EiMOL: A Secure Medical Image Encryption Algorithm based on Optimization and the Lorenz System

KN SINGH, OP SINGH, and AMIT KUMAR SINGH, Department of CSE, NIT Patna
AMRIT KUMAR AGRAWAL, Galgotias College of Engineering and Technology

Nowadays, the demand for digital images from different intelligent devices and sensors has dramatically increased in smart healthcare. Due to advanced low-cost and easily available tools and software, manipulation of these images is an easy task. Thus, the security of digital images is a serious challenge for the content owners, healthcare communities, and researchers against illegal access and fraudulent usage. In this article, a secure medical image encryption algorithm, *EiMOL*, based on optimization and the Lorenz system, is proposed for smart healthcare applications. In the first stage, an optimized random sequence (ORS) is generated through directed weighted complex network particle swarm optimization using the genetic algorithm (GDWCN-PSO). This random number matrix and the Lorenz system are adopted to encrypt plain medical images, obtaining the cipher messages with a relationship to the plain images. According to our obtained results, the proposed *EiMOL* encryption algorithm is effective and resistant to the many attacks on benchmark Kaggle and Open-i datasets. Further, extensive experimental results demonstrate that the proposed algorithm outperforms the state-of-the-art approaches.

CCS Concepts: • **Security and privacy → Symmetric cryptography and hash functions**;

Additional Key Words and Phrases: Healthcare system, medical image, encryption, optimization, security

ACM Reference format:
KN Singh, OP Singh, Amit Kumar Singh, and Amrit Kumar Agrawal. 2023. EiMOL: A Secure Medical Image Encryption Algorithm based on Optimization and the Lorenz System. *ACM Trans. Multimedia Comput. Commun. Appl.* 19, 2s, Article 94 (February 2023), 19 pages.
https://doi.org/10.1145/3561513

1 INTRODUCTION

With the proliferation of the **Internet of Things (IoT)**, the healthcare industry has experienced significant growth in recent years [1]. There is no doubt that the use of the IoT in healthcare not only improves operational efficiency for medical professionals and hospitals but also provides service convenience for supporting patients and their relatives. Particularly after the COVID-19 pandemic, medical images serve as information carriers for various purposes, such as for medical

KN Singh also associated with the Department of CSE, Noida Institute of Engineering and Technology, Greater Noida, UP, (India).
Authors' addresses: KN Singh, OP Singh, and A. K. Singh (corresponding author), Department of CSE, National Institute of Technology Patna, Patna, Bihar 800005, India; emails: {knsinghait, omprakash7667}@gmail.com, amit.singh@nitp.ac.in; A. K. Agrawal, Department of CSE, Galgotias College of Engineering and Technology, Greater Noida, Uttar Pradesh 201310, India; email: agrawal.amrit4@gmail.com.

1551-6857/2023/02-ART94 $15.00
https://doi.org/10.1145/3561513

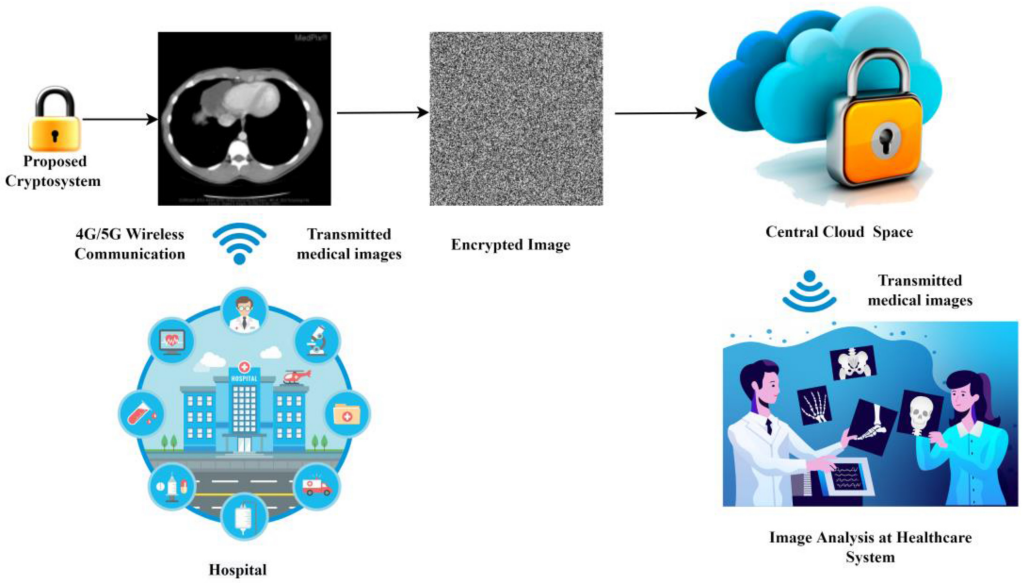

Fig. 1. Smart healthcare system using encryption.

diagnoses, telesurgeries, defence, medical education, teleconsulting, research and business analytics [2–4]. The smart healthcare system's use of encryption is shown in Figure 1. It is established that medical images bring convenience to communication, but their use also introduces serious security threats [5].

Furthermore, the issue of identity theft and copyright protection is becoming more prevalent by the day [6–8]. The integrity of data must be safeguarded against unauthorised users. Encryption is a popular technique for protecting medical data from illegitimate access [9]. Presently, terabytes of multimedia data are generated and used by the medical professionals, staff and the research community [10].

For the last few years, different encryption-based mechanisms have been proposed for healthcare scenarios. For example, Kaur and Singh [11] proposed an optimization-based image encryption scheme. The parameters of the 5D hyper-chaotic system are optimized using the multi-objective optimization method. A hyper-chaotic map then produces the secret keys by utilizing optimal parameters. Finally, two times permutation and diffusion are applied to encrypt the image. Simulation results of this optimization-based scheme yield achieve high security; however, the computational cost of the scheme needs to be minimized. Lakshmi et al. [12] designed a **Hopfield neural network (HNN)** to perform the encryption of medical images. The back propagation neural network is applied to produce the adaptive key, and the HNN is then used to generate random sequences for the permutation and diffusion process of the image. The experimental results demonstrate that the proposed scheme provides resistance to various security attacks, including chosen plain text attacks; however, the noise robustness of the scheme needs to be verified. To overcome the weakness in the image encryption scheme, Chai et al. [13] propounded **hybrid multi-objective particle swarm optimization** (**HMPSO**) and compressive sensing-based image encryption scheme. Block-based compressive sensing is utilized to reduce the size of encryption data. The scheme shows good security features; however, the computation time of the scheme is also high. Saravanan and Sivabalakrishnan [14] proposed an optimized **hybrid chaotic map** (**HCM**) based image encryption scheme in which a **two-dimensional logistic chaotic map** (**2DLCM**)

and a **piecewise linear chaotic map** (**PWLCM**) are combined to generate the random sequence for permutation and diffusion. Moreover, initial values of chaotic maps are optimized using the **coefficient improved whale optimization algorithm** (**CIWOA**). The scheme exhibits better security results than similar methods; however, the computational complexity of the scheme is high. Toktas and Erkan [15] presented an **artificial bee colony** (**ABC**) optimization-based image encryption scheme. A two-dimensional chaotic map is utilized for encryption, which is created by ABC. The proposed scheme presents better simulation results as compared to state-of-the-art techniques. Luo et al. [16] also suggested optimization-based image encryption for healthcare applications. The plain image is confused by the **particle swarm optimization** (**PSO**) method, and diffusion operation is performed using a complex Lu system. The suggested method performs well in simulations and security analyses. Yin and Li [17] suggested a quantum chaos system and optimization-cantered medical image encryption algorithm in which PSO is used with a simulated annealing algorithm to perform the scrambling operation. The result analysis shows that the proposed scheme is robust against several security attacks, and computational cost is also low. Bharadwaj et al. [18] proposed an image security scheme for a smart healthcare system, and they utilized a chaotic map, quantum map and Jacobian elliptic map to encrypt the images. The encryption process includes key initialization, synchronization of chaotic maps, generation of feature matrix, scrambling and diffusion. The results demonstrate that the proposed scheme is reliable, secure and lightweight. Song et al. [19] designed an encryption scheme for a group of medical images in which parallel permutation and a cipher-block-chaining-based substitution are performed to encrypt the images. The security analysis of the suggested scheme shows that it provides the necessary security and also takes less time to encrypt the group of medical images.

