IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 10, 2021, accepted February 26, 2021, date of publication March 2, 2021, date of current version March 11, 2021.

*Digital Object Identifier 10.1109/ACCESS.2021.3063237*

# A New Image Encryption Algorithm for Grey and Color Medical Images

**SARA T. KAMAL[1], KHALID M. HOSNY[2], (Senior Member, IEEE), TAHA M. ELGINDY[3], MOHAMED M. DARWISH[1], AND MOSTAFA M. FOUDA[4], (Senior Member, IEEE)**

[1]Department of Computer Sciences, Assiut University, Assiut 71516, Egypt
[2]Department of Information Technology, Zagazig University, Zagazig 44519, Egypt
[3]Department of Mathematics, Assiut University, Assiut 71516, Egypt
[4]Department of Electrical and Computer Engineering, Idaho State University, Pocatello, ID 83209, USA

Corresponding author: Khalid M. Hosny (k_hosny@yahoo.com)

**ABSTRACT** Recently, diagnosing diseases using medical images became crucial. As these images are transmitted through the network, they need a high level of protection. If the data in these images are liable for unauthorized usage, this may lead to severe problems. There are different methods for securing images. One of the most efficient techniques for securing medical images is encryption. Confusion and diffusion are the two main steps used in encryption algorithms. This paper presents a new encryption algorithm for encrypting both grey and color medical images. A new image splitting technique based on image blocks introduced. Then, the image blocks scrambled using a zigzag pattern, rotation, and random permutation. Then, a chaotic logistic map generates a key to diffuse the scrambled image. The efficiency of our proposed method in encrypting medical images is evaluated using security analysis and time complexity. The security is tested in entropy, histogram differential attacks, correlation coefficient, PSNR, keyspace, and sensitivity. The achieved results show a high-performance security level reached by successful encryption of both grey and color medical images. A comparison with various encryption methods is performed. The proposed encryption algorithm outperformed the recent existing encryption methods in encrypting medical images.

**INDEX TERMS** Image encryption, chaotic logistic map, color medical images, image blocks scrambling.

## I. INTRODUCTION

With the rapid development in medical device technology, it became common to diagnose various diseases using medical images. Medical images are transmitted through different networks; therefore, securing these images became an essential topic in recent years. Safe transmission of medical images requires confidentiality, integrity, and authentication. Unauthorized usage of such images may lead to loss of privacy of patients' data. Moreover, when these images are liable for any little change, it may result in an incorrect diagnosis that could threaten patients' lives.

Generally, securing digital images could be achieved by using image steganography [1], [2], image watermarking [3]–[5], and image encryption [6]–[8]. Encryption is the most straightforward and most efficient method to ensure medical image security via converting the plain image into an unreadable one using a secret key. Without having that secret key, nobody can restore the plain image. Image encryption depends on two major operations: confusion and diffusion.

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

Due to the strong correlation between the image-pixels, big-size images, and data redundancy, traditional encryption algorithms are not suitable for digital images, especially medical images. Many medical image encryption algorithms [9]–[13] were proposed to reduce correlation and redundancy. In [14], Singh *et al.* presented a medical image encryption algorithm based on an improved ElGamal encryption scheme version. The problem of data expansion is resolved, and the execution speed is improved. Hua *et al.* [15] proposed a new medical image encryption algorithm consisting of random data insertion, high-speed scrambling, and pixel adaptive diffusion. In [16], Chen *et al.* proposed a generalized optical encryption framework based on Shearlets and double random phase encoding (DRPE) for encrypting medical images. Cao *et al.* [17] presented a medical image encryption algorithm using edge maps. The algorithm based on three main parts: bit-plane decomposition, generating a random sequence, and permutation.

Different algorithms for securing medical images are introduced, yet they may be liable to attacks. A strong correlation between neighboring pixels characterizes medical images; thus, removing this correlation requires a

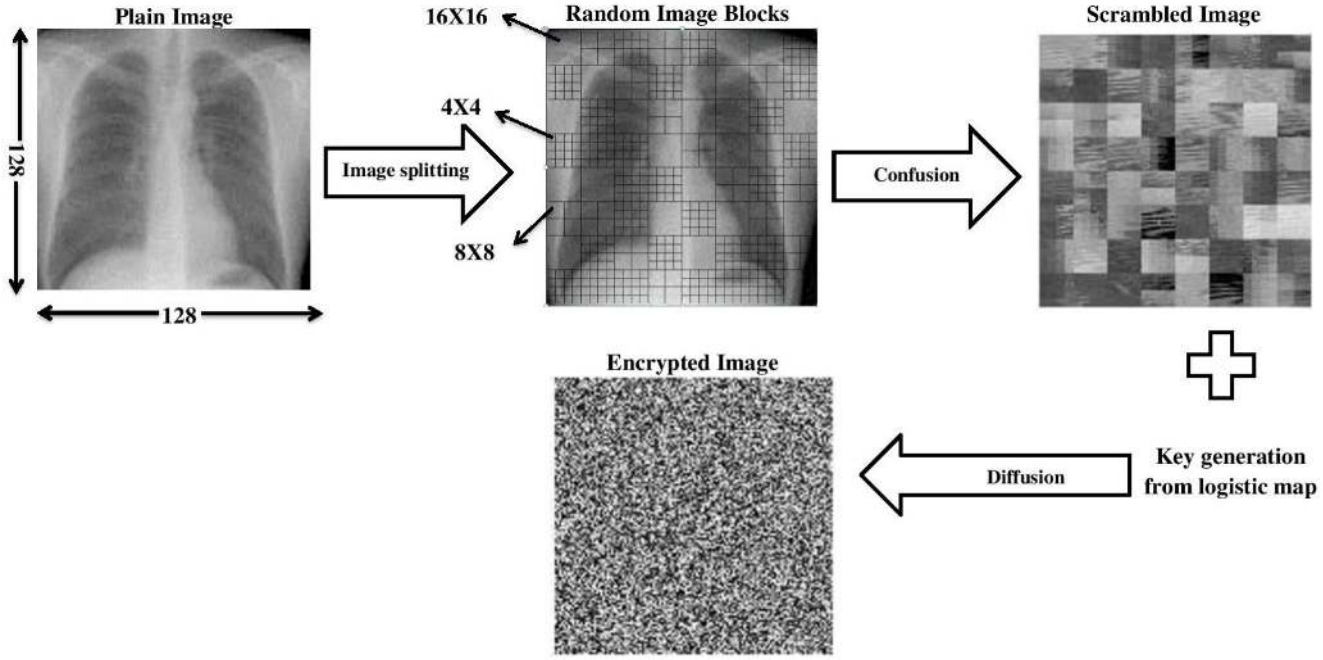


**FIGURE 1.** Medical image encryption block diagram.

permutation (scrambling) technique with a higher security level. This paper presents a new algorithm for encrypting medical images that include four parts: image splitting, image scrambling, key generation, and diffusion. First, the plain image is divided into blocks and sub-blocks using a new image splitting technique. Second, the pixels' arrangement is changed in the blocks and sub-blocks using a zigzag pattern, rotation at a 90-degree angle, and random permutation between blocks. Third, a key is generated from the logistic map, where the map's initial condition depends on the plain image. Finally, image pixel values are changed using the secret key.

