



Research Article

Securing E-Healthcare Images Using an Efficient Image Encryption Model

Jaishree Jain ^{1,2} and Arpit Jain ³

¹Computer Science & Engineering, TMU, Moradabad, India

²Department of Computer Science and Engineering, AKGEC, Ghaziabad, India

³Computer Science & Engineering, TMU, Moradabad, India

Correspondence should be addressed to Jaishree Jain; jaishree3112@gmail.com

Received 5 December 2021; Revised 2 January 2022; Accepted 11 January 2022; Published 8 March 2022

Academic Editor: Punit Gupta

Copyright © 2022 Jaishree Jain and Arpit Jain. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the advancements in e-healthcare services, it is possible to provide remote medical services to patients and swifter first aid. Medical images play an essential role in e-healthcare applications for providing quick and better remote diagnosis and treatment to patients. Medical images generally comprise secret details about the patients and are therefore prone to various security threats during their transmission over public networks. Thus, it is required to secure these images prior to their communication over public networks. But due to distinctive properties of medical images, like higher correlation and redundancy among the pixels, and larger size, it is required to design an efficient encryption model to resist against various security threats. In this paper, an efficient encryption model for medical images is proposed. To obtain the secret keys, six-dimensional hyperchaotic map (SDHM) is proposed. Firstly, plain medical image is divided into three channels such as red, green, and blue. Secret keys are used to diffuse these channels. Lastly, encrypted channels are concatenated and final encrypted medical image is obtained. Extensive experiments are drawn by considering the benchmark medical images. Also, comparisons are performed among the proposed SDHM and competitive techniques by considering various performance metrics. Comparative analysis reveals that the proposed SDHM achieves remarkably good performance than the existing encryption models.

1. Introduction

With the advancements in multimedia applications, images are playing very crucial role in various applications. One of the most important applications is e-healthcare. Due to digitalization, the communication among the doctors and patients becomes very easy. The doctors from distant areas can collaborate and work together. The e-health has wide range of applications such as drug-synergy prediction, disease diagnosis, digital surgery, telemedicine, and telehealth. Generally, healthcare data are transmitted over public networks which may cause various security threats. In this paper, we focused only on medical images. The communication and storage of medical images over the public networks is not secure. The primary concerns of medical images are authentication, confidentiality, and integrity. The security vulnerabilities of medical images can pose various

threats that further restrict the development of mobile healthcare applications [1, 2]. Therefore, it is required to protect the medical images while communication and storage. Image encryption is one the information security models that can be utilized to protect the medical images.

Many researchers have used chaotic maps to protect the medical images. The strength of the encryption model always lies on the secret keys. To produce secret keys, chaotic maps are extensively utilized. In [1], logistic map, cubic map, and sine map were used to secure the medical images. In [3], edge and chaotic maps were used to encrypt the medical images. In [4], secret key was obtained using double humped (DH) logistic map to encrypt the medical MRI and X-ray images. In [5], logistic-sine chaotic map was used to permute the original image. Then, image was divided into blocks, and the blocks were encrypted using hyperchaotic map. In [6], medical images were encrypted using the ElGamal

cryptosystem. The secret key was obtained using Mersenne Twister pseudo-random number generator. In [7], sine map and Rossler dynamical systems were utilized to secure the medical images.

Chaotic encryption models come under spatial-domain models. In spatial-domain models, operations are directly applied on the plain image. To make medical image encryption models more secure, many researchers combined spatial and frequency domain models. In [8], cosine number transform was applied to protect the medical images. In [9], fuzzy chaotic map was used to encrypt the images along with discrete wavelet transform (DWT). In [10], medical images were protected using cosine number transform. In [11], edge maps and DWT were used to encrypt the medical images. In [12, 13], integer wavelet transform (IWT), DNA, and 3D Lorenz chaotic map were utilized to secure the medical images over public networks.

There are many other concepts which have been utilized to protect the medical images. One of them is homomorphic encryption. It allows to perform the operations on medical images stored in cloud storage without compromising the confidentiality [14]. However, the use of homomorphic encryption is computationally expensive. The combination of encryption and watermarking models was also applied to improve the security and reliability [15, 16]. The concept of optimization is also utilized by many researchers in the field of image encryption. The optimization algorithms help in selection of optimized encrypted image [17–19]. However, the selection of optimization algorithm and fitness function is very challenging. Along with this, optimization algorithms are very time consuming. The concept of compression was also used to reduce the processing time [20]. Compression may reduce the quality of medical images that is not acceptable in medical field where minute details are very important [21–23].