In summary, most of the above encryption techniques are costly and do not achieve a high level of security. To overcome these deficiencies, a secure medical image encryption algorithm, called *EiMOL*, based on the GDWCN-PSO [20] and a **three-dimensional Lorenz system** (**3D-LS**) [21], is proposed for smart healthcare applications. The main contributions of this articleare outlined below.

(1) *Generation of optimized random number*: An **optimized random sequence** (**ORS**) is generated by utilizing the GDWCN-PSO and a logistic map. By optimizing, we neutralize the correlation between generated numbers by the logistic map to achieve better security.
(2) *Secure encryption using a logistic map and the Lorenz attractor*: We integrate an ORS and the 3D-LS to propose a secure and efficient encryption algorithm. The Lorenz system is mostly chaotic at every instance of the input.
(3) *Experimental analysis*: The experimental results prove that the *EiMOL* algorithm is secure against different attacks. Further, extensive experimental results on real-world datasets demonstrate that the proposed algorithm outperforms the state-of-the-art approaches.

The rest of the articleis organized as follows: Section 2 describes the proposed methodology, Section 3 discusses the experimental results, and Section 4 presents the concluding remarks.

2 THE PROPOSED *EiMOL* ALGORITHM

In the *EiMOL* algorithm, the logistic map and a 3D-LS are adopted to encrypt an image. Here, an ORS is obtained by utilizing the GDWCN-PSO and the logistic map, which is used for the permutation process. Furthermore, two rounds of diffusion are applied by the 3D-LS map to encrypt plain medical images. The complete flow diagram of the proposed *EiMOL* algorithm is presented in Figure 2. The complete *EiMOL* algorithm contains four consecutive parts: key initialization, obtaining ORS, encryption and decryption. The details of each part are presented in different sub-sections.

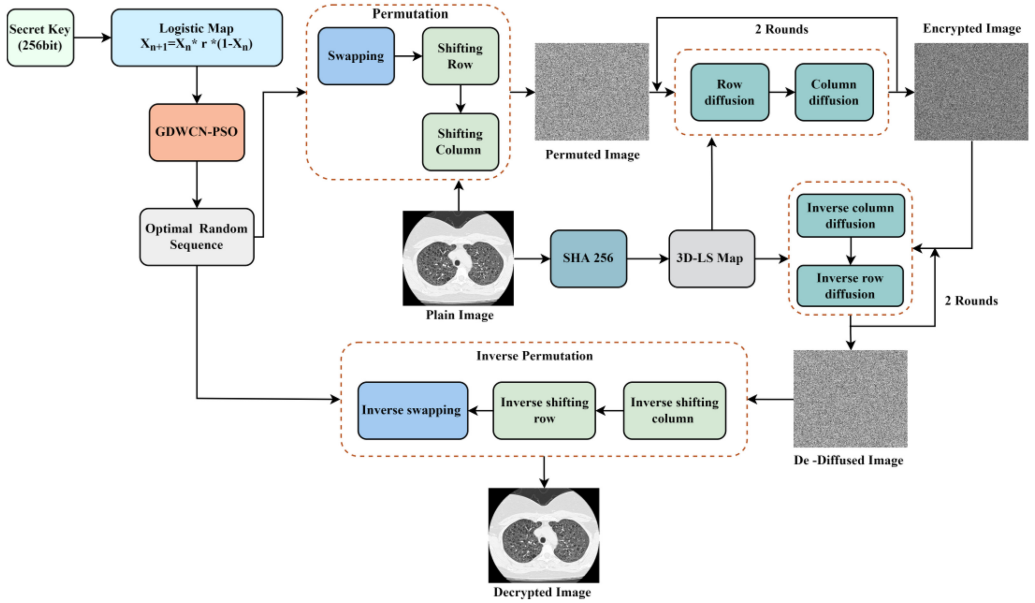

Fig. 2. Block diagram of proposed *EiMOL* algorithm.

ALGORITHM 1: Key initialization

Input: Plain Image P
Output: K_1, K_2, K_3

```
Hash = SHA256(P)
Divide 256 bit hash into 8 parts (X1, X2, X3, X4, X5, X6, X7, X8)
K1 ← X1⊕ X2 & X3
K2 ← X3⊕ X4 & X7
K3 ← X5⊕ X6 & X8
N = 20
for i = 1:N do
    // 3D- LS with K1, K2, K3 as initial value
K1, K2, K3 = 3D-LS(K1, K2, K3)
endfor
Return K1, K2, K3
```

2.1 Key Initialization

The initial points of the 3D-LS map are generated by SHA-256. An image hash of 256-bit is computed and divided into eight parts (X_1 to X_8) of 32-bit each. Three sequences K_1, K_2, and K_3 are calculated by the Equation (1)

$$\begin{cases} K_1 = X_1 \oplus X_2 \,\&\, X_3 \\ K_2 = X_3 \oplus X_4 \,\&\, X_7 \\ K_3 = X_5 \oplus X_6 \,\&\, X_8 \end{cases} \tag{1}$$

The final initial points of the 3D-LS map are obtained by iterating K_1, K_2, and K_3 up to 20 times. The detailed key initialization scheme is described in Algorithm 1.

2.2 Generation of ORS

In this stage, an ORS is obtained through the GDWCN-PSO. This random number matrix and the Lorenz System are adopted to encrypt plain medical images, obtaining the cipher messages with a relationship to the plain images. The summary of the GDWCN-PSO process is given in Algorithm 2. With the GDWCN-PSO [20], the best velocity of global best particles is adopted in our algorithm to generate a random number matrix, which is further used to permute the image at the time of the encryption phase. To do this, we created a matrix with the logistic map as the initial position (X_k) of the particles and their velocity (V_k) is assigned at random. This method creates particles from the best-performing particles and destroys the worst-performing particles. To select the best performing parent, various parent selection methods are used, which are in the term used to create X offspring's particles. The summary of obtaining an ORS is given in Algorithm 3.

ALGORITHM 2: GDWCN-PSO

Input: Logistic Map Matrix LM
Output: Random Number Matrix

1. Initialization:
   Each particle with position according to LM,
   random V, Radius R and probability p
2. Compute global and local best fitness value for each particle.
3. **while** i ≤ n_gens do
4. Calculate global best
5. Connect every particle in R together
6. Connect particles outside R with p
7. **for** k = 0 to numParticles do
8. $V_k \leftarrow wV_k + c_1 r_1 \left(pb_k - X_k\right) + c_2 r_2 (pl_k - X_k)$
9. $X_k \leftarrow X_k + V_k$
10. Selection of best parents
11. Crossover to create X offspring
12. Replace the worst performers.
13. Increase the p.
14. i ++
15. **endfor**
16. Perform gaptest()
17. **endwhile**
18. def gaptest(a)
19. Max_distance = max distance between two different digits of key

Return velocities of global best particles

Additionally, we perform the *NIST SP 800-22* test [22] to verify the randomness of the sequence generated by the GDWCN-PSO. The "*P*" values of each test are listed in Table 1. We can observe that the sequence generated by the GDWCN-PSO passes all the tests. Hence, the generated sequence is both highly random and highly suitable for the secure encryption process.