The contributions of this paper are summarized by:

1. A new technique for image splitting is proposed.
2. Random permutation between blocks is applied, and pixels substitution in each block is performed to remove the correlation between pixels.
3. A logistic map is used to diffuse the scrambled image, where the map's initial condition is based on the plain image. Therefore, the proposed algorithm is robust against differential attacks.
4. Analysis of the results proves that our algorithm gains a high performance in encrypting medical images than other methods.

This paper aims to:

1. Achieve a high level of security.
2. Propose a block and sub-block image to accelerate the entire encryption process essential in securing medical images through their transmission via IoT (Internet of Things) devices for healthcare and telemedicine systems.

The remainder of this paper is organized as follows. Section 2 discusses the proposed method in detail. Section 3 demonstrates the simulation results and analyses. Finally, the paper is concluded in section 4.

## II. THE PROPOSED METHOD

This section describes the proposed algorithm's main steps for securing medical images in detail. In the first step, the plain image is encrypted and converted into an unreadable image. Then, to recover the plain image, we apply the decryption step.

### A. ENCRYPTION

Here, our algorithm for encrypting medical images consists of four stages. In the first stage, we perform image splitting. Confusion (scrambling) is performed in the second stage. The third stage presents key generation based on a logistic map. The final stage presents the diffusion process. An illustrative diagram of medical image encryption is shown in Figure 1.

#### 1) PLAIN IMAGE SPLITTING

The plain image is divided into non-overlapping blocks of the same size. Our algorithm is appropriate for different block sizes (i.e., 16, 32, and 64), and the user can select the block size. Then, each block is either sub-divided into sub-blocks with equal sizes or remains without splitting. The sub-blocks in each block are chosen depending on a random number generated for each block.

#### 2) CONFUSION

Confusion is the process of changing pixels' arrangement in the image. In our algorithm, confusion is performed for blocks and sub-blocks as follows:

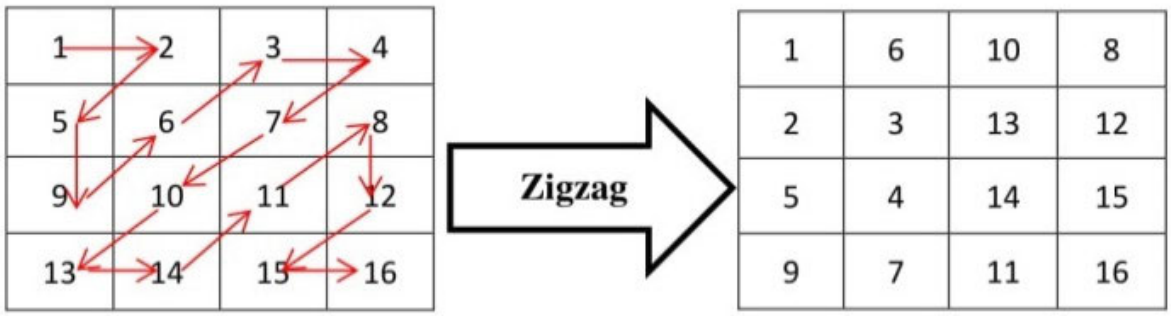


**FIGURE 2.** Demonstration of the zigzag pattern.

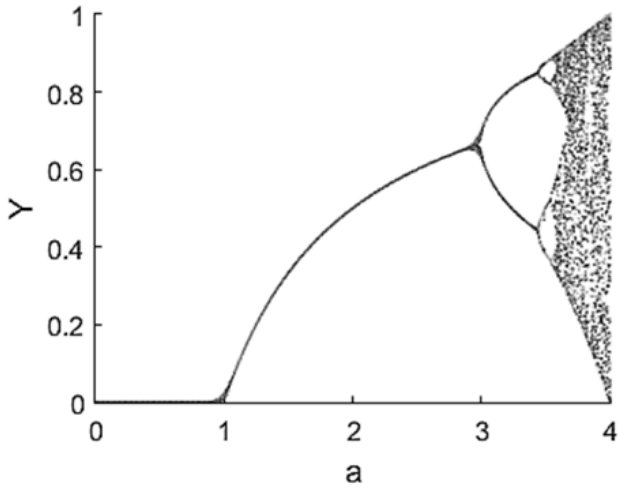


**FIGURE 3.** Bifurcation diagram of the logistic map.

1. The zigzag pattern is applied to both undivided blocks and sub-blocks, as described in Figure 2.
2. Both undivided blocks and sub-blocks rotated by 90°.
3. Random vector $r$ generated where its size is equal to the number of blocks in the plain image.
4. Random permutation between blocks based on the vector $r$ is applied to get the scrambled image.

#### 3) KEY GENERATION

The key used in the diffusion process is generated from a logistic map. The logistic map is defined by:

$$Y_{n+1} = aY_n (1 - Y_n) \tag{1}$$

where a is the control parameter with range $0 < a \leq 4$, $Y_0$ is the initial value, and $Y_n$ is the output sequence with $0 < Y_n < 1$. The map is chaotic when $a \in [3.57, 4]$. Figure 3 shows the bifurcation diagram of the logistic map. The key generation steps are defined as follows:

1. Calculate the initial value of the logistic map that depends on the plain image P by the following equation:

$$Y_0 = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} P(i, j)}{M \times N \times 255} \tag{2}$$

The numbers, M and N, refer to the number of rows and columns in the plain image, respectively.

2. Iterate the chaotic map (eq.1) $N_0 + MN$ times, and then skip the first $N_0$ elements to get a new sequence S with size MN.
3. Calculate the key using the following formula:

$$K(i) = \mathrm{mod}\left(\mathrm{floor}\left(S(i) \times 10^{14}\right), 256\right), \quad i = 1 : MN \tag{3}$$

#### 4) DIFFUSION

In the diffusion process, image pixel values are changed, and then a noise image is generated. Bit-wise exclusive OR operation between the key $K$ and the scrambled image vector is performed to obtain the encrypted image. Detailed encryption steps are presented in Algorithm 1. Also, the flowchart of the proposed algorithm is shown in Figure 4.

### *B. DECRYPTION*

With the original key and by inverting the encryption stages, we can retrieve the plain image. The decryption process is described as follows:

1. Bit-wise exclusive OR operation between the key $K$ and the encrypted image vector is applied to get the scrambled image.
2. Return each block to its original position using vector $r$.
3. The inverse operation of rotation and the zigzag pattern, respectively, are applied to both undivided blocks and sub-blocks.

## III. SIMULATION RESULTS

In this section, the efficiency of our algorithm in encrypting medical images is presented. All medical images used in this section are displayed in Figure 5, in which the grey images are from [18], and Levoy [19], and the color images are from [20]–[22]. Img1, Img2, Img6, and Img7 are $512 \times 512$, while for Img3, Img4, Img5, Img8, and Img9. The authors executed the proposed algorithm with MATLAB (R2015a) on a laptop computer equipped with Core i5-2430M 2.4GH CPU, 4GB memory, and Windows 7 OS.

The parameters used in our algorithm are: the size of blocks in image splitting is 16 (where $n = 4$), and for the logistic map: $a = 3.9$, and the iteration number $N_0 = 1000$.

