



An Evolutionary Quantum Scrambling Scheme for Medical Image with NEQR Representation

Yasameen K. Hamad¹, Ahmed Y. Yousuf² and Tayseer S. Atia¹

¹Computer Engineering Department , College of Engineering, AL Iraqia University, Baghdad, Iraq

²Computer Technology Engineering, Al Mustafa university College, Baghdad, Iraq

Received 13 Sep. 2022, Revised 6 May. 2023, Accepted 14 May. 2023, Published 30 May. 2023

Abstract: Image scrambling methods are necessary for original image processes in applications of quantum image processing like quantum image encryption, which increases the strength of the encryption process, and the resulting image is difficult to identify and detect its details. As well as obtain a high entropy value and a histogram with a uniform peak for the encrypted image. Most researches focus on scrambling the position only or the value only; however, the quantum image scrambling researches focused on scrambling both position and value together is few. The idea of the study is developing a genetic algorithm to generate different schemes of scrambling based on the fast and elementary schemes with changing the quantum logical gate (NOT / C-Not) to get the best scheme that meets the requirements such as the cost, the complexity or the type of the image. One of the essential benefits of the proposed work is developing a general framework for the automatic generation of a suitable scrambling scheme based on image type, method, and logical circuit. The tests are simulated using MATLAB. The result confirms that hybrid value/position schemes with a C-Not gate have an entropy value close to 8 and a flat histogram. It is implicated that this framework will benefit many researchers in selecting the most appropriate scrambling method for their works.

Keywords: Genetic algorithm, Medical image, NEQR, Quantum, Scrambling.

1. INTRODUCTION

There has been much interest in quantum image processing (QIP) in recent years, from quantum image representation to encrypting the quantum image (QI) [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13]. Image scrambling (IS) Image scrambling [14], [15], [16] is an essential work of image encryption. After scrambling, the image eliminates the correlation of image pixels, causing the image to lose its original information. As a result, an attacker will almost be unable to obtain the original image information, even if he manages to extract information from the image. There are primarily two types of scrambling algorithms; first, change the position of pixels in image: Its concept applies the principles of geometric features to modify the pixel's geometry in order to corrupt an original image's data. Generally, methods depending on this concept include Arnold transform [17], the orthogonal Latin square transformation [18], the affine transform [19], and other methods such as [20], [21], [22], [23], [24], [25], second, change the pixel value of an image: the concept is adjusting the pixel's gray value using particular methods. Its principle is to modify a gray level histogram of an original image so an unauthorized user can not extract informations about the original image from the histogram of the scrambled image.

However, quantum image scrambling (QIS) is still uncommon in quantum studies; some research on this topic includes the following: quantum realization of Fibonacci and Arnold [25]. Recently suggested Quantum Hilbert scrambling [26]. Nevertheless, all of these methods are depending on change the position of pixels in image. Furthermore, when the size of QI grows more significant, the circuit cost increases dramatically. In addition, the size of the QI that may be scrambled in the schemes is limited, and just the square image can be scrambled. It is clear that the efficiency of these methods varies according to the construction gates, type of representation such as novel enhanced quantum image representation (NEQR), bit-plane, or others. Moreover, they are working for only one image type.

Depending on these limitations, this study aims to propose an evolutionary algorithm for generating and optimizing scrambling method of quantum medical images thus produces the required scheme based on a predetermined condition. The importance of the current research lies in developing a general framework for automatically constructing a suitable scrambling scheme based on image type, scheme, and a logical circuit.

Objectives of the proposed search are as follows:

- 1) Investigate value and position for scrambling images based on elementary and fast.
- 2) Develop a genetic algorithm (GA) to generate different scrambling schemes based on elementary and fast schemes, the GA encode the scheme type, quantum gate as a field length chromosome length, then select the parent with tournament selection to mate them with single-point crossover finally mutate offspring and evaluate fitness.
- 3) Evaluate the proposed method's efficiency using evaluation metrics and compare it to related works.

The remains of this study are separated into the following sections: Section 2 presents related works. Section 3 discusses the background of quantum image representation, circuit design, genetic algorithm, and evaluation measurement. Section 4 offers the proposed method. Sections 5 and 6 contain the experimental results and discussion, respectively. Finally, the conclusion is documented in Section 7.

2. RELATED WORKS

The scrambling technique is a necessary process, and researchers use it to increase the randomness of the image. The factors that manage it are the cost needed to design the circuits relative to the resulting randomness. On this basis, researchers design different methods. The researches in this field: Yucheng et al. [27] to encrypt medical images, they implemented a high-speed scrambling and adaptive pixel diffusion algorithm, Shuliang Sun [28] suggested an image encryption scheme in which pixels and bits were scrambled using a chaotic map, Wang et al. [29] presented a method for encrypting images that employed Hash table structure scrambling and DNA sequence operations, Ramasamy et al. [30] suggested an improved logistic chaotic map and implemented the block scrambling with zigzag transformation for pixel confusion, Nan Jiang et al. [26] suggested a Hilbert IS algorithm, a modified recursive generation algorithm of the Hilbert scanning matrix is provided. And depending on the flexible representation of quantum images (FRQI), the Hilbert scrambling quantum circuits, which are recursive and progressively layered, are suggested. However, the efficiency of the method was unmeasured using efficiency measurement methods such as entropy, and the FRQI representation method was used, which uses one qubit to describe the colour information of pixels, while the NEQR use 2p qubits to describe the intensity of 2p-bit pixels. Nan Jiang and Luo Wang [31] investigated the Arnold QIS suggested by Jiang et al. [25]. It aims to accomplish Fibonacci and Arnold IS in a quantum-computer. Since the algorithm unperceived the specificities of "mod 2n", "multiply 2", and in binary arithmetic the subtraction. A probable simplified version is displayed depending on three theorems and a corollary representing the specificities of binary arithmetic. Yet, the method's efficiency was unmeasured using efficiency measurement methods such as entropy and histogram and also used FRQI. To cover the problem of

image representation, using FRQI Ri-Gui Zhou et al. [32], a QIS scheme based on gray code and bit-plane (GB), a whole colour value scrambling technique, is suggested. Using GB knowledge, several quantum scrambling schemes are proposed depending on the strength of NEQR. Similar to [31], the efficiency of the schemes was measured using a histogram only; also, the uniform peak was unreachd. Many other researches such as [33], [34], [35].

3. BACKGROUND

A. Quantum Representation for Gray-Scale Image

This works use NEQR [2] since suitable for QIP, and their quantum colour coding is quite similar to that in classical images [36]. It holds the colour and position information for each pixel. Mathematical model for $(2n \times 2n)$ image is :

$$|I\rangle = \frac{1}{2^n} \sum_{i=0}^{2^n-1} |c_i\rangle \otimes |i\rangle \quad (1)$$

In (1) $|c_i\rangle = |c_i^{q-1}, \dots, c_i^1 c_i^0\rangle$, $c_i^k \in \{0, 1\}$, $k = 0, 1, \dots, q-1$, $i = 0, 1, \dots, 2^{2n} - 1$. The sequence $c_i^{q-1} \dots c_i^1 c_i^0$ encodes the colour value with 2^q colour range, $|i\rangle$ for $i = 0, 1, \dots, 2^{2n} - 1$ with dimension computational basis 2^{2n} . The two parts In NEQR the two parts encode the value and corresponding positions. Figure 1 shows an example of 2×2 NEQR image:

0	100
200	255

$$\begin{aligned} |I\rangle &= \frac{1}{2} (|0\rangle \otimes |00\rangle + |100\rangle \otimes |01\rangle + |200\rangle \otimes |10\rangle \\ &\quad + |255\rangle \otimes |11\rangle) \\ &= \frac{1}{2} (|00000000\rangle \otimes |00\rangle + |01100100\rangle \otimes |01\rangle \\ &\quad + |11001000\rangle \otimes |10\rangle + |11111111\rangle \otimes |11\rangle) \end{aligned}$$

Figure 1. (2×2) image and its representation in NEQR [32].

B. Circuit design

The NOT and C-NOT quantum gates will be used, the notation of the used quantum gates is shown in Figure 2.

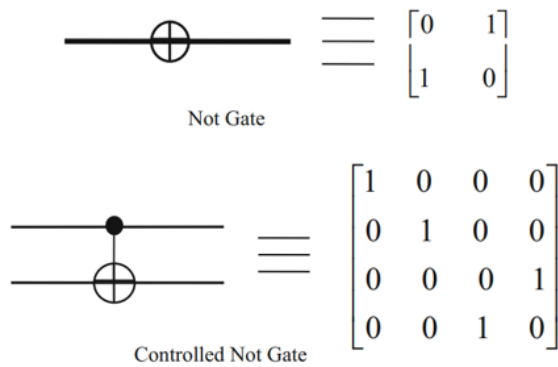


Figure 2. Quantum gates[32].