2.3 Encryption and Decryption Process

We integrate an ORS and the 3D-LS to propose a secure and efficient encryption algorithm. The Lorenz system is mostly chaotic at every instance of the input. The proposed encryption process is performed using permutation and diffusion. Conventional permutation approaches just change the position of the pixels, resulting in a reasonable statistical analysis result. However, the confused image's intensity dispersal is identical to that of the original image. As a result, statistical attacks can be used against the conventional permutation approaches. To solve this issue, the suggested

Table 1. Analysis of Randomness of Sequence

Test	P value	Result
Entropy	0.998353	Pass
Serial	0.927639	Pass
Monobit	1	Pass
Binary matrix rank	0.07179	Pass
DFT	0.448095	Pass
Linear complexity	0.59439	Pass
Cumulative sums	0.983456	Pass
Non overlapping Template	1.000012	Pass
Overlapping Template	0.797783	Pass
Random excursion	0.018073	Pass
Random excursion variant	0.089845	Pass
Universal maurers	0.608154	Pass
Frequency	0.478697	Pass
Runs	0.848972	Pass
Longest run	0.608201	Pass

ALGORITHM 3: Obtaining Optimized Random Sequence

Input: key 256 bit Secret Key
Output: R Optimized Random Sequence
1. X, Y, Z = Key Intialization with key
2. K = X xor Y xor Z
3. Initializing the empty matrix L
4. For i = 0 to W×H−1 do
5. K = LogisticMap(K)
6. L[i] = K
7. Endfor
8. O = GDWCN-PSO (L)
// R is sorted index of optimized logistic map
9. [O, R] = sort(O)
Return R

GDWCN-PSO optimization permutation may not only change the value of the plain medical image but may also make it even harder to distinguish assaults. In the proposed confusion process, the image is flattened and pixels are swapped using ORS R as Equation (2) then rows and columns are circular shifted to obtain the permuted image. Equation (3) shows the circular shift operation

$$P(i, j) = P(R(i, j)) \tag{2}$$

$$\begin{cases} P(i) = Circular\ shift\ by\ R(i) \\ P(i,\ j) = Circular\ shift\ by\ R(m + j) \end{cases} \tag{3}$$

Confused image is defused by 3D-LS map [21] row-wise and then column-wise. The 3D-LS map is the collection of three nonlinear differential equations using Equation (4)

$$\begin{cases} A_{n+1} = \delta(B_n - A_n) \\ B_{n+1} = (\Psi - C_n)A_n - B_n \\ C_{n+1} = A_n \times B_n - \Upsilon \times C_n \end{cases} \tag{4}$$

Where, δ, Ψ, and Υ are the parameters of the Lorenz system, A_n, B_n, C_n and A_{n+1}, B_{n+1}, C_{n+1} are the previous and next state of the system, respectively. The system shows chaotic properties

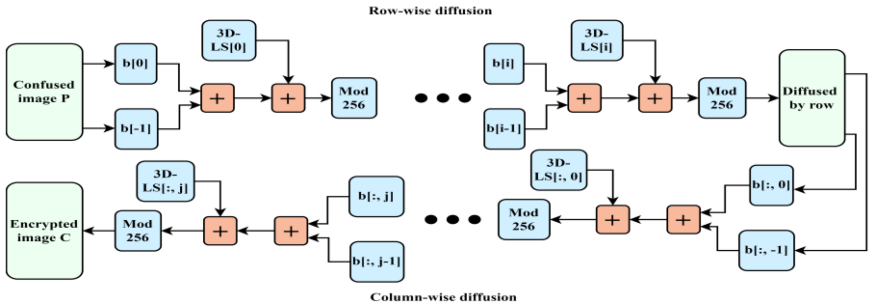

Fig. 3. Diffusion process.

when $\delta = 10$, $\Psi = 28$, and $\Upsilon = 8/3$. Positive Lyapunov exponents in the Lorenz system demonstrate its sensitivity to initial points and chaotic behaviour. The 3D-LS map is adopted in the proposed scheme for image diffusion. In Figure 3, the diffusion concept is given, and the summary of the encryption and decryption process is given in Algorithms 4 and 5, respectively.

3 EXPERIMENTAL RESULTS

This section described the simulation of the results of the proposed *EiMOL* algorithm. The experiment is performed on Python 3.9 with 8GB RAM and a 64-bit core i5-9300H processor. Different medical images are selected from benchmark Open-i [23] and Kaggle [24] datasets. Images of different sizes have been selected to evaluate the effectiveness of the proposed algorithm. Sample images used in the experiment are depicted in Figure 4. The random number matrix and the Lorenz System are adopted to encrypt plain medical images, obtaining the cipher messages with a relationship to the plain images. The visual effect of some images by our encryption algorithm is shown in Figure 5. It is observed that encrypted images are unrecognizable, and even permuted images are unidentifiable. This means that an attacker will not be able to deduce anything relevant about the plain image from the encrypted image. Therefore, the proposed encryption scheme is visually secure. In addition, statistical, differential, key analysis, robustness, and computational cost tests are performed to measure the strength and efficiency of the proposed *EiMOL* algorithm in the subsections below.

3.1 Statistical Analysis

In this section, the security performance of the *EiMOL* algorithm is evaluated from a statistical perspective.

(A) Histogram and chi-square test. Histogram evaluation is used to measure the effectiveness of an encryption scheme against statistical attacks. The histogram of an image represents the distribution of image pixels [25]. In particular, a good encryption scheme provides a uniform histogram of the cipher image. The histogram analysis of the proposed scheme is presented in Figure 6; the histogram of plain medical images (M-14 and M-15) is centered about particular gray levels, while the histogram of the corresponding encrypted image is evenly spread. Therefore, the suggested algorithm can efficiently withstand the histogram attack. Furthermore, A Chi-square test is performed to measure the uniformity in the histogram. A strong encryption scheme must have the χ^2 score less than the theoretical value i.e., 293.2478 [26]. χ^2 test is represented as

$$\chi^2 = \sum_{p=0}^{255} \left(\frac{\left(OF_p - EF_p\right)^2}{EF_p} \right) \tag{5}$$

ALGORITHM 4: Encryption

Input: Plain Image P, ORS R, 3D-LS L
Output: Cipher Image C
// Confusion
1. W, H = Size(P)
//Flatten Image to convert to 1-D array
2. C = Flatten(P)
3. for i = 0 to W×H −1 do
4. Swap C[i] and C[R[i]]
5. Endfor
6. C = Reshape to 2D array
7. for i = 0 to m do
8. Circular shift d[i] by R[i]
9. endfor
10. for i = 0 to n do
11. Circular shift d[:, i] by R[m+i]
12. endfor
// Diffusion
13. for i = 0 to 1 do
14. for r = 0 to H do
15. if r == 0 then
16. C[r,:] = (LS[r,:] + C[−1,:] + C[r,:]) mod 256
17. else if r >0 then
18. C[r,:] = (LS[r,:] + C[r−1,:] + C[r,:]) mod 256
19. Endif
20. endfor
21. for col = 0 to W do
22. if col == 0 do
23. C[:,col] = (LS[:,col]+ C[:,−1]+ C[:,col]) mod 256
24. else if col >0 do
25. C[:,col] = (LS[:,col]+ C[:,col−1]+ C [:,col]) mod 256
26. endif
27. endfor
28. endfor
Return C

ALGORITHM 5: Decryption

Input: Cipher Image C, 3D-LS L, ORS R
Output: Decrypted Image P
// De - Diffusion
1. w, h = Size(C)
2. for i = 0 to 1 do
3. for col = w−1 to 0 do
4. if col == 0 then
5. C[:, col] = (C[:,col] - LS[:,col] - C[:,−1]) mod 256
6. else if col >0 do
7. C[:,col] = (C[:,col] - C[:,col−1] − LS[:,col]) mod 256
8. endif
9. endfor
10. for r = h−1 to 0 do
11. if r == 0 do
12. C[r, :] = (C[r, :] - LS[r, :] - C[−1, :]) mod 256
13. else if r >0 then
14. C[r,:] = (C[r,:] - LS[r,:] - C[r−1,:]) mod 256
15. endif
16. Endfor
17. endfor
// De - Confusion
// Flatten Image to convert to 1-D array
18. C = Flatten(C)
19. for i = 0 to n do
20. Circular shift d[:, i] by -R[m+i]
21. Endfor
22. for i = 0 to m do
23. Circular shift d[i] by -R[i]
24. endfor
25. for i = W × H−1 to 0 do
26. Swap C[i] and C[R[i]]
27. Endfor
28. P = Reshape to 2D array
Return P

where, OF_p: observed frequency of each intensity. EF_p expected frequency of each intensity. Table 2 shows the result of χ^2 test analysis. We have performed χ^2 test on all 20 images. It can be observed that all scores are less than the theoretical score.