**Algorithm 1** The Proposed Algorithm for Medical Image Encryption

**Input:** the plain image $P$ with size $M \times N$, parameter $a$ of the logistic map and $N_0$.

1. Divide $P$ into an equal number of blocks, with a block size $h = 2^n$ where $n$ takes a value from 4, 5, 6
2. Generate a random number for each block depending on the block size $2^l$ where $l$ takes a random value from $2, 3, \ldots n$, put the generated random numbers in a vector $R_i$, $i = 1: (MN/h^2)$.
3. For i = 1: $MN/h^2$ do
4. Divide a block into sub-blocks with the same size or keep without dividing based on $R_i$.
5. End for
6. Perform a Zigzag pattern and rotation with angle 90, respectively, to both undivided blocks and sub-blocks.
7. Generate a random vector $r$ with size $MN/\mathrm{h}^2$.
8. Random permutation of image blocks based on $r$ is performed to get the scrambled image $X$.
9. Generate the initial condition of the logistic map using (eq.2)
10. Iterate the chaotic map (eq.1) $N_0 + MN$ times, and then discard first $N_0$ elements to get a new sequence $S$ with size $MN$.
11. For i = 1: $MN$ do
12. $K(i) = mod\,(floor\,(S(i) \times 10^{14}), 256)$
13. End for
14. Convert the matrix $X$ into the 1D image pixel vector $X'$
16. $E = X' \oplus K$
17. Convert $E$ into a 2D matrix C.

**Output:** the encrypted image C

### A. ANALYSIS OF INFORMATION ENTROPY

The randomness of the image is measured by information entropy. The mathematical definition of entropy is given by:

$$\mathrm{H\,(m)} = \sum_{\mathrm{i=1}}^{\mathrm{w}} \mathrm{P(m_i)log_2}\frac{1}{P\,(\mathrm{m_i})} \tag{4}$$

where P(m) is the probability of appearance of m, for greyscale images, the maximum value of entropy is 8. When the value of entropy is near 8, the randomness of pixels in the image is higher. In this experiment, we encrypt the grey test medical images using the proposed algorithm and calculate the entropy values of the encrypted images as listed in Table 1. From the results, we can observe that all the entropy values are near 8, which indicates the true randomness of the encrypted images. The first test image (i.e., Img1) is encrypted using our algorithm and other encryption algorithms, as listed in Table 2. As can be seen, our proposed algorithm shows a higher entropy value compared to the different algorithms in Table 2. From this experiment, we conclude that our proposed algorithm assures generating encrypted images with high randomness.

### B. ANALYSIS OF IMAGE HISTOGRAM

The histogram presents the distribution of pixels in the image. For an encrypted image, the histogram should be flat to prevent the attackers from guessing any image information. Also, the histogram of both the encrypted image and the plain image should not be similar. Figure 6 shows the histograms of three medical images and their encrypted ones. As can be observed, the histograms of the encrypted images using our algorithm are uniform and not similar to their corresponding plain image histograms.

An additional experiment was performed to confirm that the histogram of the encrypted image is uniform. This experiment is based on the chi-square test ($\chi^2$) which is calculated by [27]:

$$\chi^2 = \sum_{i=1}^{256} \frac{(O_i - EV)^2}{EV} \tag{5}$$

where $O_i$ refers to the recurrence rate of grey value $i$, and $EV = O/256$ is the expected frequency of each grey value.

The value of $\chi^2_{(\alpha,d)}$ is 293.2478, where the significance level $\alpha$ is 0.05 and the degree of freedom $d$ is 255. The values $\chi^2$ of the encrypted image are presented in Table 3. All the values are less than 293, which means that the histogram of the images encrypted with our proposed algorithm is uniform.

### C. ANALYSIS OF CORRELATION COEFFICIENT

Principally in the plain image, adjacent pixels show high correlation as their values are nearly identical. The encryption algorithm's efficiency is based on generating an encrypted image with a low correlation between adjacent pixels. Mathematically, the correlation coefficient between two adjacent pixels defined by the following equations:

$$\mathrm{r_{A,B}} = \frac{\mathrm{E(\,(A - E\,(A))\,(B - E\,(B)))}}{\sqrt{\mathrm{D(A)D(B)}}} \tag{6}$$

$$\mathrm{E\,(A)} = \frac{1}{\mathrm{s}}\sum_{\mathrm{i=1}}^{\mathrm{s}} \mathrm{A_i} \tag{7}$$

$$\mathrm{D\,(A)} = \frac{1}{\mathrm{s}}\sum\nolimits_{\mathrm{i=1}}^{\mathrm{s}} \mathrm{(A_i - E(A))^2} \tag{8}$$

where **A** and **B** are the grey values of two adjacent pixels, and **s** is the total number of selected pairs (**A**, **B**). Table 4 presents the correlation coefficient values for both grey test images and their encrypted ones in the horizontal (H), vertical (V), and diagonal (D) directions. All the test images have correlation coefficient values close to one; however, the encrypted images' correlation coefficient values are near to zero. The comparison with other methods based on Img1 is listed in Table 5. This experiment demonstrates that the proposed algorithm effectively reduces the adjacent pixels' correlation in the encrypted image.