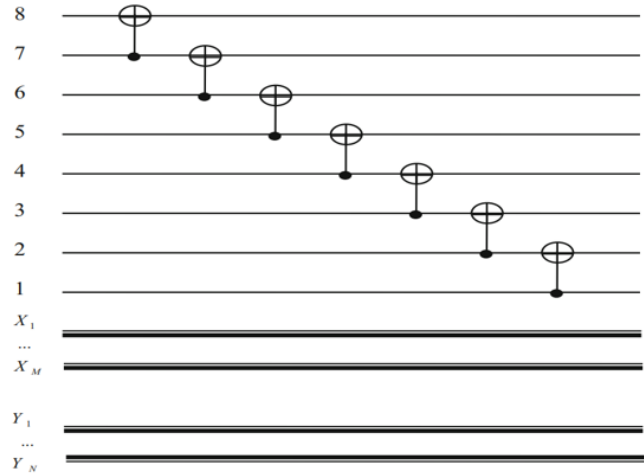


Figure 3. Circuit of EGB-scrambling [32].

1) Scrambling algorithm and circuit

In a QI, the gray information scrambling of pixels can be represented as:

$$\begin{aligned}
 Scr(|I\rangle) &= \frac{1}{2^n} \sum_{X=0}^{2^M-1} \sum_{Y=0}^{2^N-1} Scr(|f(X, Y)\rangle|XY) \\
 &= \frac{1}{2^n} \sum_{X=0}^{2^M-1} \sum_{Y=0}^{2^N-1} |g(X, Y)\rangle|XY)
 \end{aligned}
 \tag{2}$$

Scr in (2) denotes the operation of scrambling, and $g(X, Y)$ represents the image's grayscale value of the scrambled image.

1) Elementary Gray-code and bit-plane (EGB):

First, image bit-planes are listed in primary order. Regarding an information rule, the highest bit-plane holds the majority information of the grayscale, whilst the lowest holds less information. EGB schemes applies the transformation of Gray-code in reverse order. EGB-scrambling function is described as:

$$\begin{aligned}
 EGB(|I\rangle) &= \frac{1}{2^n} \sum_{X=0}^{2^M-1} \sum_{Y=0}^{2^N-1} EGB(|f(X, Y)\rangle|XY) \\
 &= \frac{1}{2^n} \sum_{X=0}^{2^M-1} \sum_{Y=0}^{2^N-1} |g(X, Y)\rangle|XY)
 \end{aligned}
 \tag{3}$$

EGB in (3) refers to an operation of EGB. The quantum circuit of the method is shown in Figure 3.

2) Improved fast GB-scrambling:

This method is proposed to increase scrambling speed while lowering the cost of quantum gates used. It does not require iterative or repetitive scrambling operations. In this method, the bit-plane is unarranged in a positive sequence; rather, the appropriate combination and permutation of bit-planes are selected for fast scrambling. Depending on the information rule of bit-plane, the scheme works on the lowest bit-planes and then implements the outcome to the highest planes to dramatically change the original image. Figure 4 shows that the bit-planes '8 with 4', '7 with 3', '6 with 2', and '5 with 1' perform the C-NOT operations. After that, likewise, the bit-planes '4 with 5', '3 with 6', '2 with 7', and '1 with 8' all performed the C-NOT operations.

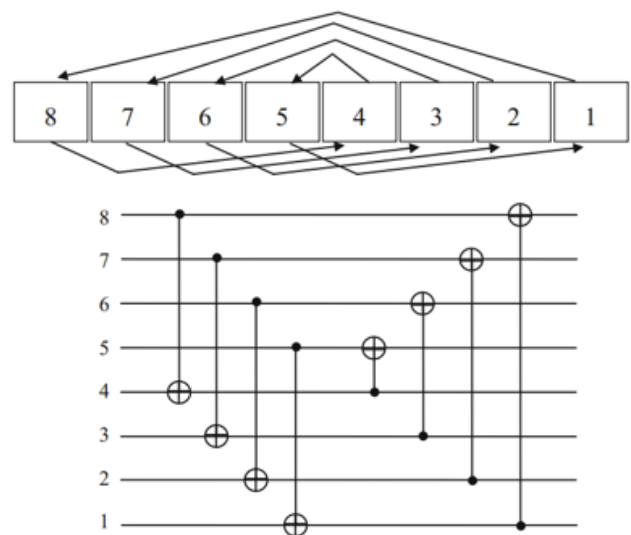


Figure 4. Bit-plane arrangement and its circuit [32].

3) **GB-scrambling combines with position information:**

There are a few IS methods depending on position and value space in the traditional IS processing. Moreover, the extremely high computational cost. Nevertheless, in QIP, scrambling for the QI becomes relatively easy because of the FRQI and the properties of the qubit. As a result, in QIP the construction of algorithms for IS with position has immense potential. This scheme is entirely dependent on GB-scrambling, which implemented for every qubit, including the qubits representing position and gray-scale information. The GB-scrambled position function is the following:

$$\begin{aligned}
 ECB(|I\rangle) &= \frac{1}{2^n} \sum_{X=0}^{2^M-1} \sum_{Y=0}^{2^N-1} GB(|f(X, Y)\rangle) NOT|XY\rangle \\
 &= \frac{1}{2^n} \sum_{X=0}^{2^M-1} \sum_{Y=0}^{2^N-1} |g(X, Y)\rangle NOT|X\rangle NOT|Y\rangle
 \end{aligned}
 \tag{4}$$

The EGB in (4) denotes implementing the GB-scrambling position scheme. Figure 5 shows an example of the quantum circuit.

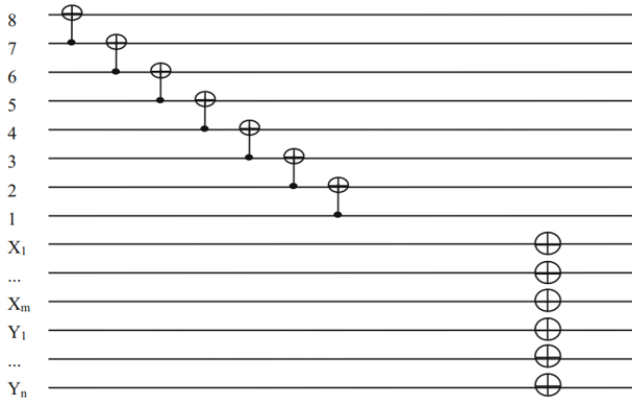


Figure 5. GB-scrambling circuit with the entire position [32].

C. Genetic algorithm

GAs are one of the most well-known natural-inspired algorithms. GAs have been successfully used in various fields, including optimization, pattern recognition, and image processing [37]. GAs address optimization issues using a set of bioinspired operators like a selection, crossover, and mutation to simulate biological evolution [38], [39]. In general, a GA operates as follows:

Step 1/ Create a population of individuals, every representing a potential solution to the problem based on the encoding approach used.

Step 2/ Evaluate every individual's fitness in the population depending on the encoded information.

Step 3/ Select prospective parent individuals from the existing population using tournament selection, crossover,

and mutation operators to generate offspring.

Step 4/ Use a single point crossover operator for the exchange process between two chromosomes to produce new individuals.

Step 5/ Assessing the fitness of the produced offspring.

Step 6/ Change the chromosome if not effective.

Step 7/ Update a random individual with a new value .

Step 8/ Delete a specific individual to cover all possibilities if solutions were ignored in the crossover process.

D. Evaluation measurement

1) entropy analysis

It is a statistical measurement of the distribution of image pixels at every level. It is a vital indicator to evaluate the randomness of the image. The following equation can be used to calculate an image's information entropy:

$$Entropy = - \sum_{i=1}^{2^L-1} p(ui) \log_2(p(ui))
 \tag{5}$$

In (5) $p(ui)$ denotes the probability of ui . There possible values for the gray-scale images are 2^8 (0,255). Perfect entropy value is (8-bit). Therefore, the entropy value of the scrambled image must be close to 8 for 256 gray-scale images to verify the efficiency of the suggested algorithm.

2) Histogram analysis

Histogram is a crucial statistical analytic tool for evaluating the IS scheme's performance, reflecting the frequency distribution of image pixels. It can be used to calculate the statistical similarity between the original and scrambled images. At every intensity level the number of pixels is plotted on a histogram to show how pixels distributed in the image. The effective scrambling schemes can enhance resistance against statistical cryptanalysis by guaranteeing a uniform peak for scrambled images.

