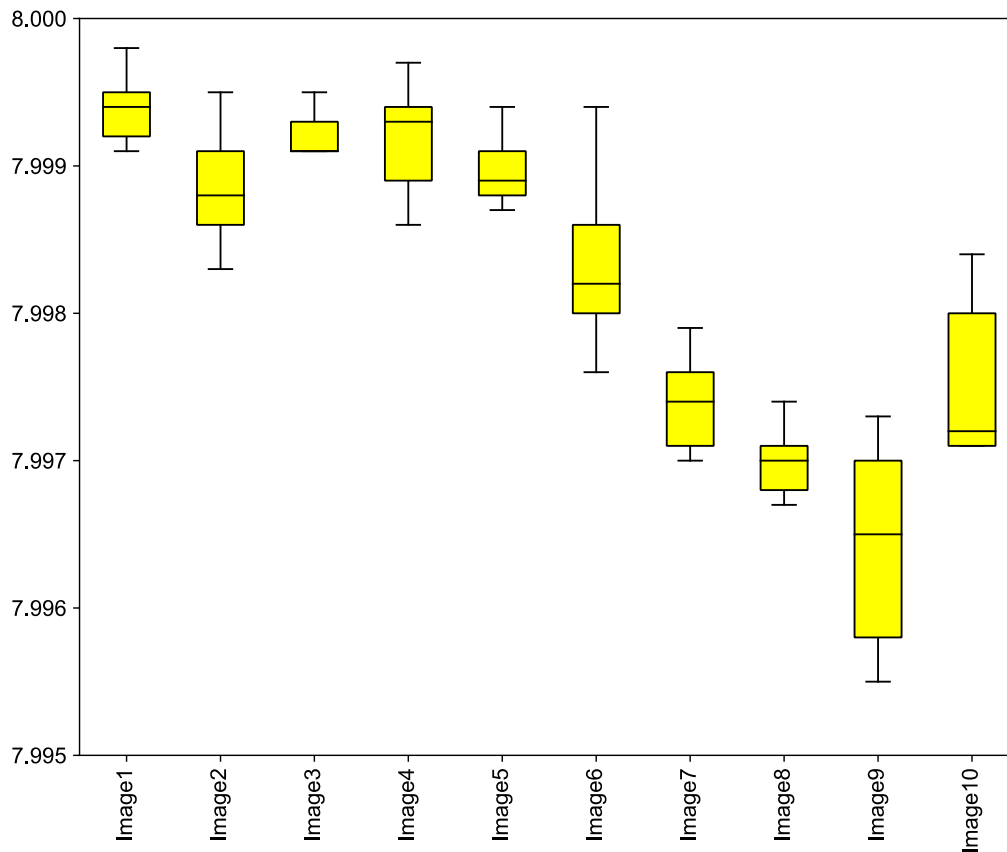


FIGURE 10. Box plot analysis of the embedded ICA within the proposed method

TABLE 8  
EMPIRE COLLAPSE IN SUCCESSIVE ITERATIONS

Iteration	Empire 1	Empire 2	Empire 3	Empire 4	Empire 5
28	7.9964	7.9978	7.9964	7.9961	7.9973
49	7.9965	7.9984	7.9971	---	7.9976
65	---	7.9993	7.9975	---	7.9979
102	---	7.9997	---	---	7.9992
138	---	7.9997	---	---	---

TABLE 9  
COMPARISON OF THE PROPOSED METHOD AND THE RELATED WORKS BASED ON THE EXECUTION TIME AND WELL-KNOWN ATTACKS IN THE LITERATURE

	Entropy	Correlation Coefficient			NPCR	UACI	Exe.Time
		vertical	Horizontal	diagonal			
GA [15]	7.9964	0.0069	0.0078	0.0051	0.993273	0.329094	3597
DHS [14]	7.9952	0.0246	0.0139	0.0093	0.993882	0.322673	2419
ADE [22]	7.9937	0.0091	0.0055	0.0012	0.995186	0.329519	3725
ICA [23]	7.9969	0.0117	0.0071	0.0064	0.993750	0.327701	4184
GA-DNA [17]	7.9987	0.0032	0.0027	0.0029	0.994918	0.333825	3986
Proposed method	7.9984	0.0046	0.0011	0.0015	0.995949	0.334961	4705

## F. COMPARISON

Table 9 compares the encryption power of the proposed method against background encryption methods regarding Image10. The results clearly show the superiority of the proposed method for entropy, correlation coefficient in three dimensions, NPCR and UACI in most of the cases. However, the execution time of the proposed method is not any better. Even in [4] the performance of the embedded ICA is slightly better than proposed method. The reason is that the ICA in [4] intelligently adjusts the weights to converge in less iteration. The superior results of the proposed method make it an appropriate candidate to be used in offline encryption generally.