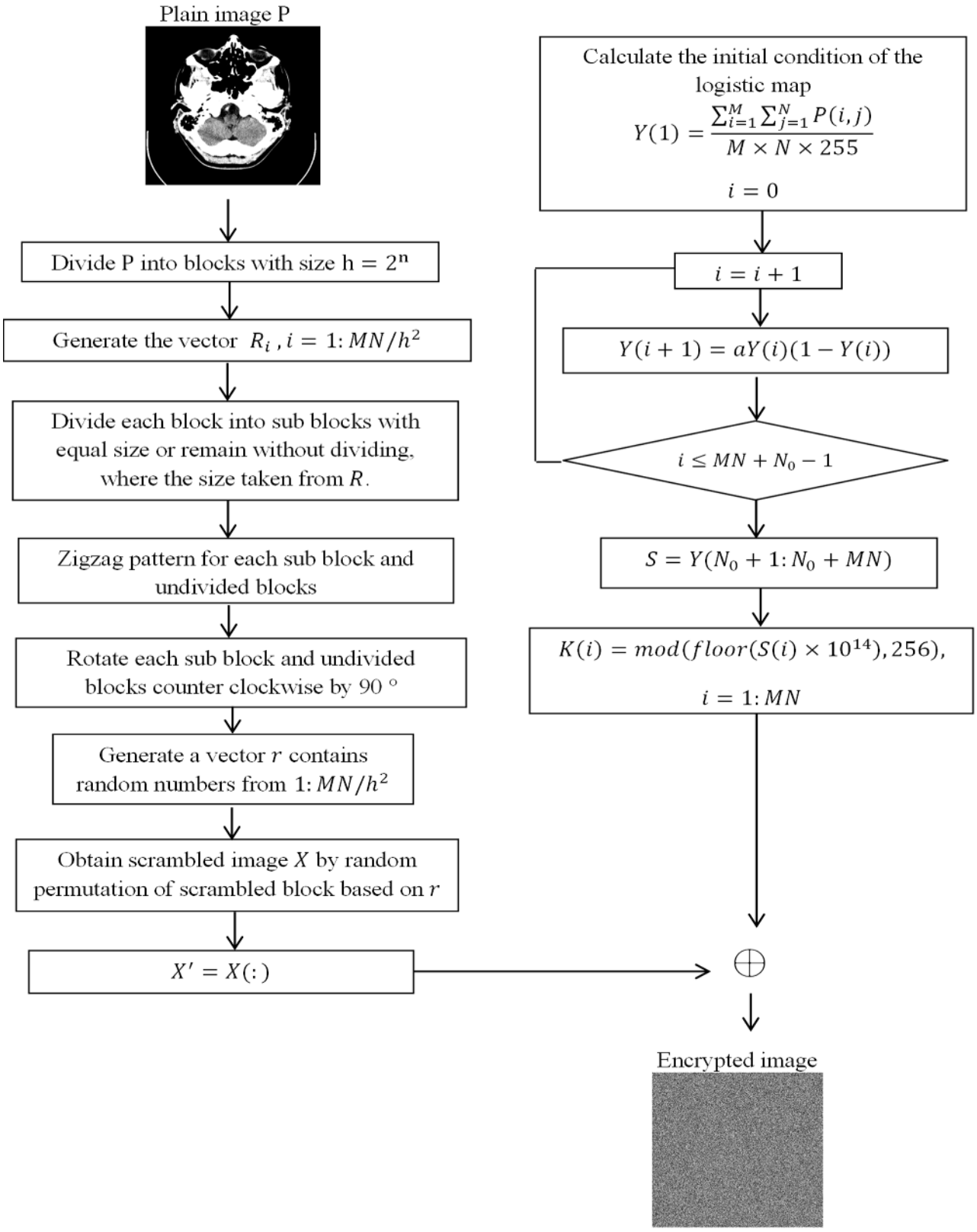


**FIGURE 4.** Flowchart of the proposed algorithm.

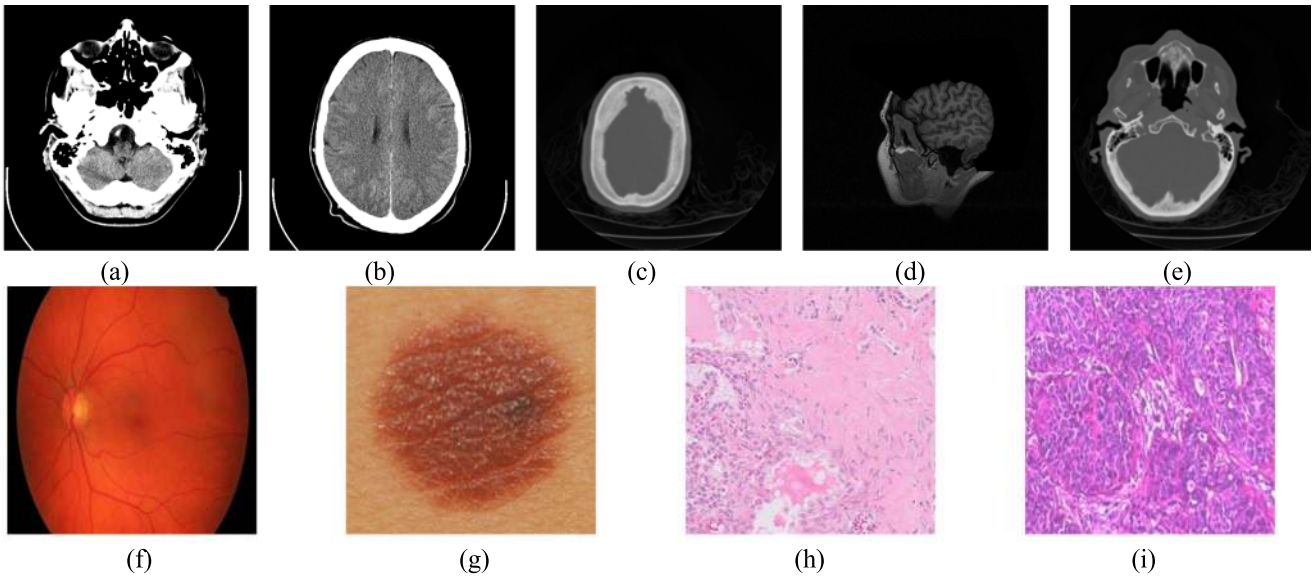


**FIGURE 5.** The test images. (a) The image Img1 [18]. (b) The image Img2 [18]. (c) The image Img3 [19]. (d) The image Img4 [19]. (e) The image Img5 [19]. (f) The image Img6 [20]. (g) The image Img7 [21]. (h) The image Img8 [22]. (i) The image Img9 [22].

**TABLE 1.** Encrypted images entropy.

| Test image | Entropy |
|---|---|
| Img1 | 7.9993 |
| Img2 | 7.9994 |
| Img3 | 7.9974 |
| Img4 | 7.9972 |
| Img5 | 7.9977 |

**TABLE 2.** Entropy value of our algorithm and other algorithms.

| Method | Entropy |
|---|---|
| Proposed | 7.9993 |
| [23] | 7.909 |
| [24] | 7.9926 |
| [25] | 7.99 |
| [26] | 4.745 |
| [15] | 7.9993 |

### D. ANALYSIS OF DIFFERENTIAL ATTACK

The differential attack depends on guessing information about an image by making a slight change in the plain image and encrypting both images using the same algorithm. We compare both images to detect a correlation between the plain image and the encrypted image. Using a practical algorithm, any slight change in the plain image should produce a different encrypted image. To assess the algorithm's performance, the Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI) used. The NPCR and UACI are calculated as follows:

$$\mathrm{NPCR} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\,(\%) \tag{9}$$

$$D(i,j) = \begin{cases} 0 & \text{if } E_1(i,j) = E_2(i,j), \\ 1 & \text{if } E_1(i,j) \neq E_2(i,j), \end{cases} \tag{10}$$

$$\mathrm{UACI} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} \frac{|E_1(i,j) - E_2(i,j)|}{255} \times 100\,(\%) \tag{11}$$

The symbols $E_1$ and $E_2$ refer to two encrypted images from the plain image and the modified image (made by changing one pixel in the plain image). The image width is M. Its height is N. Here, we study our proposed algorithm's effectiveness in resisting differential attacks by recording the NPCR and UACI values between the two encrypted images in table 6. The ideal value of NPCR is 99.6094%, and of UACI is 33.4635%. All values in Table 6 are close to their ideal values. Table 7 shows a comparison between our algorithm and other image encryption algorithms. The results show that our proposed algorithm is highly capable of resisting differential attacks.

### E. ANALYSIS OF KEYSPACE

The keyspace of a good image encryption algorithm should be at least $2^{100}$. If the keyspace is not large enough, the algorithm could be broken using brute-force attacks. In this algorithm, the keyspace includes the initial condition $Y_0$, the control parameter a, and the initial iteration number $N_0$ of the chaotic map. Here, we consider the precision of $Y_0$ and a to be $10^{16}$, and $N_0 = 10^3$ So the total keyspace is $10^{35}$. Therefore, our algorithm can resist brute-force attacks as the keyspace is large enough.