4. PROPOSED METHOD

This section discusses the suggested algorithm and its primary components in depth.

A. Algorithm Overview

Algorithm (Genetic algorithm) shows the proposed scrambling scheme, divided into three sections. Firstly, the population is given a predetermined size of S and is randomly initialized (step 1). After that, the individuals' fitness is evaluated (step 2). Then, with the maximum generation number of P (steps 3 to 14), the individuals in the population participate in the evolutionary process of GA. Finally, the best Scrambling scheme is chosen from the end population's finest individual depending on fitness (step 15). An empty population is created to include offspring during the evolutionary process (step 5). After that, a new offspring is produced from chosen parents via crossover and mutation operations. On the other hand, the parents are chosen using a binary tournament selection (steps 6 to 10). After the evaluation fitness of generated offspring (step



11), the environmental selection operation (step 12) is used to produce a new population from the present population (includes the existing individuals as well as the offspring generated) as the parent solutions survive into the following evolutionary process (next generation). The symbol $|\cdot|$ in (step 6) represent a cardinality operator. The stages of “initialization of the population”, “evaluation of fitness”, and “generation of the offspring”, are presented in B, C, D, respectively.

Algorithm 1 (Genetic algorithm)

Input The size of population S , the number of maximal generation P , and the probability of crossover K , the probability of mutation J .

Outcome Best Scrambling scheme.

- 1: $P_0 \leftarrow$ Size S is used to initiate a population.
- 2: in P_0 , Evaluate individual’s fitness;
- 3: $b \leftarrow 0$;
- 4: **while** $b < P$ **do**
- 5: $P_s \leftarrow \phi$;
- 6: **for** $i = 1$ to S **do**
- 7: $p_1, p_2 \leftarrow$ by using binary tournament selection, select two parent individuals from P_b ;
- 8: $q_1, q_2 \leftarrow$ using crossover operation with K and mutation operation with J , generate two offspring by p_1 and p_2 ;
- 9: $P_s \leftarrow P_s \cup q_1 \cup q_2$;
- 10: **Next**
- 11: in P_s , evaluate the individuals’ fitness;
- 12: $P_{b+1} \leftarrow$ from $P_b \cup P_s$, by using environmental selection, select S individuals;
- 13: $b \leftarrow (b + 1)$;
- 14: **end**
- 15: Choose a finest individual from P_b then assign it to an appropriate scrambling scheme.

B. Initialization of the population

For the next evolutionary process, initialization of the population provides a primary population including many individuals. In general, all individuals are initialized at random. In GAs, apiece individual denotes a probable solution to the problem that must be solved. Because GAs are used to find the optimal scrambling scheme in the suggested algorithm, and every individual must represent a scrambling scheme. The initialization is random, and each chromosome is encoded in the form of a character with a fixed length, as shown in Figure 6:

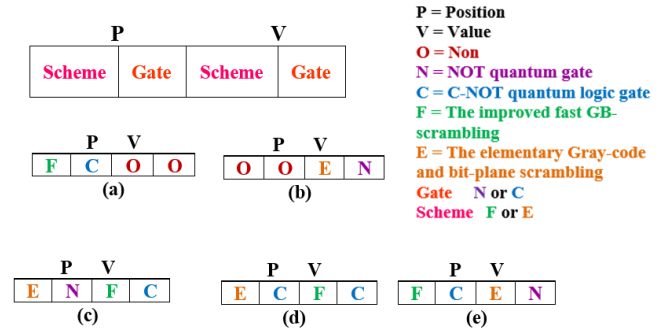


Figure 6. Representation of chromosomes.

as in Figure 6, each chromosome consists of two parts, value and position; each consists of two elements. First represents the gate used; either it is a NOT or a C-NOT. The second is the scheme, whether it is Fast or elementary. There is also the possibility of Non to cover all possible cases, whether scrambling the position only or scrambling the value only. The compensation process is based on these possibilities to get the best scheme for scrambling.

C. Evaluation of fitness

Individual fitness is determined depending on the information encoded by individuals and the task to quantify how well they adapt to the environment. An individual’s fitness in a scrambling scheme is the classification accuracy depending on the individual’s encoding scheme.. According to evolutionary algorithms, the individual with a highest fitness has a highest possibility of producing offspring with higher fitness than themselves. The fitness of individuals is evaluated using entropy. There are several ways to scramble for position and value: the improved fast GB-scrambling and the EGB scrambling using NOT and C-NOT quantum logic gates. Every individual in the scrambling scheme is decoded to evaluate the fitness. Algorithm (Fitness evaluation) shows the fitness evaluation the suggested algorithm. Every individual in the population is evaluated in same way. First, The chromosome-encoded scheme information is converted into the primary individuals with the associated scheme (step 2). Second, the scrambling is initialized with individuals (step 3). Finally, the initialized scrambling is evaluated on the entropy (step 4). The evaluated entropy is considered the individual’s fitness (step 5).

Algorithm 2 (Fitness evaluation)

Input The population A for fitness evaluation, Entropy E, image.

Outcome Population A with fitness.

- 1: **for** every individual in A **do**
- 2: scheme ← decodes information to design the circuit of the corresponding scheme;
- 3: in the input image, apply the scrambling scheme;
- 4: E ← Evaluate the E to output scrambled image;
- 5: assign E and H as the individual's fitness;
- 6: **end**
- 7: **Return** A

D. Generation the offspring

To produce a population of offspring, the parents must be selected beforehand. According to evolutionary algorithms, the produced offspring should have greater fitness than parents by inheriting the quality qualities from the parents. Because of this, individuals with highest level of fitness must be selected as parents. After that, these two parent individuals execute the crossover operation. And each crossover operation generates two offspring. the single-point crossover operator was employed in the suggested algorithm. The crossover operation shows in Figure 7 (crossover operation).

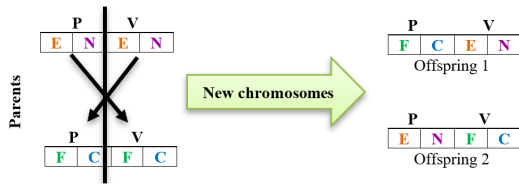


Figure 7. Crossover operation.

Depending on the proposed encoding scheme, the available mutation types are designed. The available mutation types are shown below:

- 1) Flipping (flip the random position if inefficient): Choosing an individual at random and giving it a value, whose results are more effective, for example, replacing the N gate with the C gate, as in Figure 8:

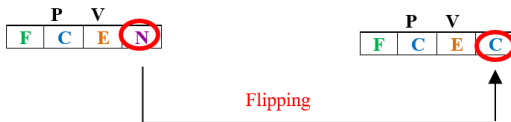


Figure 8. Example of flipping.

- 2) Adding (add a specific individual): Adding a specific value to the chromosome, meaning instead of using only P or V only, a new value is

added to strengthen the scrambling scheme, as in Figure 9:

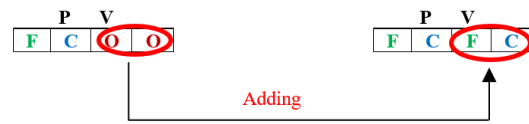


Figure 9. Example of adding.

- 3) Deleting (delete a specific individual to cover all possibilities if there are solutions that were ignored in the crossover process). In the case that there is unscrambled the position only or the value only, the gate and the scheme will be deleted and replaced with O as in Figure 10:

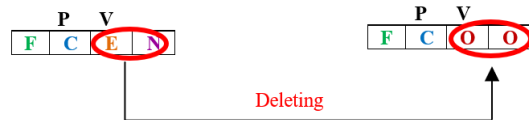


Figure 10. Example of adding.

5. EXPERIMENTAL RESULT

In this section, experiments were conducted to answer the research questions posed in the aim of the research, which is that a scheme can be designed based on either the image type, the logical circuit, or the scheme. For the first question, it depends on the image type. The first group includes Figs. from 12 to 17, where the first image is an image with high details. The second group includes Figs. from 19 to 24, where the group contains an image that has lower details. With these two groups, the question about the image type will be covered. The second question, which is the type of scheme, is answered with Figs. 12 and 19; what is meant by the type of scheme is whether it is scrambling the value only, the position only, or both. The NOT logic gate was used assuming that it is a standard operation and whose style of its work is evident. Figure 14 and Figure 21 answer the last question, which is the type of logical circuit.