It is found that the medical images generally comprise secret details about the patients and are therefore prone to various security threats during their transmission over public networks. Thus, it is required to secure these images prior to their communication over public networks. But due to distinctive properties of medical images, like higher correlation and redundancy among the pixels, and larger size, the existing encryption models are unable to achieve high security. Therefore, they are unable to resist various security attacks. Thus, the main objective of this paper is to design an efficient image encryption model that can develop significantly complex secret keys.

The main contributions of this paper are as follows:

- (1) An efficient image encryption model is proposed to encrypt e-healthcare images.
- (2) To obtain the secret keys, six-dimensional hyperchaotic map (SDHM) is proposed.
- (3) Efficient permutation-diffusion-based encryption approach is proposed to encrypt the biomedical images.

The rest of the paper is organized as follows. Literature review is presented in Section 2. Section 3 discusses the proposed model. Section 4 presents the experimental analysis. The conclusion is presented in Section 5.

2. Literature Review

Every day many healthcare related images are transmitted over public networks. These images contain potential secret information related to patients. But these healthcare images are susceptible to numerous security attacks [24–26]. Therefore, many medical image encryption models have been implemented. In [27], Ding et al. designed a deep learning-based medical image encryption model. Cycle-generative adversarial network (CGAN) was used to encrypt the images. In [28], Khedr and Glenn implemented a GPU-accelerated homomorphic encryption model. This model can provide encryption results at a rapid speed. In [29], Liu et al. designed a verifiable multi-keyword search (VMKS) encryption model. It has utilized anonymous key generation for medical images. Convergence key was utilized to scramble electronic health records.

In [30], Yi et al. utilized Paillier and ElGamal cryptosystems (PECs) to implement statistical analysis on the healthcare data without compromising the patients' privacy. In [31], Haddad et al. presented a joint watermarking encryption approach so called JWL for medical images. Bit substitution watermarking modulation with JPEG-LS was also used to encrypt the data. In [32], Qiu et al. designed a secure communication model by using a selective encryption model (SET) combined with fragmentation and dispersion. In [33], Jiang et al. utilized somewhat homomorphic encryption (SHE) for homomorphic evaluation over single instruction multiple data. It can encrypt data with lesser number of overheads. In [34], Bao et al. designed a revocable, privacy-preserving fine-grained data sharing method with keyword search to encrypt the healthcare data. For data authenticity, a pseudo-identity-based signature approach was also used. In [35], Wang designed a blind batch encryption model to encrypt the healthcare data. It has been found that this model can resist six typical attacks. In [36], Zeng et al. studied that attribute-based encryption can ensure data confidentiality and user privacy in healthcare environment. Partially policy-hidden and large universe-based encryption model was also used.

In [37], Sara et al. used permutation and substitution framework to encrypt the medical images. Images were divided into blocks and these blocks are permuted using zigzag pattern. Logistic map was applied to obtain the secret keys and perform the substitution operation. In [38], Shafique et al. proposed a medical image encryption scheme using DWT, logistic map, and bit-plane extraction system. In [39], Ravichandran et al. protected the medical images by using chaotic maps and deoxyribonucleic acid (DNA). Multiple chaotic maps were applied to create random keys further used in permutation, encoding, and substitution

processes to carry out the encryption. In [40], Ibrahim et al. designed an encryption scheme using chaotic maps and S-boxes to secure the medical images. In [41], Belazi et al. used DNA and chaotic maps to encrypt the medical images. SHA-256 was also used to obtain the initial values for secret keys. In [42], Wang et al. encrypted the medical images based on Galois field. In [43], Shankar et al. used adaptive grasshopper optimization algorithm to select the optimal secret key to encrypt the medical images.

From the literature, it is observed that the development of efficient encryption approach for e-healthcare is a challenging problem. Increasing the key space size is desirable. Therefore, high-dimensional hyperchaotic map can be designed to increase the key size.

3. Proposed Model

In this section, the proposed encryption model is presented for healthcare data. A SDHM is used to obtain the secret keys. These keys are then used to diffuse the medical images. The proposed SDHM is mainly divided into three parts: key generation, encryption process, and decryption process. The proposed encryption model is illustrated in Figure 1.