(B) Correlation Analysis. There is a high correlation exists among neighbouring pixels in medical images. A good encryption scheme should be able to efficiently reduce the high correlation [27]. In most cases, the correlation coefficient is used to assess the degree of correlation between neighbouring pixels in an image. Horizontal (H), vertical (V), and diagonal (D) correlation coefficient is mathematically described as

$$Col_{x,y} = \frac{Avg\left[(x - Avg(x))(y - Avg(y))\right]}{\sqrt{Var(x)\ Var(y)}}, \tag{6}$$

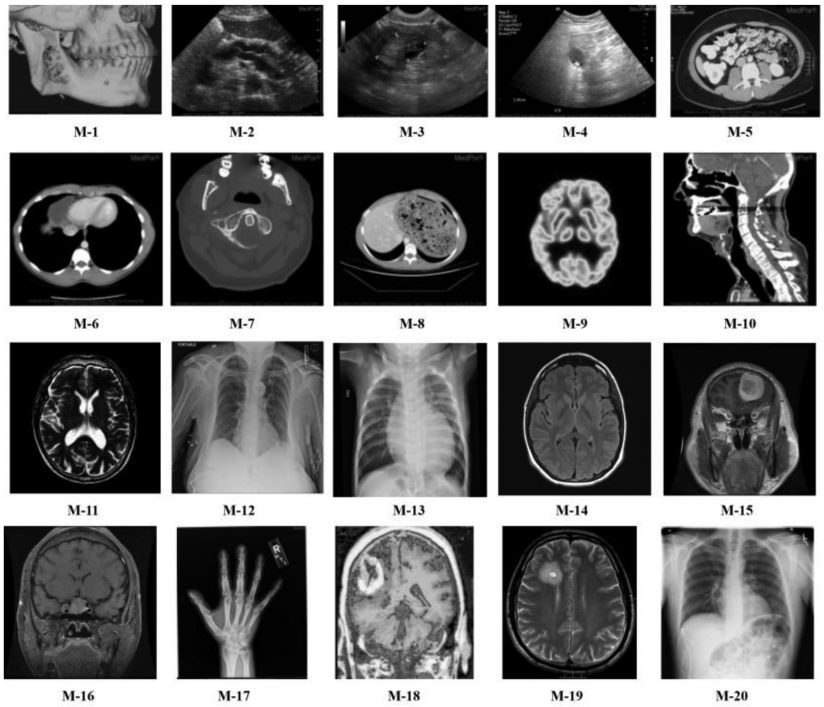

Fig. 4. Sample images.

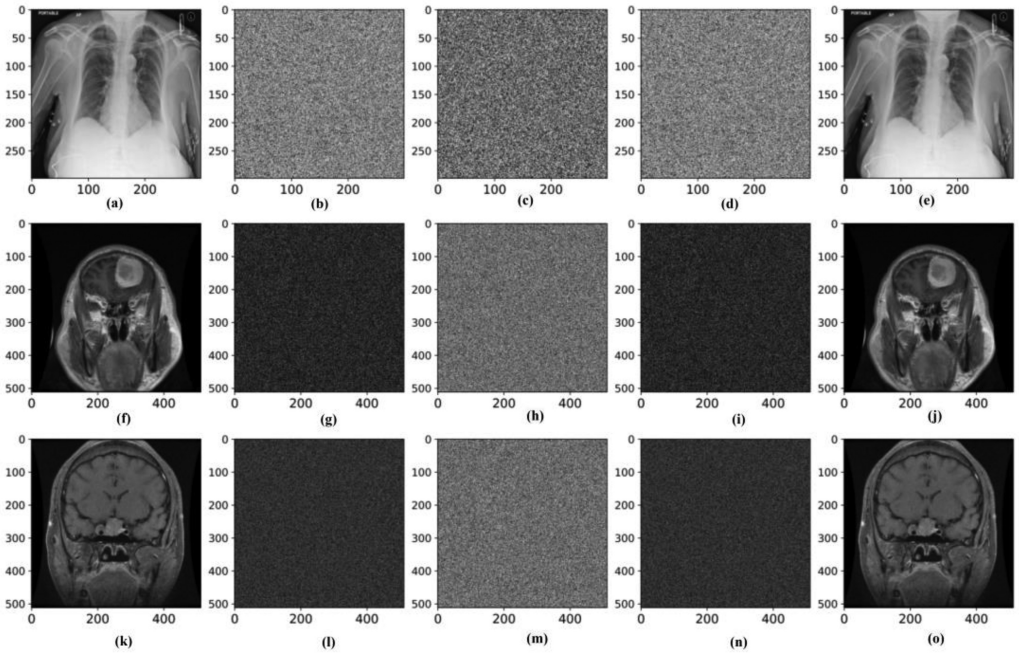

Fig. 5. (a), (f), (k): Plain images (M-12, M-15, M-16). (b),(g), (f): corresponding permuted images. (c), (h), (m) corresponding encrypted images. (d), (i), (n): corresponding de-diffused images. (e), (j), (o): corresponding decrypted images.

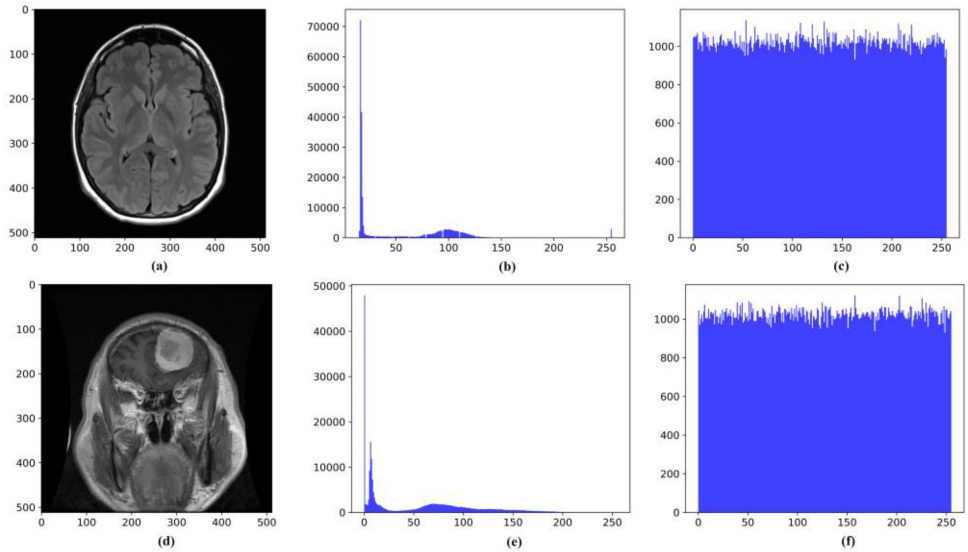

Fig. 6. (a), (d): Plain images. (b), (e): histogram of plain images (c), (f): corresponding histogram of encrypted images.

Table 2. χ^2 Test Analysis

Image	χ^2 Value	Decision	Image	χ^2 Value	Decision
M-1	272.7045	Pass	M-11	231.0156	Pass
M-2	214.2615	Pass	M-12	260.2074	Pass
M-3	284.8423	Pass	M-13	251.3248	Pass
M-4	211.3398	Pass	M-14	283.3125	Pass
M-5	263.7739	Pass	M-15	243.4141	Pass
M-6	276.8775	Pass	M-16	243.5586	Pass
M-7	290.1362	Pass	M-17	278.1067	Pass
M-8	261.0852	Pass	M-18	279.2546	Pass
M-9	235.9219	Pass	M-19	223.6503	Pass
M10	279.4489	Pass	M-20	266.2031	Pass

$$Avg\,(x) = \frac{1}{M}\sum_{i=1}^{M} x_j, \tag{7}$$

$$Var(y) = \frac{1}{M}\sum_{i=1}^{M} (x_i - Avg(x))^2. \tag{8}$$

Where $Col_{x,y}$ represents the correlation between pixels x and y. $Avg(x)$ and $Var(y)$ represents the mean and variance of pixels respectively. Generally, the correlation coefficient varies from -1 to 1. Correlation score 1 indicates the high correlation between image pixels pair. We have selected 5,000-pixel pairs to measure the correlation coefficient in each direction. The correlation analysis of our proposed scheme is presented in Table 3. As demonstrated in this table, all correlation coefficient scores of encrypted images are very close to zero. Hence, the proposed scheme effectively reduces the correlation between neighbouring pixels. Furthermore, we also compared the results of the proposed scheme with recent encryption techniques [14–16], [19], and [28] in this table, which shows that our scheme's result is better than most other encryption schemes.