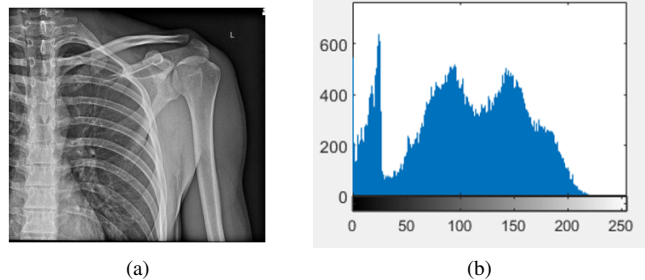


Figure 11. (a) The original image 1 (b) The histogram of (a)

As shown in Figure 11, the original image and its

histogram. The following Figures are the results of different schemes.

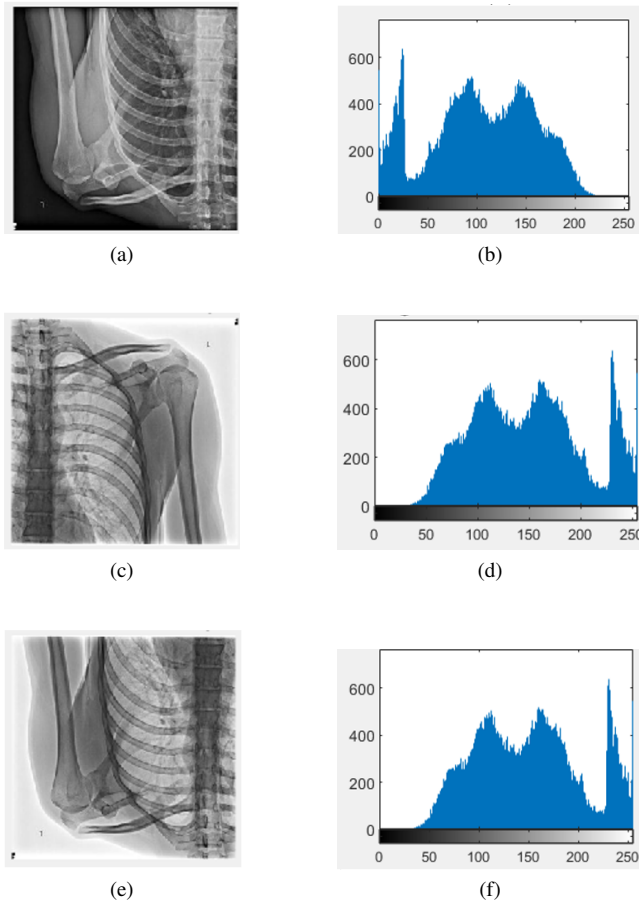


Figure 12. (a) Scrambled image 1 using ENOTP(Proposed), (b) Histogram of (a), (c) Scrambled image 1 using ENOTVP(Proposed), (d) Histogram of (c), (e) Scrambled image 1 using ENOTVP(Proposed), (f) Histogram of (e)

Figure 12 shows the use of the E scheme by the NOT gate, its effect on the histogram was expected, as an insignificant change occurred in (d) and (f), while in (b), the histogram has unchanged, the peak is non-uniform for all schemes.

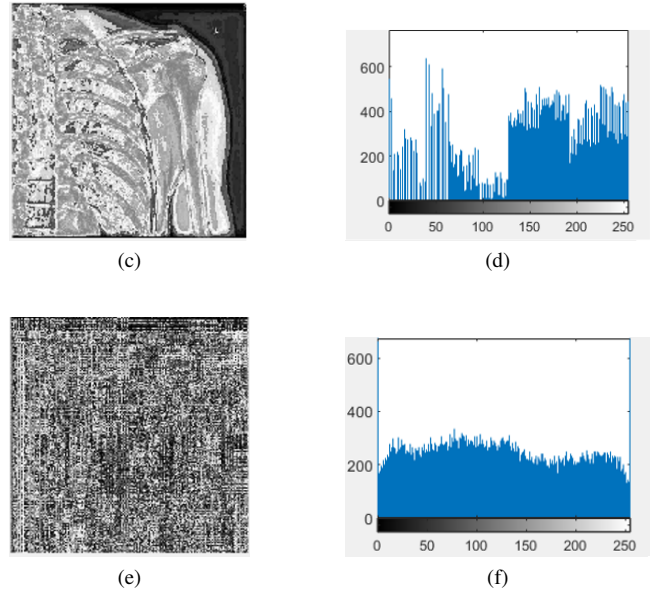
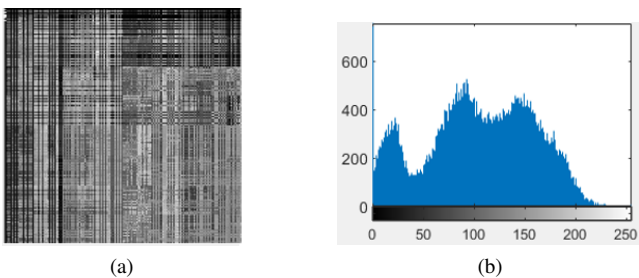


Figure 13. (a) Scrambled image 1 using EC-NOTP(Proposed), (b) Histogram of (a), (c) Scrambled image 1 using EC-NOTV[32], (d) Histogram of (c), (e) Scrambled image 1 using EC-NOTVP(Proposed), (f) Histogram of (e)

Figure 13 presents the results obtained from E C-NOT schemes; what stands out in the Figure is that the best histogram obtained is f, which has an almost uniform peak in contrast to d. the c image is clear and easily distinguished; unlike e, it is unreadable. As for b, there was a slight change in the histogram.

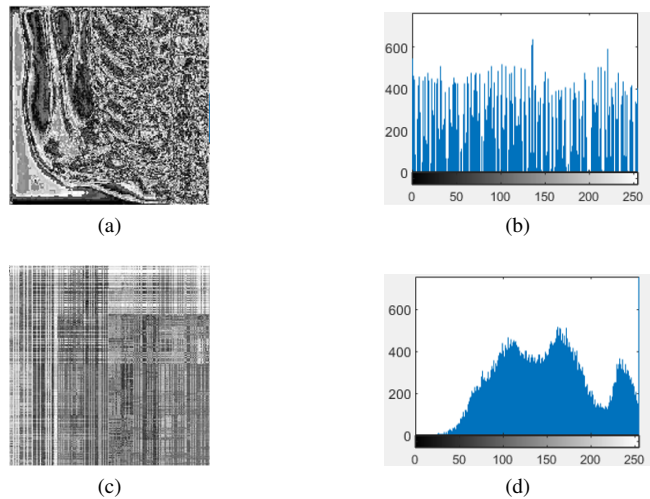


Figure 14. (a) Scrambled image 1 using ENOTP+EC-NOTV [32], (b) Histogram of (a), (c) Scrambled image 1 using EC-NOTP+ENOTVP(Proposed), (d) Histogram of (c)

As shown in Figure 14, in b, the histogram is almost a uniform peak, but image a can easily distinguish contrary to c is hard to distinguish image.

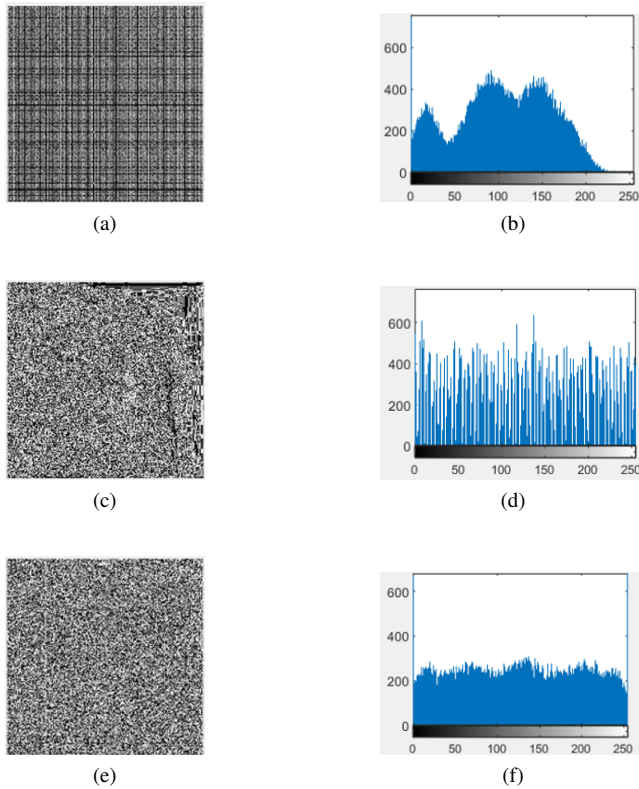


Figure 15. (a) Scrambled image 1 using FC-NOTP (Proposed), (b) Histogram of (a), (c) Scrambled image 1 using FC-NOTV[32], (d) Histogram of (c), (e) Scrambled image 1 using FC-NOTVP (Proposed), (f) Histogram of (e)

A closer inspection of Figure 15 shows the histogram of f is a uniform peak, and the image e is hard to recognize and distinguish, while the histogram of b and d are non-uniform peaks.