## V. CONCLUSION

This paper proposed a hybrid method of logistic map, DNA, and ICA for symmetric medical image encryption. First, initial population of ICA is constructed using logistic map DNA iteratively. Thus, the initial population incorporates specified number of cipher images which are then used in ICA for successive optimization. Then, the assimilation operator of ICA proposed in this paper constructs checkered offsprings from parents. However, the proposed method keeps track of assimilation by introducing a decryption table. Box plot analysis and empire collapse trend of ICA validate the convergence behavior of ICA. The results also show how the proposed method outperforms related works while it is exposed against statistical, brute force, and differential attacks. The best entropy achieved is also 7.9998 for the image size of 696×876.

## REFERENCES

- [1] Ghadirli, H.M., A. Nodehi, and R. Enayatifar, *An overview of encryption algorithms in color images*. Signal Processing, 2019. **164**: p. 163-185.
- [2] Gong, Q., et al., *Modified diffractive-imaging-based image encryption*. Optics and Lasers in Engineering, 2019. **121**: p. 66-73.
- [3] Wang, B., F.C. Zou, and J. Cheng, *A memristor-based chaotic system and its application in image encryption*. Optik, 2018. **154**: p. 538-544.
- [4] Vargas Valencia, J.A. and B.A. Rodríguez Rey, *Phase chaotic encryption and efficiency evaluation for an image multiplexing method*. Optics and Lasers in Engineering, 2019. **121**: p. 464-472.
- [5] Han, C., *An image encryption algorithm based on modified logistic chaotic map*. Optik, 2019. **181**: p. 779-785.
- [6] Liu, H., et al., *Image encryption using complex hyper chaotic system by injecting impulse into parameters*. Applied Mathematics and Computation, 2019. **360**: p. 83-93.
- [7] Lan, R., et al., *Integrated chaotic systems for image encryption*. Signal Processing, 2018. **147**: p. 133-145.
- [8] Akhavan, A., A. Samsudin, and A. Akhshani, *Cryptanalysis of an image encryption algorithm based on DNA encoding*. Optics & Laser Technology, 2017. **95**: p. 94-99.
- [9] Wu, J., X. Liao, and B. Yang, *Image encryption using 2D Hénon-Sine map and DNA approach*. Signal Processing, 2018. **153**: p. 11-23.
- [10] Chai, X., et al., *A color image cryptosystem based on dynamic DNA encryption and chaos*. Signal Processing, 2019. **155**: p. 44-62.
- [11] Huo, D., et al., *Image encryption using exclusive-OR with DNA complementary rules and double random phase encoding*. Physics Letters A, 2019. **383**(9): p. 915-922.
- [12] Enayatifar, R., F.G. Guimarães, and P. Siarry, *Index-based permutation-diffusion in multiple-image encryption using DNA*

- sequence*. Optics and Lasers in Engineering, 2019. **115**: p. 131-140.
- [13] Nematzadeh, H., et al., *Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices*. Optics and Lasers in Engineering, 2018. **110**: p. 24-32.
- [14] Mirzaei Talarposhti, K. and M. Khaki Jamei, *A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map*. Optics and Lasers in Engineering, 2016. **81**: p. 21-34.
- [15] Abdullah, A.H., R. Enayatifar, and M. Lee, *A hybrid genetic algorithm and chaotic function model for image encryption*. AEU - International Journal of Electronics and Communications, 2012. **66**(10): p. 806-816.
- [16] Enayatifar, R., et al., *Image encryption using a synchronous permutation-diffusion technique*. Optics and Lasers in Engineering, 2017. **90**: p. 146-154.
- [17] Enayatifar, R., A.H. Abdullah, and I.F. Isnin, *Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence*. Optics and Lasers in Engineering, 2014. **56**: p. 83-93.
- [18] Pujari, S.K., G. Bhattacharjee, and S. Bhoi, *A Hybridized Model for Image Encryption through Genetic Algorithm and DNA Sequence*. Procedia Computer Science, 2018. **125**: p. 165-171.
- [19] Li, M., D. Lei, and J. Cai, *Two-level imperialist competitive algorithm for energy-efficient hybrid flow shop scheduling problem with relative importance of objectives*. Swarm and Evolutionary Computation, 2019. **49**: p. 34-43.
- [20] Rabiee, A., M. Sadeghi, and J. Aghaei, *Modified imperialist competitive algorithm for environmental constrained energy management of microgrids*. Journal of Cleaner Production, 2018. **202**: p. 273-292.
- [21] Al Dossary, M.A. and H. Nasrabadi, *Well placement optimization using imperialist competitive algorithm*. Journal of Petroleum Science and Engineering, 2016. **147**: p. 237-248.
- [22] Kaur, M. and V. Kumar, *Adaptive Differential Evolution-Based Lorenz Chaotic System for Image Encryption*. Arabian Journal for Science and Engineering, 2018. **43**(12): p. 8127-8144.
- [23] Enayatifar, R., A.H. Abdullah, and M. Lee, *A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption*. Optics and Lasers in Engineering, 2013. **51**(9): p. 1066-1077.