Table 3. Correlation Coefficients of the Plain and Encrypted Image

Method	Image	Plain Image Correlation			Encrypted Image Correlation		
		H	V	D	H	V	D
EiMOL	M-1	0.97804	0.99121	0.97577	−0.01376	−0.01453	−0.00688
	M-2	0.95474	0.92474	0.89496	−0.00857	0.01904	−0.02571
	M-3	0.95439	0.94125	0.91559	0.01790	0.00461	−0.01300
	M-4	0.97305	0.96598	0.95436	−0.01482	−0.00180	−0.02218
	M-5	0.96011	0.93669	0.91262	−0.00911	0.01015	−0.00346
	M-6	0.96026	0.93562	0.90905	−0.01825	0.03081	−0.01308
	M-7	0.94948	0.95059	0.92707	0.00587	−0.02037	−0.03131
	M-8	0.96305	0.92967	0.91264	0.00373	−0.01284	0.00637
	M-9	0.99560	0.99708	0.99172	−0.01779	−0.02185	0.01523
	M-10	0.93627	0.94054	0.90445	−0.00372	0.00099	0.00389
	M-11	0.92027	0.92127	0.86793	0.00367	0.02238	−0.00325
	M-12	0.98332	0.98811	0.97467	0.02122	−0.00459	−0.02711
	M-13	0.99456	0.99810	0.99218	−0.02444	−0.02794	0.00469
	M-14	0.98042	0.99161	0.97420	−0.02422	−0.00910	0.00294
	M-15	0.99412	0.99304	0.98791	0.03136	−0.00048	−0.02061
	M-16	0.98186	0.98710	0.97112	0.00254	−0.00343	0.01069
	M-17	0.93875	0.96111	0.91187	−0.02528	0.00661	−0.02226
	M-18	0.96546	0.99041	0.95706	0.02832	0.01029	0.02628
	M-19	0.98613	0.97543	0.96428	0.00820	0.00646	−0.01212
	M-20	0.99856	0.99619	0.99444	0.01319	0.00785	−0.00949
[14]	Medical				0.001018	0.000176	0.001586
[15]	Peppers				-21×10^{-6}	-13×10^{-5}	-28×10^{-6}
[16]	Peppers	0.9800	0.9750	0.9604	−0.0027	0.0014	−0.0034
[19]	CT_abdomen0	0.994393	0.996926	0.992866	−0.002151	−0.002660	−0.003474
[28]	OPENi4	0.9803	0.9803	0.9688	0.0048	−0.0012	−2.3609e-04

The correlation between nearby pixels is typically shown using a scatterplot. We plot the correlation of plain image M-1 and M-19 in the horizontal, vertical, and diagonal directions in Figure 7(b), (c), (d), (j), (k), and (l), and their corresponding encrypted image's correlation is shown in Figure 7(f), (g), (h) and (n), (o), (p), respectively. We can see from this figure that the neighbouring pixels in the plain images are strongly correlated, whereas the uniformly scattered distribution findings in Figure 7(f)–(h) and (n)–(p) show that the adjacent pixels in the encrypted image have essentially no correlation. This property of the encryption scheme can withstand Statistical attacks, which provides better security against hackers.

(C) Entropy Analysis. A strong image encryption scheme should be able to conceal the statistical information contained in plain images. Information entropy is utilized to scale the degree of randomness in an image. An entropy score of 8 for a grayscale image represents the highest degree of randomness in the image [29]. Information entropy is defined as

$$Ent(X) = -\sum_{l=0}^{255}(P(X_l) \times \log_2 P(X_l)). \tag{9}$$

Where the probability of pixel (X_l) is represented as $P(X_l)$ and entropy of image as $Ent(X)$. Entropy analysis of *EiMOL* scheme is depicted in Table 4. The result of the entropy score describes that we obtain a maximum entropy score of 7.99933 for the image M-16 and a minimum entropy of

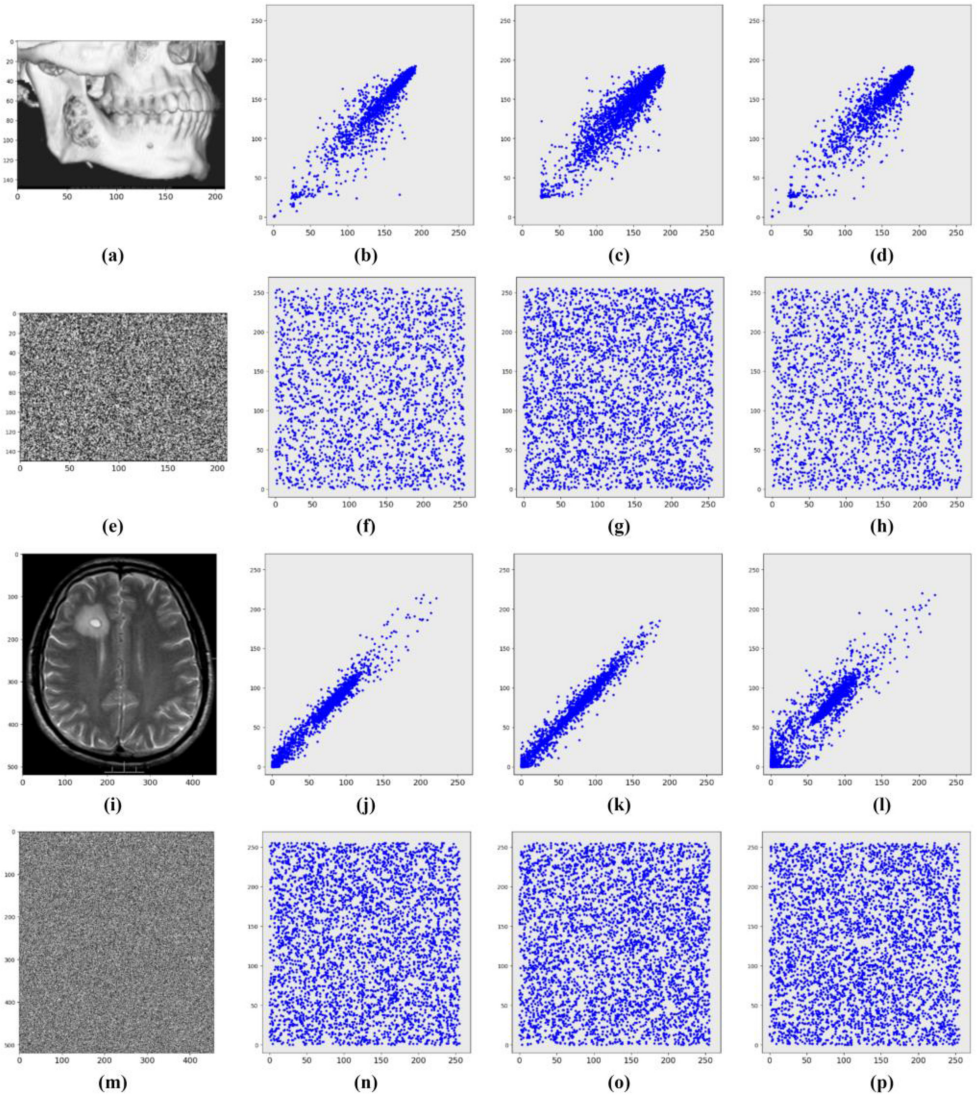

Fig. 7. (a), (i): Plain images. (e), (m): corresponding encrypted images. (b)–(d): correlation coefficient of (a) in H, V, and D direction. (f)–(h): correlation coefficient of (e) in H, V, and D direction. (j)–(l): correlation coefficient of (i) in H, V, and D direction. (n)–(p): correlation coefficient of (m) in H, V, and D direction.

7.98942 for the image M-17, while the average entropy score for the 20 medical images is 7.99548. The simulation results show that our scheme achieves an entropy score that is very close to the optimal entropy value. Moreover, comparison results with Reference [14–16], [19] and [28] also show the superiority of our proposed scheme. Therefore, the proposed scheme provides the highest level of randomness in cipher images and is protected against entropy attacks.