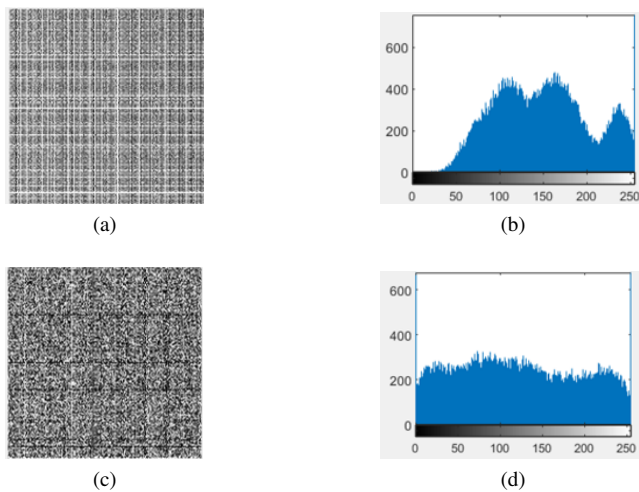


Figure 16. (a) Scrambled image 1 using FC-NOTP+ENOTV (Proposed), (b) Histogram of (a), (c) Scrambled image 1 using FC-NOTP+EC-NOTV (Proposed), (d) Histogram of (c)

It is apparent from Figure 16 that the histogram in d is almost a uniform peak, while the histogram in b was an insignificant change from the original histogram.

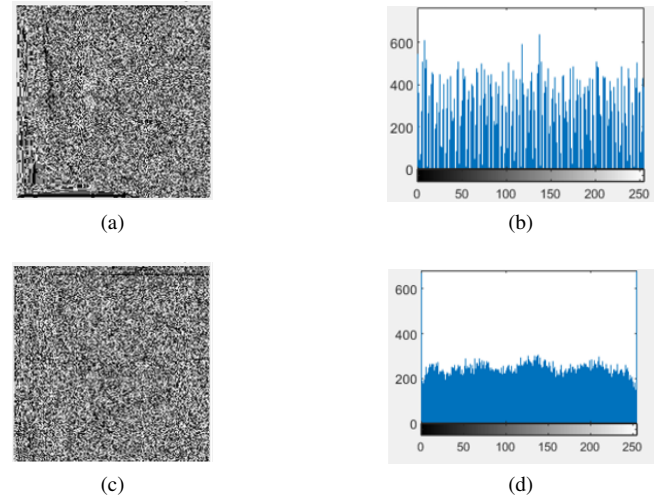


Figure 17. (a) Scrambled image 1 using FC-NOTV+ENOTP (Proposed), (b) Histogram of (a), (c) Scrambled image 1 using FC-NOTV+EC-NOTP (Proposed), (d) Histogram of (c)

A closer inspection of Figure 17 shows the histogram of d is a uniform peak more than in b means that scheme c is better than scheme a.

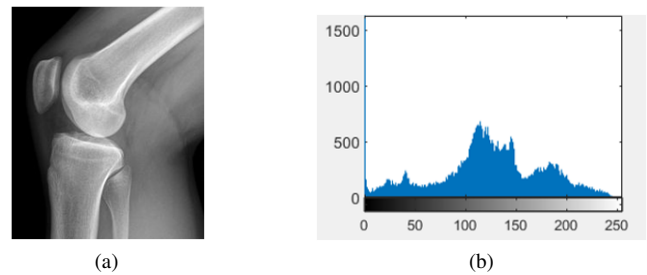
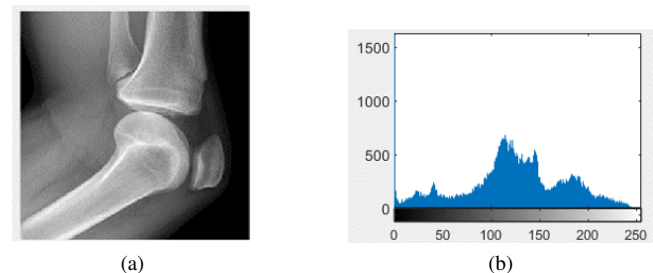


Figure 18. (a) The original image 2, (b) The histogram of (a)

Figure 18 shows the original image 2 and its histogram. The following Figures are the results of different schemes for image 2.



(a) (b)

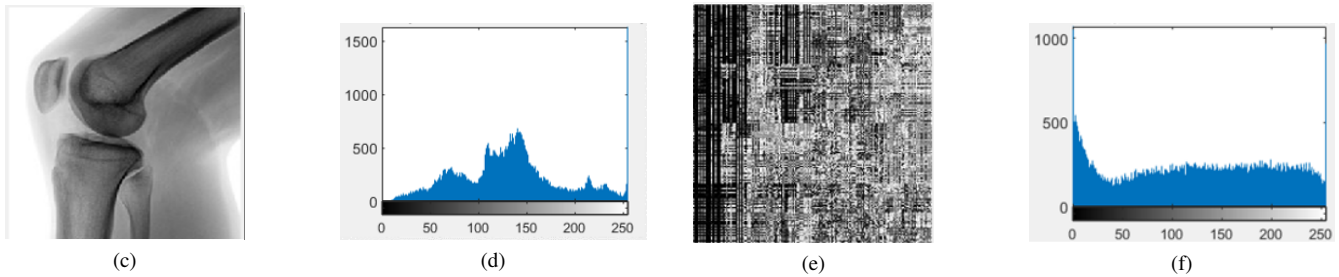


Figure 20. (a) Scrambled image 2 using EC-NOTP (Proposed), (b) Histogram of (a), (c) Scrambled image 2 using EC-NOTV[32], (d) Histogram of (c), (e) Scrambled image 2 using EC-NOTVP (Proposed), (f) Histogram of (e)

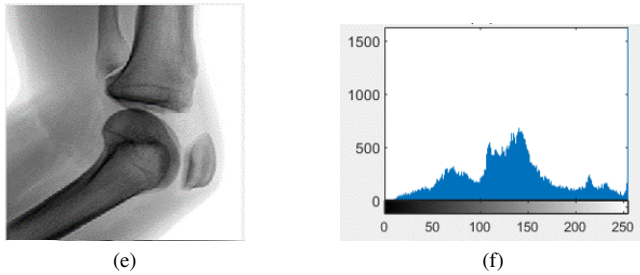


Figure 19. (a) Scrambled image 2 using ENOTP(Proposed), (b) Histogram of (a), (c) Scrambled image 2 using ENOTV(Proposed), (d) Histogram of (c), (e) Scrambled image 2 using ENOTVP(Proposed), (f) Histogram of (e)

Figure 19 shows that the effect of E NOT on the histogram was expected, as an insignificant change occurred in (d) and (f), while in (b), the histogram has unchanged, and the peak is non-uniform for all schemes

Figure 20 presents the results obtained from E C-NOT schemes; what stands out in the Figure is that the best histogram obtained is f, which has an almost uniform peak in contrast to d and b. the c image is clear and easily distinguished; unlike e, it is unreadable. As for b, there was a slight change in the histogram.