### F. ANALYSIS OF KEY SENSITIVITY

A practical algorithm should be susceptible to any slight change to its secret key. Attackers can break the encryption algorithm using a similar key, so any small change in the key used in the decryption step cannot reconstruct the plain image. Here, we generate two secret keys with only a slight change in $Y_0$ by modifying it to $Y_0 + 10\hat{}(-10)$. The first key used in the plain image's encryption step is shown in Figure 7(a), and the results are shown in Figure 7(b). The second key used in the decryption step (the obtained results are shown in Figure (7c)). As can be seen, the second key failed to retrieve the plain image. When using the first

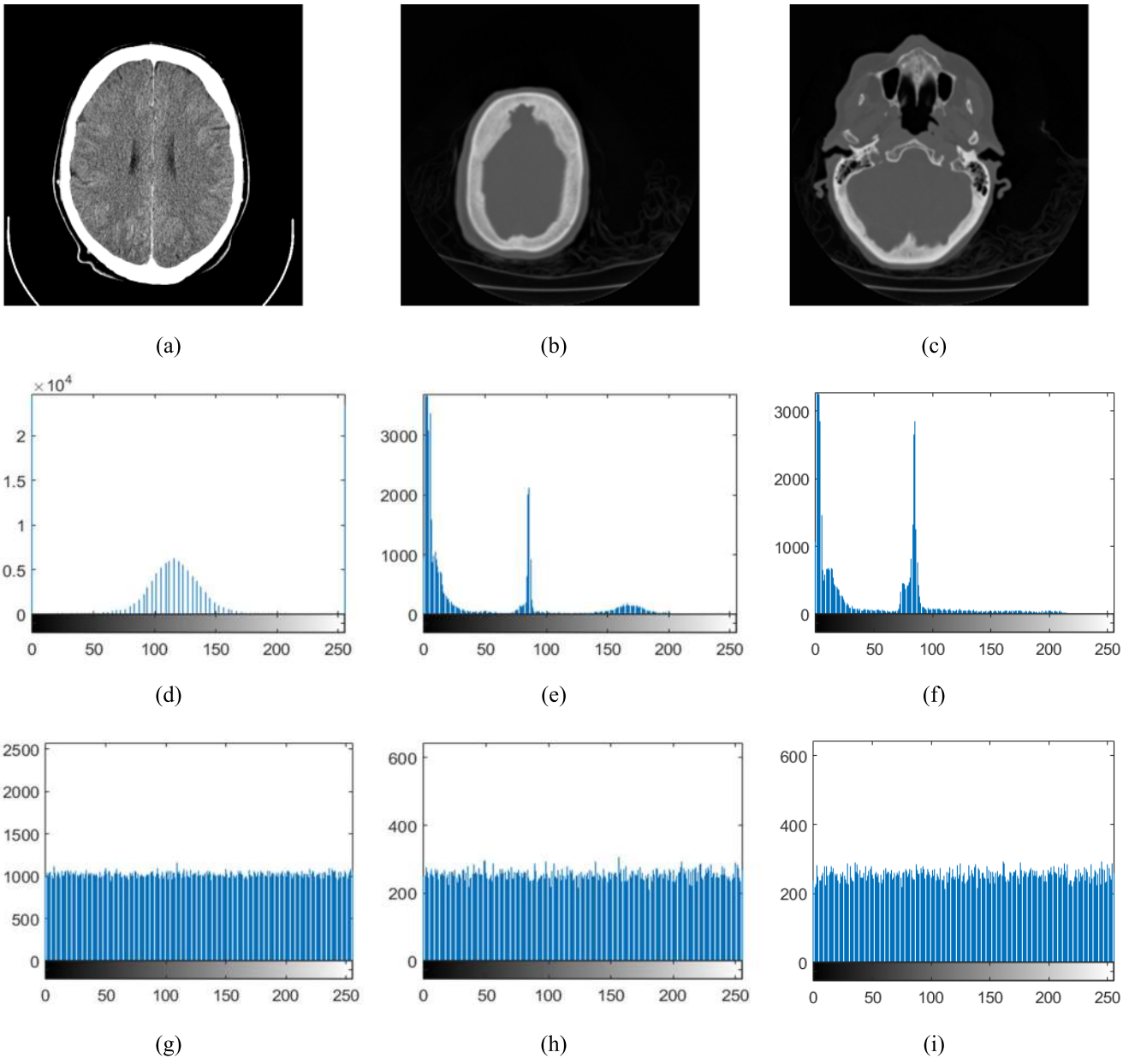


**FIGURE 6.** Histogram analysis of gray images. (a) The plain image Img 2. (b) The plain image Img 3. (c) The plain image Img 5. (d) Histogram of (a). (e) Histogram of (b). (f) Histogram of (c). (g) Histogram of the encrypted image in (a). (h) Histogram of the encrypted image in (b). (i) Histogram of the encrypted image in (c).

**TABLE 3.** Chi-Square analysis.

| Test image | Encrypted image |
|---|---|
| Img1 | 262.9102 |
| Img2 | 242.0332 |
| Img3 | 232.2969 |
| Img4 | 270.7578 |
| Img5 | 212.4219 |

key in the decryption step, the plain image is reconstructed successfully, as shown in Figure 7(d).

### G. ANALYSIS OF ENCRYPTION EFFICIENCY

Peak signal to noise ratio (PSNR) is used to measure the difference between the original image and the encrypted image and is calculated by:

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{\text{MSE}}\right) \text{(db)} \tag{12}$$

$$\text{MSE} = \frac{1}{\text{MN}} \sum_{\text{i}=1}^{\text{M}} \sum_{\text{j}=1}^{\text{N}} |\text{OI}\,(\text{i}, \text{j}) - \text{EI}(\text{i}, \text{j})|^2 \tag{13}$$

The OI refers to the original image, and EI is the encrypted image. The lower values of PSNR indicate a significant difference between the original and the encrypted image. Table 8 lists the PSNR values for different grey medical images. From the results, we can conclude that our proposed algorithm is highly efficient in medical image encryption.

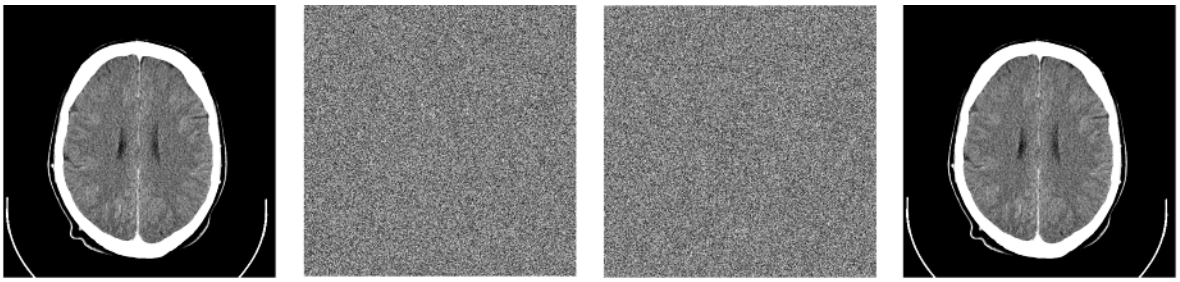


**FIGURE 7.** The sensitivity of our algorithm to the key. (a) Plain image. (b) The encrypted image of (a) using the first key. (c) A decrypted image of (b) using the second key. (d) The decrypted image of (b) using the first key.