3.2 Differential Attack Analysis

A robust encryption scheme should be highly sensitive to a very minor change in a plain image. For example, if there is even a slight difference between two plain images, an ideal encryption process

Table 4. Entropy Analysis

Method	Image	Original Entropy	Encrypted Entropy	Image	Original Entropy	Encrypted Entropy
EiMOL	M-1	6.310824	7.993739	M-11	4.494498	7.99745
	M-2	6.549544	7.994952	M-12	7.521828	7.997895
	M-3	6.319574	7.993155	M-13	7.129090	7.997962
	M-4	5.821718	7.995275	M-14	5.138086	7.999223
	M-5	7.053709	7.993634	M-15	6.373161	7.999329
	M-6	3.940155	7.991091	M-16	6.736475	7.999331
	M-7	5.319478	7.990307	M-17	5.493418	7.989421
	M-8	3.928677	7.991631	M-18	7.752448	7.998218
	M-9	4.10926	7.997413	M-19	5.847754	7.999318
	M10	5.472093	7.991004	M-20	7.697953	7.999266
[14]	Medical		7.9889			
[15]	Peppers		7.9995			
[16]	Lena		7.9994			
[19]	CT_abdomena	5.782	7.9913			
[28]	OPENi4		7.9971			

should produce completely different cipher images. Otherwise, a differential attack is possible on the encryption system.

The differential attack is assessed by two parameters the **number of pixel change rate** (**NPCR**), and the **unified average changing intensity** (**UACI**) which are mathematically defined as

$$NPCR = \frac{1}{H \times W} \sum_{x,y} T(x,y) \times 100\%, \tag{10}$$

$$UACI = \frac{1}{H \times W} \sum_{x,y} \frac{|U(x,\ y) - U'(x,\ y)|}{255} \times 100\%, \tag{11}$$

$$T(x,y) = \begin{cases} 0, & if\ U(x,\ y) = U'(x,\ y) \\ 1, & if\ U(x,\ y) \neq U'(x,\ y) \end{cases}. \tag{12}$$

Where the height and width of the image are H and W, respectively, $U(x,\ y)$: encrypted plain image and $U'(x,\ y)$: encrypted slightly changed plain image. A strong encryption scheme shows the ideal value of NPCR and UACI as 99.6094% and 33.4635%, respectively [30]. We analyze the NPCR and UACI scores in Table 5. By testing 20 medical images, we found the average NPCR and UACI scores to be 99.6091% and 33.4788%, respectively, which are equal to the ideal values. Furthermore, each image's NPCR and UACI scores are also very close to theoretical values. Hence, the proposed scheme is able to effectively resist the differential attacks. We also compare the result of the *EiMOL* scheme with the schemes in References [14–16], [19], and [28], which indicate that the proposed scheme provides better results to withstand the differential attack.

3.3 Key Space Analysis

Any image cryptosystem should have a large key space to resist the brute-force attack, which consists of trying every possible permutation of a key in a defined key space. An encryption scheme with small a key space can easily be cracked by an attacker. A key space must be greater than 2100 to efficiently withstand a brute-force attack [31].

Table 5. Analysis of Differential Attack

Method	Image	NPCR	UACI	Image	NPCR	UACI
EiMOL	M-1	99.6197	33.5055	M-11	99.6307	33.5387
	M-2	99.6000	33.4855	M-12	99.6239	33.3746
	M-3	99.6053	33.4329	M-13	99.5864	33.5028
	M-4	99.6211	33.4920	M-14	99.6055	33.4312
	M-5	99.6040	33.4130	M-15	99.6028	33.4423
	M-6	99.6213	33.4832	M-16	99.6155	33.4589
	M-7	99.6222	33.5869	M-17	99.6031	33.6063
	M-8	99.6009	33.5688	M-18	99.6216	33.4844
	M-9	99.5908	33.3558	M-19	99.6096	33.4541
	M-10	99.5902	33.4555	M-20	99.6076	33.5030
[14]	Medical	99.69	33.4821			
[15]	Peppers	99.6087	33.4679			
[16]	Peppers	99.6109	33.4828			
[19]	CT_abdomen4	0.99205	0.33443			
[28]	OPENi4	99.6155	33.5477			

The suggested encryption approach generates the key for confusion and diffusion using a 256-bit secret key and a 256-bit hash, resulting in a total key space of 2512, which is substantially larger than 2100. Therefore, the proposed scheme is highly secure against brute-force attacks.

3.4 Key Sensitivity Analysis

A qualified cryptosystem must be very sensitive to its encryption key. That is, changing one bit in the encryption key should yield a completely different decrypted image. Evaluation is done by using two keys, one of which is the original (k1) and the other (k2) of which has been changed by one bit. The result is shown in Figure 8. Figure 8(b) and (c) represent the result of encryption by key k1 and k2, respectively. Figure 8(d) and (e) depict the result of the decryption by key k1 and k2, respectively, which were encrypted by key k1, indicating that a minor changed key is not able to decrypt the image. Furthermore, we also calculated the difference between two cipher images 8(b) and 8(c), which was 99.6189%. Therefore, the EiMOL encryption scheme's key sensitivity is very high.

3.5 Classical Attack Analysis

Practically, **ciphertext only** (**CA**), **known-plaintext** (**KPA**), **chosen-plaintext** (**CPA**), and **chosen-ciphertext** (**CCA**) are the most prevalent classical attacks, CPA is one of the most powerful attacks among them. If an encryption scheme withstands CPA, it can also resist all of the other three attacks [32]. When perfect black and perfect white images are effectively confused and diffused, the encryption method is considered effective against CPA attacks [33]. To test resistance to the CPA attack, we encrypt perfect black and perfect white images, the result of which is shown in Figure 9. It is clear from this figure that the proposed scheme effectively confuses and diffuses the perfect black and white images. Also, the histogram of encrypted images is uniform. Hence, the proposed scheme is qualified to resist the CPA attack.

3.6 Computational Complexity

An encryption system with strong security and a short processing time is qualified for real-world applications. To measure the computational efficiency, we have calculated the encryption time

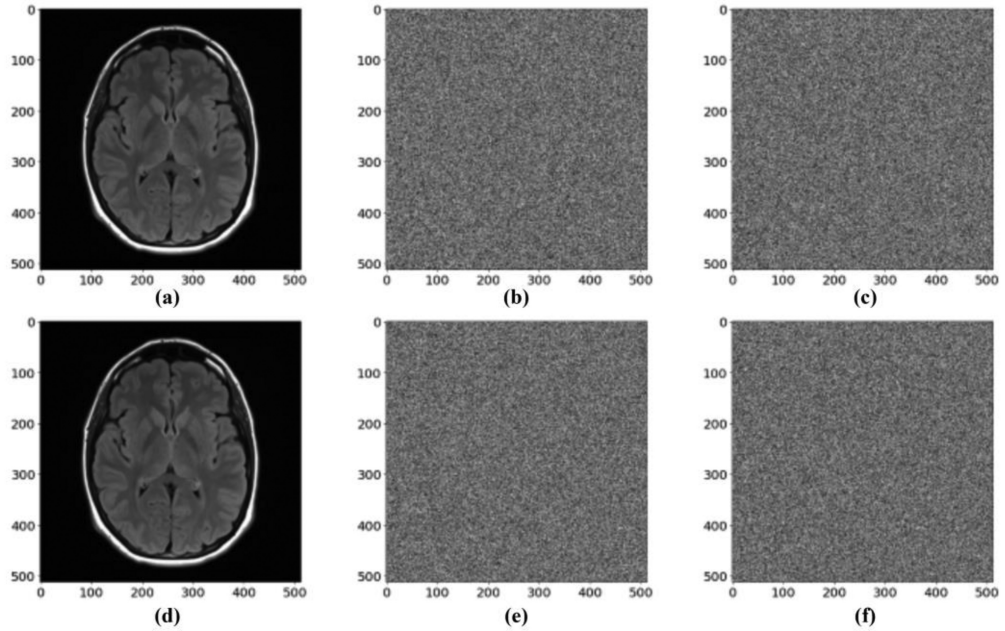

Fig. 8. (a): plain image (M-14). (b): image encrypted by k_1. (c): image encrypted by K_2 (d): decrypted image (enc: k_1, dec: k_1). (e): decrypted image (enc: k_1, dec: k_2). (f): difference of (b) and (c).