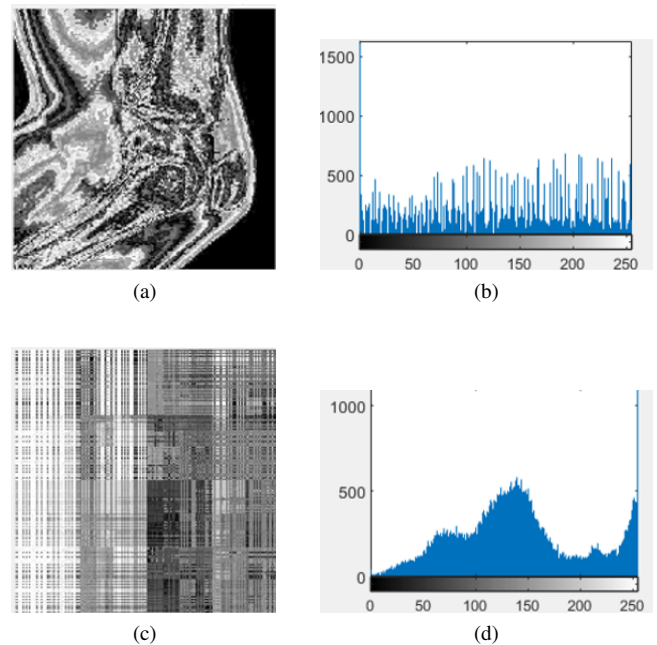
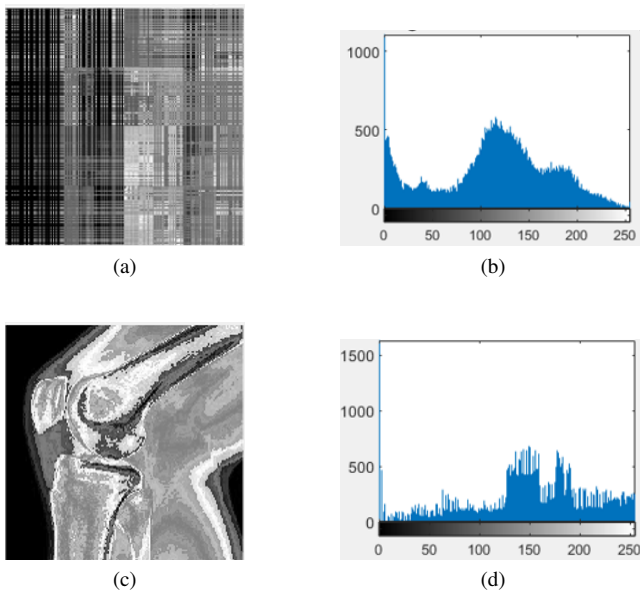


Figure 21. (a) Scrambled image 2 using ENOTP+EC-NOTV [32], (b) Histogram of (a), (c) Scrambled image 2 using EC-NOTP+ENOTV (Proposed), (d) Histogram of (c)

As shown in Figure 21, in b, the histogram is almost a uniform peak, but image a can easily distinguish contrary to c is hard to distinguish image.

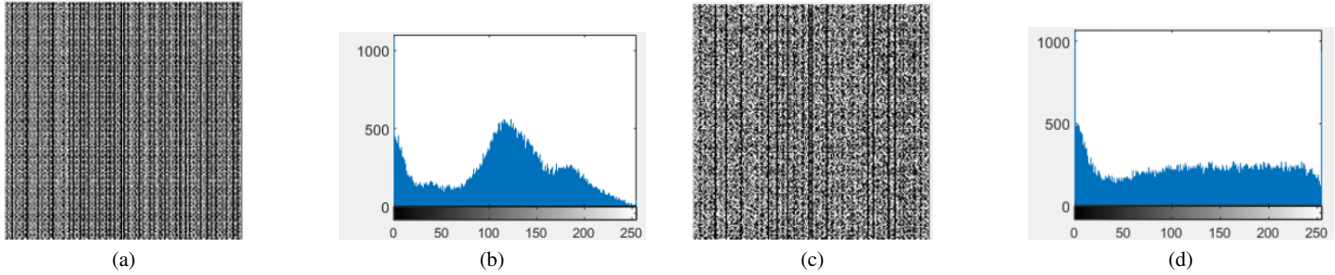


Figure 23. (a) Scrambled image 2 using FC-NOTP+ENOTV (Proposed), (b) Histogram of (a), (c) Scrambled image 2 using FC-NOTP+EC-NOTV (Proposed), (d) Histogram of (c)

It is apparent from Figure 23 that the histogram in d is almost a uniform peak, while the histogram in b was an insignificant change from the original histogram.

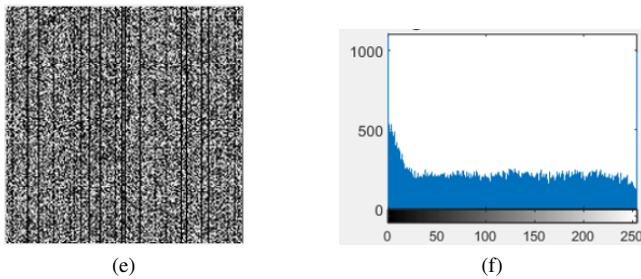
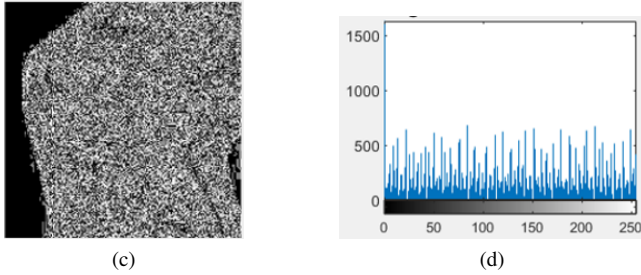


Figure 22. (a) Scrambled image 2 using FC-NOTP(Proposed), (b) Histogram of (a), (c) Scrambled image 2 using FC-NOTV [32], (d) Histogram of (c), (e) Scrambled image 2 using FC-NOTVP (Proposed), (f) Histogram of (e)

A closer inspection of Figure 22 shows the histogram of f is nearly a uniform peak, and the image e is hard to recognize and distinguish, while the histogram of b and d are non-uniform peaks. The image c easy to distinguish.

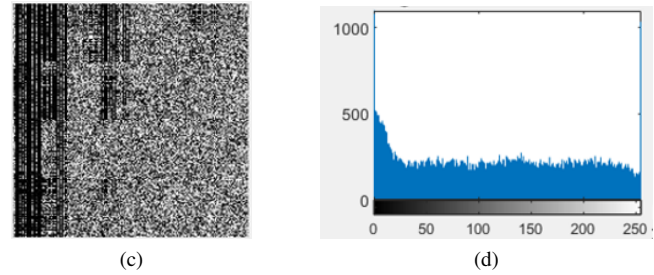
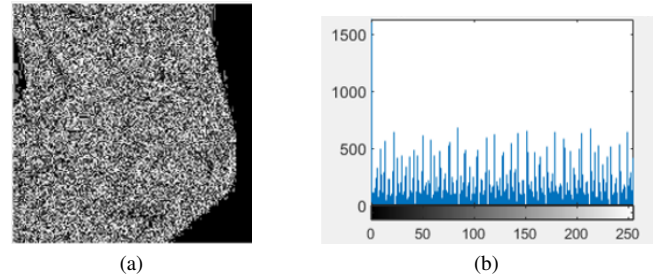
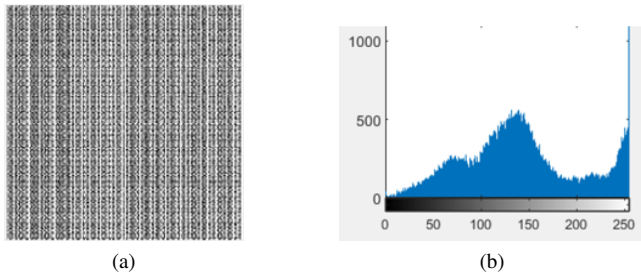


Figure 24. (a) Scrambled image 2 using FC-NOTV+ENOTP (Proposed), (b) Histogram of (a), (c) Scrambled image 2 using FC-NOTV+EC-NOTP (Proposed), (d) Histogram of (c)

A closer inspection of Figure 24 shows the histogram of d is nearly a uniform peak more than in b means that scheme c is better than scheme a.

From Figure 25, further statistical tests show that the scrambling of both position and value using the C-NOT gate in (FC-NOTVP(N), FC-NOTV+EC-NOTP(N), EC-NOTV+FC-NOTP(N), EC-NOTVP(N)) had the highest entropy (close to 8). while no significant differences were found when using each of (EC-NOTV(P), EC-NOTV+ENOTP(P), FC-NOTV(P), ENOTV(N), FC-NOTV+ENOTP(N)), the entropy was unchanged; it is precisely the entropy of the original image, meanwhile, in (ENOTV+EC-NOTP(N), EC-NOTP(N), ENOTV+FC-NOTP(N), FC-NOTP(N)) A slightly higher entropy was