**TABLE 4.** Correlation coefficient values.

| Test image | Direction | Plain image | Encrypted image |
|---|---|---|---|
| Img2 | V | 0.9863 | -0.0108 |
| | H | 0.9727 | 0.0182 |
| | D | 0.9656 | 0.0165 |
| Img3 | V | 0.9917 | -0.0237 |
| | H | 0.9934 | 0.0059 |
| | D | 0.9849 | 0.0080 |
| Img4 | V | 0.9730 | 0.0046 |
| | H | 0.9543 | -0.0044 |
| | D | 0.9414 | 0.0081 |
| Img5 | V | 0.9841 | 0.0063 |
| | H | 0.9837 | 0.0298 |
| | D | 0.9708 | 0.0012 |

**TABLE 5.** Comparison of the correlation coefficient values between our algorithm and other algorithms.

| Method | H | V | D |
|---|---|---|---|
| Proposed | -0.0093 | 0.0025 | -0.0024 |
| [23] | -0.0012 | 0.0099 | -0.0032 |
| [24] | 0.0027 | 0.0015 | 0.0019 |
| [25] | 0.0023 | -0.0010 | 0.0009 |
| [26] | 0.0944 | 0.0057 | 0.0067 |
| [15] | 0.0098 | -0.0078 | 0.0181 |

**TABLE 6.** NPCR and UACI performances.

| Test image | NPCR | UACI |
|---|---|---|
| Img2 | 99.6223 | 33.4406 |
| Img3 | 99.6216 | 33.4813 |
| Img4 | 99.6002 | 33.4535 |
| Img5 | 99.6231 | 33.4903 |

**TABLE 7.** Comparison of NPCR and UACI.

| Method | NPCR | UACI |
|---|---|---|
| Proposed | 99.6010 | 33.4389 |
| [23] | 99.610 | 33.261 |
| [24] | 99.532 | 33.450 |
| [25] | 99.51 | 33.39 |
| [26] | 99.79 | 33.16 |
| [15] | 99.6067 | 33.4954 |

Our proposed algorithm was also tested on images from Levoy [19]. The average of entropy, NPCR, UACI, correlation coefficient in the three directions, PSNR, and chi-square listed in Table 9. All image formats are 8-bit TIF and size 256 × 256. All the results obtained with our proposed algorithm are ideal, which evidences the robustness of our algorithm.

**TABLE 8.** PSNR analysis.

| Test image | PSNR |
|---|---|
| Img1 | 5.1192 |
| Img2 | 5.8811 |
| Img3 | 5.6824 |
| Img4 | 5.2935 |
| Img5 | 6.0865 |

**TABLE 9.** The average of entropy, correlation coefficient, NPCR, UACI, PSNR and Chi-Square values for grey medical images.

| Entropy | Correlation coefficient | | | NPCR | UACI | PSNR | $\chi^2$ |
|---|---|---|---|---|---|---|---|
| | V | H | D | | | | |
| 7.9973 | -0.0008 | 0.0057 | 0.0037 | 99.604 | 33.4654 | 5.62806 | 243.5238 |

**TABLE 10.** Maximum deviation analysis.

| Test image | Maximum deviation |
|---|---|
| Img1 | 33,2191 |
| Img2 | 370931 |
| Img3 | 96,016 |
| Img4 | 95,821 |
| Img5 | 89,861 |

### H. ANALYSIS OF ENCRYPTION QUALITY

#### 1) MAXIMUM DEVIATION

The quality of encryption is evaluated by measuring the difference in pixel values between the plain and encrypted images. The encryption algorithm is considered to be efficient if this difference is significant. The maximum deviation is calculated by

$$D = \frac{M_0 + M_{255}}{2} + \sum_{i=1}^{254} M_i \tag{14}$$

where $M_i$ the difference of histogram between the plain and the encrypted image at index i. The high value of D indicates the significant difference between the plain and the encrypted image. The maximum deviation values using our proposed algorithm listed in table 10. Large values indicate that the images encrypted using proposed algorithms are entirely