Table 6. Time Cost Analysis

Method	Image	Size	Enctime (sec)	Dectime (sec)	Image	Size	Enctime (sec)	Dectime (sec)
EiMOL	M-1	210 × 150	0.408634	0.408246	M-11	256 × 256	0.103581	0.094526
	M-2	205 × 150	0.057086	0.057855	M-12	299 × 299	0.116935	0.126807
	M-3	201 × 150	0.042433	0.046155	M-13	299 × 299	0.161003	0.137896
	M-4	215 × 150	0.040542	0.040275	M-14	512 × 512	0.328286	0.332152
	M-5	200 × 150	0.038436	0.038086	M-15	512 × 512	0.309726	0.317866
	M-6	150 × 150	0.03368	0.034151	M-16	512 × 512	0.361162	0.37443
	M-7	150 × 150	0.028818	0.029349	M-17	128 × 150	0.088897	0.078829
	M-8	150 × 150	0.030252	0.03136	M-18	321 × 352	0.152975	0.14999
	M-9	256 × 256	0.086462	0.087085	M-19	456 × 519	0.296313	0.301251
	M10	150 × 150	0.035165	0.034889	M-20	512 × 512	0.303707	0.31044
[14]	Medical	256 × 256	7.9889					
[15]	–	512 × 512	0.205					
[16]	Lena	512 × 512	0.4219					
[19]	–	–	NA					
[28]	OPENi4	256 × 256	3.9					

(Enctime) and decryption time (Dectime) of the proposed scheme. We test the different sizes of images to measure the processing time of the *EiMOL* scheme. The key generation, permutation, and diffusion time of the M-9 image are shown in Figure 10, and the encryption and decryption time for 20 medical images are depicted in Table 6. The average encryption time for the image of sizes 150 × 150, 256 × 256, and 512 × 512 are 0.031979 sec, 0.095021 sec, and 0.325720 sec, respectively. This

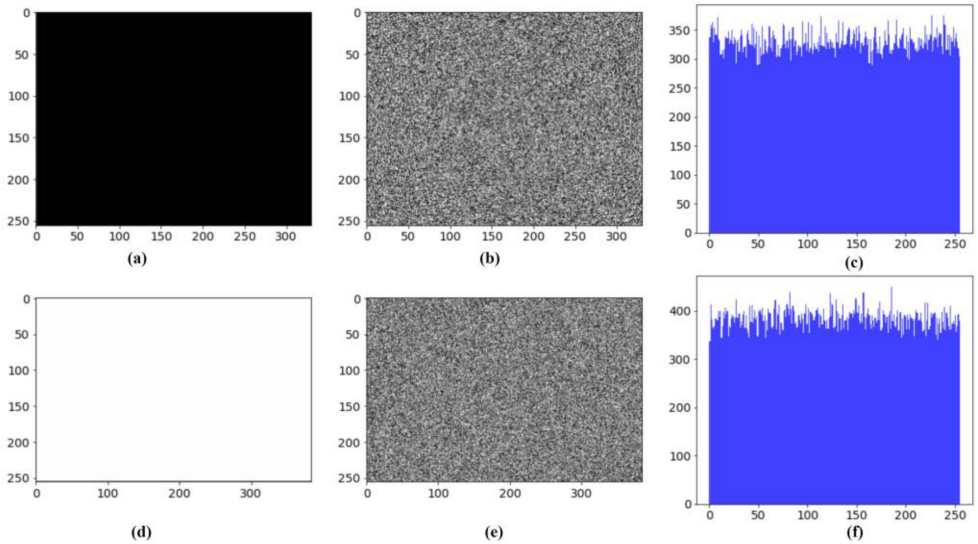

Fig. 9. (a), (d): Perfect black and perfect white images. (b), (e): Encrypted images corresponding to (a) and (d). (c), (f): histogram of (b) and (e).

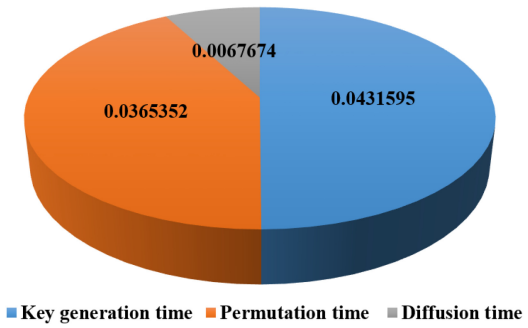

Fig. 10. Processing time of each step (sec).

analysis verifies that our scheme takes much less time to encrypt and decrypt the digital images, making it suitable for real-time applications. Furthermore, encryption and decryption time is also compared with References [14–16], [19], and [28]. The efficiency of our scheme is better than most of the other schemes. Hence, the proposed scheme is computationally efficient.

3.7 Robustness Analysis.

During data transfer across the network, noise interference or partial data loss can corrupt the encrypted image. Therefore, a better encryption scheme must be robust against various noise and data loss. To test the robustness of the proposed scheme, salt and pepper noise and Gaussian noise of different strengths are added to the encrypted image, and then we analyse the quality of the decrypted image. Figure 11(a), (b) and (c) represents the decryption result of salt and pepper noise of strength 1%, 0.5% and 0.1%, respectively. Furthermore, Figure 11(d), (e) and (f) represents the decrypted image with a Gaussian noise of strength 1%, 0.5% and 0.1%, respectively. The visual quality of the decrypted image indicates that our scheme is very robust against noise. Table 7 represents the robustness analysis of the decrypted image. We can see that for 0.1%, the Gaussian noise **peak**

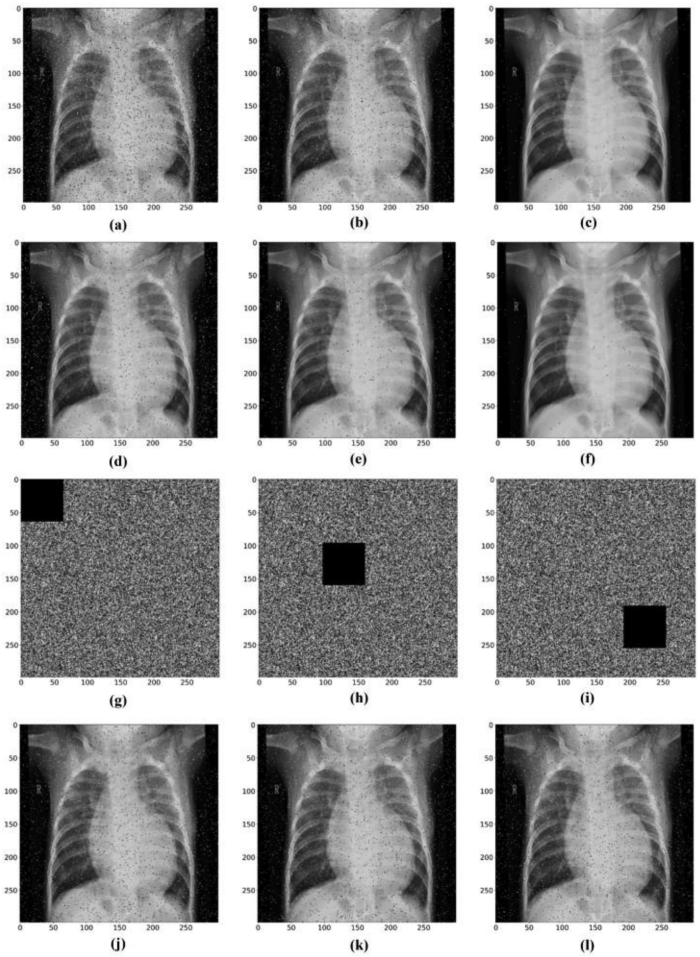

Fig. 11. (a), (b), (c): decrypted image with S&P noise intensities 1%, 0.5%, 0.1%. (d), (e), (f): decrypted image with Gaussian noise intensities 1%, 0.5%, 0.1%. (g), (h), (i): Clipping of 1/16 part at different position of the encrypted image. (j), (k), (l): decrypted images with clipping attack.

signal to noise ratio (**PSNR**) is 30.20. We also measure the effects of data loss in the encrypted image.

Figure 11(g), (h), and (i) shows the 1/16 data loss encrypted images at the left corner, middle and lower right, respectively, and their corresponding decrypted images are shown in Figure 11(j), (k), and (l). The PSNR value of 1/16, 1/32 and 1/64 data loss are listed in Table 7, and the result of the data loss analysis shows that the proposed scheme provides a high-quality decrypted image. Therefore, the scheme is robust against a data loss attack.