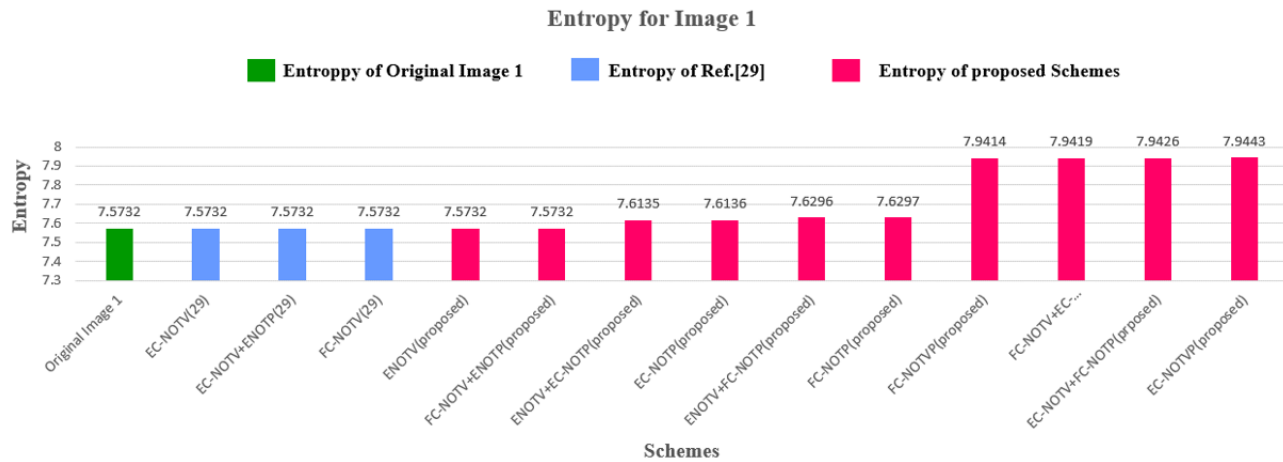


Figure 25. entropy for all schemes of image 1.

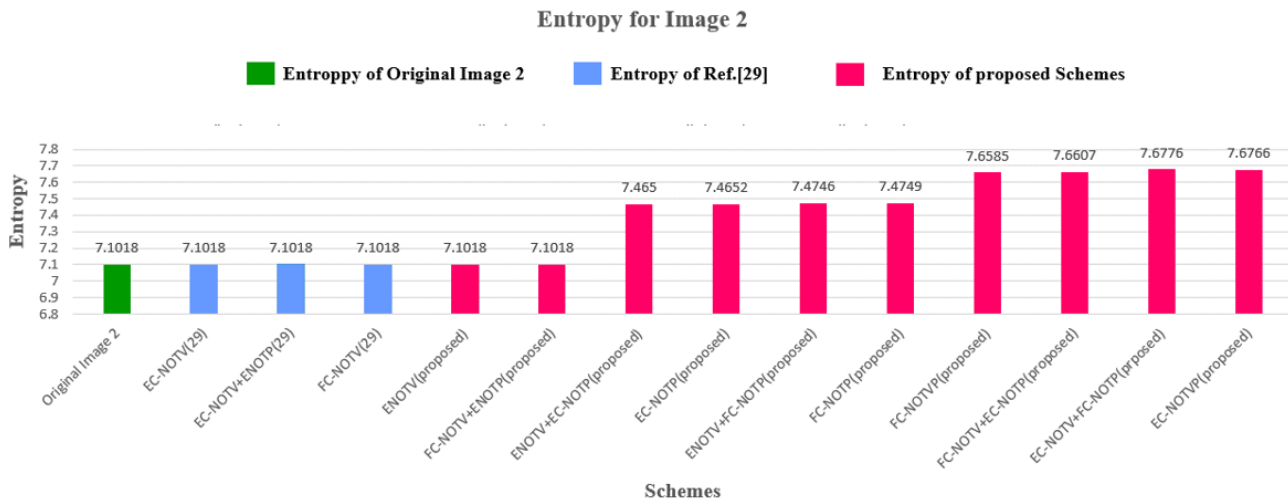


Figure 26. entropy for all schemes of image 2

obtained.


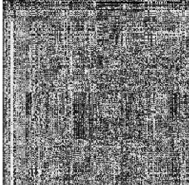

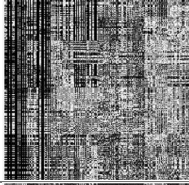

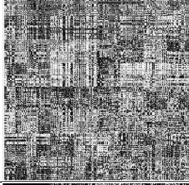

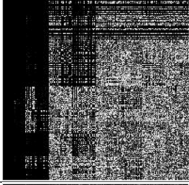
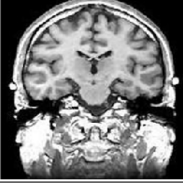
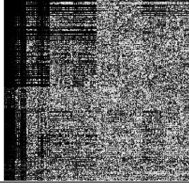
Figure 26 show that the scrambling of both position and value using the C-NOT gate in (FC-NOTVP(N), FC-NOTV+EC-NOTP(N), EC-NOTV+FC-NOTP(N), EC-NOTVP(N)) had the highest entropy (close to 8). At the time that, no significant differences were found when using each of (EC-NOTV(P), EC-NOTV+ENOTP(P), FC-NOTV(P), ENOTV(N), FC-NOTV+ENOTP(N)), the entropy unchanged, it is precisely the entropy of the original image, meanwhile, in (ENOTV+EC-NOTP(N), EC-NOTP(N), ENOTV+FC-NOTP(N), FC-NOTP(N)) A higher entropy was obtained. Based on the results of the genetic algorithm, it was found that the best scrambling scheme is the EGB scrambling using C-Not for both position and value, and it will be applied to a set of different images to see the effectiveness of the method as shown in Table I.

Over the results presented in Table I, we note that the method is effective on different images through the noticeable increase in the value of the entropy and obtaining an entropy close to 8 in some images, as well as observing the scrambling images where they cannot be identified or identify its details.

6. DISCUSSION

- Findings for the first research question in which NOT operation was used in their schemes, shows an expected behavior, and the reason for this is that it is a unary operation, and its work is flipping the values. While Figures in which the C-NOT operation was used their behavior is more potent than the NOT operation because it is a binary operation.
- For the second question, finding that scramble value and position in their schemes are most potent because

TABLE I. Summary of results

Original image	Scrambled image	Original entropy	Scrambled entropy
		7.5732	7.9443
		7.1018	7.6766
		7.7449	7.9506
		5.5396	6.4170
		7.1490	7.4905

they work on two levels. The best uniform peak was obtained when the schemes contained the scrambling of both value and position using the C-NOT logic gate, and the uniform peak is reduced when the NOT logic gate is used.

- As for the third question, image type, the output scrambled image of the image with lower details is incompletely scrambled or incompletely distorted due to the presence of areas in the image being of the same value; therefore, the image after the scrambling still indicates the type of the original image.
- For the entropy, the strength of the schemes depends on the circuit, the scheme, and the type of the image. As shown in Figs. 21 and 22, the first five schemes have low entropy values relative to the rest of the schemes. The highest entropy was obtained for the last four schemes because of the scrambling of both

the position and the value. It was also possible to conclude that each scheme contains a NOT logic gate; its entropy values are lower, which means that the NOT logic gate weakens the scheme in which it is used.

It could be argued that the positive results were due to scrambling position and value together, not separately. It can thus be suggested that the best schemes are (FC-NOTVP(N), FC-NOTV+EC-NOTP(N), EC-NOTV+FC-NOTP(N), EC-NOTVP(N)) in which both position and value are scrambled and use a C-NOT logic gate to obtain a better scrambling, a histogram with a uniform peak, higher entropy, and an indistinguishable image.

7. CONCLUSION

This study set out to design an evolutionary algorithm for generating and optimizing schemes for medical images and produce the required scheme based on predetermined



conditions. The research has also shown that the results with high entropy (approximately 8) and histogram with uniform peak were obtained compared to results in [32]. This research supports the idea that it is possible to automatically develop a general framework for the genetic algorithm to generate a suitable scrambling scheme. This work is the first comprehensive investigation of all possible scrambling position and value cases using NOT and C-NOT gates. These findings will interest many researchers in choosing a suitable scheme for their search through the displayed results. The study should be repeated using other quantum logic gates for other and possibly better results. The proposed algorithm's limitations are that it only works on grayscale images, and in the future it can be developed to work on color images.