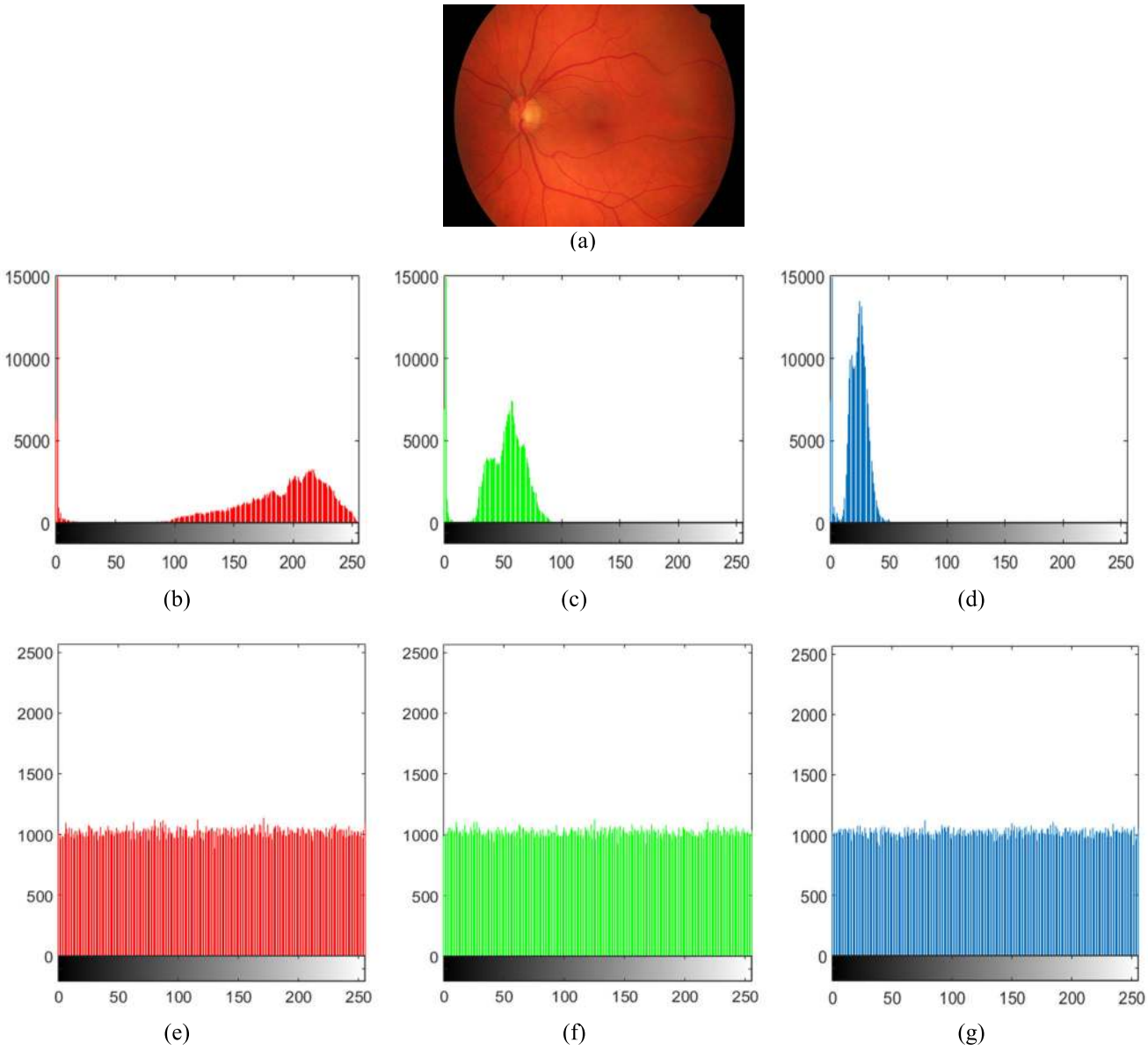


**FIGURE 8.** Histogram analysis of Img6. (a) Original plain image. (b) Plain image histograms of red channel. (c) plain image histograms of green channel. (d) Plain image histograms of blue channel. (e) Encrypted image histograms of red channel. (f) Encrypted image histograms of red channel. (g) Encrypted image histograms of blue channel.

different from the plain image that proves our algorithm's excellent performance in terms of security.

#### 2) DEVIATION FROM UNIFORM HISTOGRAM

A good encryption algorithm should produce an encrypted image with a uniform histogram. The quality of the encryption algorithm assessed by histogram deviation, which is defined by:

$$H_{C_i} = \begin{cases} \dfrac{M \times N}{256}, & 0 \le C_i \le 255 \\ 0, & elsewhere \end{cases} \tag{15}$$

$$D_H = \frac{\sum_{C_i=0}^{255} |H_{C_i} - H_C|}{M \times N} \tag{16}$$

The $H_C$ refers to the histogram of the encrypted image. A lower value $D_H$ indicates the histogram's uniformity, which ensures high encryption quality—results in table 11 show low values of $D_H$ that poof high encryption quality of the proposed algorithm.

### *I. COLOR MEDICAL IMAGE TESTING RESULTS*

With the advancement of medical devices' modern technology, color medical images became widely used in diagnosing diseases. Our proposed algorithm can also be applied to encrypt color medical images. Generally, color images contain more information than grey ones as each pixel in a color image has three values (Red, Green, and Blue). So, encrypting color images could be done by separating the image into three channels (R, G, and B) then using the algorithm to encrypt

**TABLE 11.** Deviation from a uniform histogram.

| Test image | Histogram deviation |
|---|---|
| Img1 | 0.0253 |
| Img2 | 0.0227 |
| Img3 | 0.0510 |
| Img4 | 0.0473 |
| Img5 | 0.0524 |

**TABLE 12.** The entropy, Correlation coefficient, and NPCR and UACI values for color medical images in three channels.

| Image | | Entropy | Correlation coefficient | | | NPCR | UACI |
|---|---|---|---|---|---|---|---|
| | | | V | H | D | | |
| Img6 | R | 7.9992 | -0.0166 | 0.0271 | -0.0060 | 99.6120 | 33.4301 |
| | G | 7.9993 | 0.0050 | -0.0157 | -0.0066 | 99.6197 | 33.4274 |
| | B | 7.9992 | -0.0051 | -0.0242 | 0.0053 | 99.6132 | 33.4339 |
| Img7 | R | 7.9994 | 0.0046 | -0.0013 | 0.0071 | 99.6029 | 33.5269 |
| | G | 7.9993 | -0.0075 | 0.0031 | 0.0046 | 99.6262 | 33.4666 |
| | B | 7.9994 | -0.0132 | 0.0033 | 0.0073 | 99.6151 | 33.4805 |
| Img8 | R | 7.9972 | 0.0130 | 0.0029 | 0.0065 | 99.6231 | 33.4816 |
| | G | 7.9974 | -0.0064 | 0.0139 | -0.0026 | 99.6262 | 33.4150 |
| | B | 7.9974 | -0.0144 | 0.0160 | 0.0065 | 99.6307 | 33.4774 |
| Img9 | R | 7.9978 | 0.0015 | 0.0002 | -0.0079 | 99.6063 | 33.4874 |
| | G | 7.9972 | 0.0071 | -0.0054 | -0.0031 | 99.6048 | 33.4563 |
| | B | 7.9975 | 0.0074 | 0.0063 | -0.0057 | 99.6216 | 33.4739 |
| Average | R | 7.9993 | -0.0015 | 0.0192 | 0.0091 | 99.6115 | 33.4507 |
| | G | 7.9993 | 0.0067 | 0.0098 | 0.0142 | 99.5974 | 33.4375 |
| | B | 7.9992 | 0.0014 | 0.0238 | 0.0007 | 99.6107 | 33.4903 |

each channel independently. In this experiment, we used four color medical images, shown in Figure 5 (i.e., Img6, Img7, Img8, and Img9), as test images. Table 12 shows the entropy results, correlation coefficient values in the three directions, NPCR, and UACI of the three channels for the encrypted color medical images. All the obtained results are close to their ideal values. Also, the histogram analysis of the color image (Img6) is shown in Figure 8. Encrypted image histograms of the three channels are all flat and different from the plain image histograms.

Our proposed algorithm was also tested on the dataset [21] that consists of 70 melanoma and 100 naevus images. The image format is JPG, and we resize all images to $512 \times 512$, and the averages of all images in each channel listed in table 12. Therefore, our proposed algorithm is efficient in encrypting color medical images.

### J. ANALYSIS OF TIME COMPLEXITY

Here we estimate the time complexity in each step of the encryption process to evaluate our proposed algorithm's total time complexity. Assume that the plain image is with size $\boldsymbol{M} \times \boldsymbol{N}$, and the block size $\boldsymbol{h} = \boldsymbol{2^n}$ where $\boldsymbol{n} = \boldsymbol{4}$. The time complexity for the plain image splitting and confusion stages is $\boldsymbol{O}((\mathbf{M} \times \mathbf{N})/\boldsymbol{h^2})$. For the key generation stage and the diffusion stage, the time complexity is $\boldsymbol{O}(\boldsymbol{M} \times \boldsymbol{N})$. Therefore, the total time complexity of our proposed algorithm is $\boldsymbol{O}(\boldsymbol{M} \times \boldsymbol{N})$.

## IV. CONCLUSION

This paper introduced a new algorithm for encrypting medical images based on image blocks and chaos. The proposed algorithm's image encryption performance tested using entropy, histogram, correlation coefficient, differential attack, keyspace, and key sensitivity. Results showed that the proposed algorithm is efficient in encrypting both grey and color medical images. Our algorithm compared to other recent encryption algorithms, and the results confirm that the proposed algorithm has good characteristics in encrypting both grey and color medical images.

## REFERENCES

[1] X. Liao, J. Yin, S. Guo, X. Li, and A. K. Sangaiah, "Medical JPEG image steganography based on preserving inter-block dependencies," *Comput. Electr. Eng.*, vol. 67, pp. 320–329, Apr. 2018.