4 CONCLUSION

In this article, a secure medical image encryption algorithm, called *EiMOL*, based on optimization and the Lorenz system, has been proposed. In the first stage, an ORS is obtained by utilizing the GDWCN-PSO and a logistic map for the secure encryption process. The randomness of the sequence obtained from the GDWCN-PSO is tested for *NIST SP 800-22* test. Hence, the

Table 7. Robustness Analysis

Noise/Clipping position	Noise strength/ Clipping portion	PSNR (db)
Salt & pepper	1%	18.34
	0.50%	21.2
	0.10%	28.38
Gaussian	1%	20.21
	0.50%	23.17
	0.10%	30.20
Upper left	1/16	20.92
Middle		20.96
Lower right		20.85
Upper left	1/32	23.77
Middle		23.76
Lower right		23.69
Upper left	1/64	26.66
Middle		26.56
Lower right		26.65

generated sequence is highly random and highly suitable for the secure encryption process. After that, this random number matrix and the Lorenz system are adopted to encrypt plain medical images, obtaining the cipher messages with a relationship to the plain images. Extensive simulation and testing results are performed to demonstrate that the *EiMOL* algorithm in this articleis secure, which will be useful for smart healthcare applications. Further, the outcomes on real-world datasets demonstrate that the proposed algorithm outperforms the state-of-the-art approaches. The proposed *EiMOL* algorithm can be improved with efficient deep-learning models in the near future.

ACKNOWLEDGEMENTS

This work is supported by seed project entitled "Robust and Secure Copyright Protection Techniques for E-Government Document," order no. NITP/1457/19 dt. 13 June, 2019, NIT Patna, Bihar, India.

REFERENCES

[1] M. N. Bhuiyan, M. M. Rahman, M. M. Billah, and D. Saha. 2021. Internet of things (IoT): A review of its enabling technologies in healthcare applications, standards protocols, security, and market opportunities. *IEEE Internet of Things Journal* 8, 13 (2021), 10474–10498.

[2] A. K. Singh, A. Anand, Z. Lv, H. Ko, and A. Mohan. 2021. A survey on healthcare data: A security perspective. *ACM Transactions on Multimedia Computing Communications and Applications* 17, 2s (2021), 1–26.

[3] K. Amine, K. Fares, K. M. Redouane, and E. Salah. 2022. Medical image watermarking for telemedicine application security. *Journal of Circuits, Systems, and Computers* 31, 5 (2022), 2250097.

[4] N. Sharma, O. P. Singh, A. Anand, and A. K. Singh. 2021. Improved method of optimization-based ECG signal watermarking. *Journal of Electronic Imaging* 31, 4 (2021), 041207.

[5] D. Ravichandran, S. A. Banu, B. K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan. 2021. An efficient medical image encryption using hybrid DNA computing and chaos in transform domain. *Medical and Biological Engineering and Computing* 59, 3 (2021), 589–605.

[6] O. P. Singh, Amit Kumar Singh, A. K. Agrawal, and Huiyu Zhou. 2022. SecDH: Security of COVID-19 images based on data hiding with PCA. *Computer Communications* 191 (2022), 368–377.

[7] A. Anand and A. K. Singh. 2022. Hybrid nature-inspired optimization and encryption-based watermarking for E-Healthcare. *IEEE Transactions on Computational Social Systems* (2022), 1–8.

[8] B. Wang, J. Shi, W. Wang, and P. Zhao. 2022. Image copyright protection based on blockchain and zero-watermark. *IEEE Transactions on Network Science and Engineering* 9, 4 (2022), 2188–2199.
[9] F. Masood, M. Driss, W. Boulila, J. Ahmad, S. U. Rehman, S. U. Jan, A. Qayyum, and W. J. Buchanan. 2021. A light-weight chaos-based medical image encryption scheme using random shuffling and XOR operations. *Wireless Personal Communications* (2021), 1–28.
[10] M. Shamim Hossain, Rita Cucchiara, Ghulam Muhammad, Diana P. Tobón, and Abdulmotaleb El Saddik. 2022. Special section on AI-empowered multimedia data analytics for smart healthcare. *ACM Transactions on Multimedia Computing, Communications, and Applications* 18, 1s (2022), 38.
[11] M. Kaur and D. Singh. 2021. Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption. *Multidimensional Systems and Signal Processing* 32, 1 (2021), 281–301.
[12] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, S. Rajagopalan, R. Amirtharajan, and N. Chidambaram. 2021. Neural-assisted image-dependent encryption scheme for medical image cloud storage. *Neural Computing and Applications* 33, 12 (2021), 6671–6684.
[13] X. Chai, J. Fu, Z. Gan, Y. Lu, and Y. Zhang. 2022. An image encryption scheme based on multi-objective optimization and block compressed sensing. *Nonlinear Dynamics* 108, 3 (2022), 2671–2704.
[14] S. Saravanan and M. Sivabalakrishnan. 2021. A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption. *Soft Computing* 25, 7 (2021), 5299–5322.
[15] A. Toktas and U. Erkan. 2022. 2D fully chaotic map for image encryption constructed through a quadruple-objective optimization via artificial bee colony algorithm. *Neural Computing and Applications* 34, 6 (2022), 4295–4319.
[16] Y. Luo, X. Ouyang, J. Liu, L. Cao, and Y. Zou. 2022. An image encryption scheme based on particle swarm optimization algorithm and hyperchaotic system. *Soft Computing* 26, 11 (2022), 5409–5435.
[17] S. Yin and H. Li. 2021. GSAPSO-MQC:Medical image encryption based on genetic simulated annealing particle swarm optimization and modified quantum chaos system. *Evolutionary Intelligence* 14, 4 (2021), 1817–1829.
[18] V. Bharadwaj, A. Lakshman, G. Bhatnagar, and C. Chattopadhyay. 2022. A novel security framework for medical data in IoT ecosystem. *IEEE MultiMedia* 29, 02 (2022), 34–44.
[19] W. Song, C. Fu, Y. Zheng, L. Cao, and M. Tie. 2022. A practical medical image cryptosystem with parallel acceleration. *Journal of Ambient Intelligence and Humanized Computing* (2022), 1–15.
[20] Vandana Bharti, Bhaskar Biswas, and Kaushal Kumar Shukla. 2021. A novel multiobjective gdwcn-pso algorithm and its application to medical data security. *ACM Transactions on Internet Technology* 21, 2 (2021), 1–28.
[21] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari. 2019. Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. *Neural Computing and Applications* 31, 7 (2019), 2395–2405.
[22] L. G. Nardo, E. G. Nepomuceno, J. Arias-Garcia, and D. N. Butusov. 2019. Image encryption using finite-precision error. *Chaos, Solitons and Fractals* 123 (2019), 69–78.
[23] https://openi.nlm.nih.gov/gridquery?it=c,xg,m,u&m=1&n=100.
[24] https://www.kaggle.com/datasets/navoneel/brain-mri-images-for-brain-tumor- detection.
[25] Xing-Yuan Wang, Ying-Qian Zhang, and Xue-Mei Bao. 2015. A novel chaotic image encryption scheme using DNA sequence operations. *Optics and Lasers in Engineering* 73 (2015), 53–61.
[26] G. Ye, C. Pan, X. Huang, and Q. Mei. 2018. An efficient pixel-level chaotic image encryption algorithm. *Nonlinear Dynamics* 94, 1 (2018), 745–756.
[27] A. Souyah and K. M. Faraoun. 2016. An image encryption scheme combining chaos-memory cellular automata and weighted histogram. *Nonlinear Dynamics* 86, 1 (2016), 639–653.
[28] Parsa Sarosh, Shabir A. Parah, and G. Mohiuddin Bhat. 2022. An efficient image encryption scheme for healthcare applications. *Multimedia Tools and Applications* 81, 5 (2022), 7253–7270.
[29] K. N. Singh and A. K. Singh. 2022. Towards integrating image encryption with compression: A survey. *ACM Transactions on Multimedia Computing, Communications, and Applications* 18, 3 (2022), 1–21.
[30] Y. Wu, J. P. Noonan, and S. Agaian. 2011. NPCR and UACI randomness tests for image encryption. *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications* 1, 2 (2011), 31–38.
[31] G. Alvarez and S. Li. 2006. Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos* 16, 8 (2006), 2129–2151.
[32] X. Wang, L. Teng, and X. Qin. 2012. A novel colour image encryption algorithm based on chaos. *Signal Processing* 92, 4 (2012), 1101–1108.
[33] U. Hayat and N. A. Azam. 2019. A novel image encryption scheme based on an elliptic curve. *Signal Processing* 155 (2019), 391–402.

Received 29 June 2022; revised 10 August 2022; accepted 1 September 2022