REFERENCES

- [1] P. Q. Le, F. Dong, and K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," *Quantum Information Processing*, vol. 10, no. 1, pp. 63–84, 2011.
- [2] Y. Zhang, K. Lu, Y. Gao, and M. Wang, "Neqr: a novel enhanced quantum representation of digital images," *Quantum information processing*, vol. 12, no. 8, pp. 2833–2860, 2013.
- [3] H.-S. Li, Q. Zhu, R.-G. Zhou, L. Song, and X.-j. Yang, "Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state," *Quantum Information Processing*, vol. 13, no. 4, pp. 991–1011, 2014.
- [4] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, "Elementary gates for quantum computation," *Physical review A*, vol. 52, no. 5, p. 3457, 1995.
- [5] P. Q. Le, A. M. Ilyyasu, F. Dong, and K. Hirota, "Efficient color transformations on quantum images," *J. Adv. Comput. Intell. Intell. Informatics*, vol. 15, no. 6, pp. 698–706, 2011.
- [6] C.-Y. Pang, R.-G. Zhou, C.-B. Ding, and B.-Q. Hu, "Quantum search algorithm for set operation," *Quantum information processing*, vol. 12, no. 1, pp. 481–492, 2013.
- [7] A. Fijany and C. P. Williams, "Quantum wavelet transforms: Fast algorithms and complete circuits," in *NASA international conference on quantum computing and quantum communications*. Springer, 1998, pp. 10–33.
- [8] W.-W. Zhang, F. Gao, B. Liu, Q.-Y. Wen, and H. Chen, "A watermark strategy for quantum images based on quantum fourier transform," *Quantum information processing*, vol. 12, no. 2, pp. 793–803, 2013.
- [9] A. M. Ilyyasu, P. Q. Le, F. Dong, and K. Hirota, "Watermarking and authentication of quantum images based on restricted geometric transformations," *Information Sciences*, vol. 186, no. 1, pp. 126–149, 2012.
- [10] R.-G. Zhou, Q. Wu, M.-Q. Zhang, and C.-Y. Shen, "Quantum image encryption and decryption algorithms based on quantum image geometric transformations," *International Journal of Theoretical Physics*, vol. 52, no. 6, pp. 1802–1817, 2013.
- [11] C.-H. Lin, J.-X. Wu, P.-Y. Chen, H.-Y. Lai, C.-M. Li, C.-L. Kuo, and N.-S. Pai, "Intelligent symmetric cryptography with chaotic map and quantum based key generator for medical images infosecurity," *IEEE Access*, vol. 9, pp. 118 624–118 639, 2021.
- [12] T. Janani and M. Brindha, "A secure medical image transmission scheme aided by quantum representation," *Journal of Information Security and Applications*, vol. 59, p. 102832, 2021.
- [13] B. Wang, J. Xu, and H. Song, "Research on the improved algorithm for image quantum encryption in multimedia networks," *Computers & Electrical Engineering*, vol. 62, pp. 414–428, 2017.
- [14] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letters*, vol. 31, no. 5, pp. 347–354, 2010.
- [15] A. L. Abu Dalhoum, B. A. Mahafzah, A. A. Awwad, I. Aldhamari, A. Ortega, M. Alfonseca *et al.*, "Digital image scrambling using 2d cellular automata," *IEEE Multimedia*, 2012.
- [16] H.-S. Li, X. Chen, S. Song, Z. Liao, and J. Fang, "A block-based quantum image scrambling for gneqr," *IEEE Access*, vol. 7, pp. 138 233–138 243, 2019.
- [17] L. Wu, J. Zhang, W. Deng, and D. He, "Arnold transformation algorithm and anti-arnold transformation algorithm," in *2009 first international conference on information science and engineering*. IEEE, 2009, pp. 1164–1167.
- [18] Y. Li, Y. Hao, and C. Wang, "A research on the robust digital watermark of color radar images," in *The 2010 IEEE International Conference on Information and Automation*. IEEE, 2010, pp. 1091–1096.
- [19] A. Nag, J. P. Singh, S. Khan, S. Ghosh, S. Biswas, D. Sarkar, and P. P. Sarkar, "Image encryption using affine transform and xor operation," in *2011 International conference on signal processing, communication, computing and networking technologies*. IEEE, 2011, pp. 309–312.
- [20] L. Zhang, S. Ji, Y. Xie, Q. Yuan, Y. Wan, and G. Bao, "Principle of image encrypting algorithm based on magic cube transformation," in *International Conference on Computational and Information Science*. Springer, 2005, pp. 977–982.
- [21] A. B. Abugharsa, A. S. B. H. Basari, and H. Almangush, "A novel image encryption using an integration technique of blocks rotation based on the magic cube and the aes algorithm," *arXiv preprint arXiv:1209.4777*, 2012.
- [22] J. Delei, B. Sen, and D. Wenming, "An image encryption algorithm based on knight's tour and slip encryption-filter," in *2008 International Conference on Computer Science and Software Engineering*, vol. 1. IEEE, 2008, pp. 251–255.
- [23] J. Zou, R. K. Ward, and D. Qi, "The generalized fibonacci transformations and application to image scrambling," in *2004 IEEE International Conference on Acoustics, Speech, and Signal Processing*, vol. 3. IEEE, 2004, pp. iii–385.
- [24] Y. Zhou, K. Panetta, S. Aгаian, and C. P. Chen, "Image encryption using p-fibonacci transform and decomposition," *Optics Communications*, vol. 285, no. 5, pp. 594–608, 2012.
- [25] N. Jiang, W.-Y. Wu, and L. Wang, "The quantum realization



- of arnold and fibonacci image scrambling,” *Quantum information processing*, vol. 13, no. 5, pp. 1223–1236, 2014.
- [26] N. Jiang, L. Wang, and W.-Y. Wu, “Quantum hilbert image scrambling,” *International Journal of Theoretical Physics*, vol. 53, no. 7, pp. 2463–2484, 2014.
- [27] Y. Chen, C. Tang, and R. Ye, “Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion,” *Signal Processing*, vol. 167, p. 107286, 2020.
- [28] S. Sun, “A novel hyperchaotic image encryption scheme based on dna encoding, pixel-level scrambling and bit-level scrambling,” *IEEE Photonics Journal*, vol. 10, no. 2, pp. 1–14, 2018.
- [29] X. Wang and L. Liu, “Image encryption based on hash table scrambling and dna substitution,” *IEEE Access*, vol. 8, pp. 68 533–68 547, 2020.
- [30] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, “An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—tent map,” *Entropy*, vol. 21, no. 7, p. 656, 2019.
- [31] N. Jiang and L. Wang, “Analysis and improvement of the quantum arnold image scrambling,” *Quantum information processing*, vol. 13, no. 7, pp. 1545–1551, 2014.
- [32] R.-G. Zhou, Y.-J. Sun, and P. Fan, “Quantum image gray-code and bit-plane scrambling,” *Quantum Information Processing*, vol. 14, no. 5, pp. 1717–1734, 2015.
- [33] W.-W. Hu, R.-G. Zhou, J. Luo, S.-X. Jiang, and G.-F. Luo, “Quantum image encryption algorithm based on arnold scrambling and wavelet transforms,” *Quantum Information Processing*, vol. 19, no. 3, pp. 1–29, 2020.
- [34] S. Heidari, M. Vafaei, M. Houshmand, and N. Tabatabaey-Mashadi, “A dual quantum image scrambling method,” *Quantum Information Processing*, vol. 18, no. 1, pp. 1–23, 2019.
- [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. 57 188–57 199, 2019.
- [36] A. A. Abd El-Latif, B. Abd-El-Atty, and M. Talha, “Robust encryption of quantum medical images,” *IEEE Access*, vol. 6, pp. 1073–1081, 2017.
- [37] J. H. Holland, *Adaptation in natural and artificial systems: an introductory analysis with applications to biology, control, and artificial intelligence*. MIT press, 1992.
- [38] M. Mitchell, *An introduction to genetic algorithms*. MIT press, 1998.
- [39] L. M. Schmitt, “Theory of genetic algorithms,” *Theoretical Computer Science*, vol. 259, no. 1-2, pp. 1–61, 2001.



Yasameen K. Hamad is a master degree student at the Computer Engineering Department, College of Engineering, AL Iraqia University, Baghdad, Iraq. Yasameen graduated with a first-class B.Sc. degree in Computer technologies Engineering in 2018. Her research interests are data security, artificial intelligence, and image processing.



Ahmed Y. Yousuf is a Lecturer at the department of computer Technology engineering, Al Mustafa University College, Iraq, where he has been a faculty member since 2012. Tayseer graduated with a first-class B.Sc. degree in computer science in 2003 and a M.Sc. in data security in 2007 from the University of Technology, Iraq. He completed his Ph.D. in computer science from Al Mosul University, Iraq. Her research interests are data security and artificial intelligence, especially mobile agent techniques.



Tayseer S. Atia is a professor at the department of computer engineering, Al Iraqia University, Iraq, where she has been a faculty member since 2012. From 2013-2014 she was the head of the computer engineering department. From 2014-2015 she was the dean’s assistant for scientific affairs. Tayseer graduated with a first-class B.Sc. degree in computer science in 2004 and a M.Sc. in data security in 2007 from the University of Technology, Iraq. She completed her Ph.D. in computer science from Al Mosul University, Iraq. Her research interests are data security and artificial intelligence, especially computational intelligence techniques.