[2] M. A. Usman and M. R. Usman, "Using image steganography for providing enhanced medical data security," in *Proc. 15th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2018.

[3] K. M. Hosny, M. M. Darwish, K. Li, and A. Salah, "Parallel multi-core CPU and GPU for fast and robust medical image watermarking," *IEEE Access*, vol. 6, pp. 77212–77225, Dec. 2018.

[4] K. M. Hosny and M. M. Darwish, "Robust color image watermarking using invariant quaternion legendre-Fourier moments," *Multimedia Tools Appl.*, vol. 77, no. 19, pp. 24727–24750, Oct. 2018.

[5] K. M. Hosny and M. M. Darwish, "Resilient color image watermarking using accurate quaternion radial substituted chebyshev moments," *ACM Trans. Multimedia Comput., Commun., Appl.*, vol. 15, no. 2, pp. 1–25, Jun. 2019.

[6] A. M. Vengadapurvaja, G. Nisha, R. Aarthy, and N. Sasikaladevi, "An efficient homomorphic medical image encryption algorithm for cloud storage security," *Procedia Comput. Sci.*, vol. 115, pp. 643–650, 2017.

[7] J. Liu, Y. Ma, S. Li, J. Lian, and X. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimedia Tools Appl.*, vol. 77, no. 17, pp. 22787–22808, Sep. 2018.

[8] J. Liu, S. Tang, J. Lian, Y. Ma, and X. Zhang, "A novel fourth order chaotic system and its algorithm for medical image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 4, pp. 1637–1657, Oct. 2019.

[9] K. Shankar, M. Elhoseny, E. D. Chelvi, S. K. Lakshmanaprabu, and W. Wu, "An efficient optimal key based chaos function for medical image security," *IEEE Access*, vol. 6, pp. 77145–77154, 2018.

[10] J. Chen, L. Chen, L. Y. Zhang, and Z.-L. Zhu, "Medical image cipher using hierarchical diffusion and non-sequential encryption," *Nonlinear Dyn.*, vol. 96, no. 1, pp. 301–322, Apr. 2019.

[11] G. Ke, H. Wang, S. Zhou, and H. Zhang, "Encryption of medical image with most significant bit and high capacity in piecewise linear chaos graphics," *Measurement*, vol. 135, pp. 385–391, Mar. 2019.

[12] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019.

[13] Z. Mishra and B. Acharya, "High throughput and low area architectures of secure IoT algorithm for medical image encryption," *J. Inf. Secur. Appl.*, vol. 53, Aug. 2020, Art. no. 102533.

[14] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017.

[15] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 144, pp. 134–144, Mar. 2018.

[16] M. Chen, G. Ma, C. Tang, and Z. Lei, "Generalized optical encryption framework based on shearlets for medical image," *Opt. Lasers Eng.*, vol. 128, May 2020, Art. no. 106026.

[17] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Process.*, vol. 132, pp. 96–109, Mar. 2017.

[18] *Category: Computed Tomography Images of Mikael Häggström's Brain*. Accessed: Feb. 9, 2021. [Online]. Available: https://commons.wikimedia.org/wiki/Category:Computed_tomography_images_of_Mikael_H%C3%A4ggstr%C3%B6m%27s_brain

[19] *The Stanford Volume Data Archive*. Accessed: Feb. 9, 2021. [Online]. Available: https://graphics.stanford.edu/data/voldata/

[20] *RITE (Retinal Images Vessel Tree Extraction) Database*. Accessed: Feb. 9, 2021. [Online]. Available: https://uiowa.qualtrics.com/jfe/form/SV_a3mc5H4SG2B3e2p?Q_JFE=qdg

[21] *Dermatology Database Used in MED-NODE*. Accessed: Feb. 9, 2021. [Online]. Available: http://www.cs.rug.nl/~imaging/databases/melanoma_naevi/
[22] *Breast Cancer Histopathological Database (BreakHis)*. Accessed: Jan. 8, 2021. [Online]. Available: https://web.inf.ufpr.br/vri/databases/breast-cancer-histopathological-database-breakhis/
[23] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, Jan. 2019.
[24] J. Chandrasekaran and S. J. Thiruvengadam, "A hybrid chaotic and number theoretic approach for securing DICOM images," *Secur. Commun. Netw.*, vol. 2017, Jan. 2017, Art. no. 6729896.
[25] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and DNA encoding," *Multimedia Tools Appl.*, vol. 76, no. 5, pp. 6229–6245, Mar. 2017.
[26] S. Kumar, B. Panna, and R. Kumar, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Med. Biol. Eng. Comput.*, vol. 57, no. 11, pp. 2517–2533, 2019.
[27] A. Banu S and R. Amirtharajan, "A robust medical image encryption in dual domain: Chaos-DNA-IWT combined approach," *Med. Biol. Eng. Comput.*, vol. 58, no. 7, pp. 1445–1458, Jul. 2020.

**SARA T. KAMAL** received the B.Sc. and M.Sc. degrees in computer science from the Faculty of Science, Assiut University, Assiut, Egypt. She is currently an Assistant Lecturer with the Faculty of Computers and Informatics, Assiut University.

**KHALID M. HOSNY** (Senior Member, IEEE) was born in Zagazig, Egypt, in 1966. He received the B.Sc., M.Sc., and Ph.D. degrees from Zagazig University, Egypt, in 1988, 1994, and 2000, respectively. From 1997 to 1999, he was a Visiting Scholar with the University of Michigan, Ann Arbor, and the University of Cincinnati, Cincinnati, USA. He is currently a Professor of information technology with the Faculty of Computers and Informatics, Zagazig University. He published three edited books and more than 80 articles in international journals. His research interests include image processing, pattern recognition, multimedia, and computer vision. He is a Senior Member of ACM. He is an Editor and a Scientific Reviewer of more than 40 international journals.

**TAHA M. ELGINDY** received the B.Sc. and M.Sc. degrees from Assiut University, in 1967 and 1971, respectively, and the Ph.D. degree from Swansea University (G.B), in 1977. He is currently a Professor of operation research (OR). He is the supervisor of more than 60 students in many universities in Egypt in (OR) and numerical analysis.

**MOHAMED M. DARWISH** received the B.Sc. (Hons.) and M.Sc. degrees in computer science from the Faculty of Science, Assiut University, Assiut, Egypt. He is currently a Lecturer with the Department of Computer Sciences, Faculty of Computers and Informatics, Assiut University. His research interests include image processing and data mining.

**MOSTAFA M. FOUDA** (Senior Member, IEEE) received the Ph.D. degree in information sciences from Tohoku University, Japan, in 2011. He has worked at Tohoku University, Japan, as an Assistant Professor. He has also worked at Tennessee Technological University, TN, USA, as a Postdoctoral Research Associate. He is currently an Assistant Professor with Idaho State University, Pocatello, ID, USA. He also holds the position of an Associate Professor with Benha University, Egypt. He has published over 30 papers in IEEE conference proceedings and journals. His research interests include cybersecurity, machine learning, blockchain, the IoT, 5G networks, and smart grid communications. He has served on the technical committees of several IEEE conferences. He is also a Reviewer in several IEEE Transactions/Magazines and an Associate Editor of IEEE Access.