3.1. Six-Dimensional Hyperchaotic Map. To obtain the secret keys, a SDHM is used. It is more complex and dynamic than low-order dimensional chaotic maps. Due to this, it becomes difficult to guess the secret keys without the knowledge of initial values. It improves the security as well as robustness of the model. It is defined as [44, 45]

$$\left. \begin{aligned} w'_1 &= \lambda_1(w_2 - w_1) + w_4 + \lambda_2 w_6, \\ w'_2 &= p w_1 - w_2 - w_1 w_3 + w_5, \\ w'_3 &= -v w_3 + w_1 w_2, \\ w'_4 &= f w_4 - w_1 w_3, \\ w'_5 &= -b w_2 + w_6, \\ w'_6 &= u_1 w_1 + u_2 w_2, \end{aligned} \right\} \quad (1)$$

where $w_1, w_2, w_3, w_4, w_5,$ and w_6 are initial state variables of SDHM. $\lambda_2, b, u_1, u_2,$ and h are the control parameters. $\lambda_1, v,$ and p are the constant parameters. f is the coupling parameter. In this proposed SDHM, seven secret keys are used, and seventh secret key (w'_7) is obtained as

$$w'_7 = z w_1 \oplus f w_4, \quad (2)$$

where z is the constant parameter. The hyperchaotic nature of SDHM with attributes $\lambda_1 = 9, f = 2, b = 8.7, v = 7/2, \lambda_2 = 2, u_1 = 2, p = 31, u_2 = 3,$ and $z = 1$ is shown in Figure 2. It can be seen that SDHM is dynamic in nature and provides more complexity that is needed for security of medical images.

3.2. Encryption Process. Algorithm. 1 represents various steps to encrypt the medical images. Firstly, plain image (P_{mg}) is divided into red (P_r), green (P_g), and blue (P_b) channels. The six keys $w'_1, w'_2, w'_3, w'_4, w'_5,$ and w'_6 are

obtained using equation (1). Another key, i.e., w'_7 , is computed by utilizing the XOR (\oplus) (see equation (2)). P_r is diffused using w'_1 and \oplus operation and obtains P'_r . Similarly, P_g and P_b are diffused as P'_g and P'_b using w'_2 and w'_3 , respectively. The diffused channels P'_g and P'_b are further diffused as P''_g and P''_b using P'_r and P'_g , respectively. To increase the complexity and strength of the secret keys, keys are further modified. w'_5 is modified using w'_4 and \oplus operation as w''_5 . w'_6 is modified using w'_4 and \oplus operation as w''_6 . w'_7 is modified using w''_5 and \oplus operation as w''_7 . The diffused channels $P''_r, P''_g,$ and P''_b are encrypted using $w''_5, w''_6,$ and w''_7 with encryption factor E_f . The obtained resultant encrypted channels are $C_r, C_g,$ and C_b . Finally, encrypted image (C_{mg}) is obtained by concatenating the ciphered channels $C_r, C_g,$ and C_b (Algorithm 1).

3.3. Decryption Process. Decryption process converts the encrypted image back into original image. Algorithm. 2 shows the various steps to decrypt the encrypted image. Before starting the decryption, the algorithm needs parameters such as initial values of $w_1, w_2, w_3, w_4, w_5, w_6, w_7, \lambda_1, \lambda_2, b, v, f, u_1, u_2, z,$ and p to obtain the secret keys using equations (1) and (2) and encryption factor E_f to perform the decryption. Decryption algorithm is identical to encryption algorithm, but in reverse order (Algorithm 2).

4. Experimental Analysis

The proposed method is implemented on MATLAB2021a with 16GB RAM on i7 processor. The proposed SDHM is compared with existing models such as CGAN, VMKS, PEC, JIL, SET, and SHE to assess the performance. Five colored medical images such as CT of ascites (CTA) [46], brain MRI (BMRI) [47], dermoscopy (DM) [48], fundus (FS) [49], and ultrasound (US) [50] are taken for testing. Figure 3 shows the visual analysis of the proposed medical image encryption. Figure 3(a) shows the plain medical images which are used for encryption. The histograms of the plain images are shown in Figure 3(b). The encrypted images and their respective histograms are shown in Figures 3(c) and 3(d), respectively. Here, we can see that the histograms of encrypted images are uniform which means that it does not reveal any statistical information to attackers. Figure 3(e) shows the decrypted images that exactly look like plain images.

4.1. Performance Parameters. To assess the performance of the proposed medical image encryption model, various parameters such as peak signal to noise ratio, entropy, and correlation coefficient are utilized.

4.1.1. Peak Signal to Noise Ratio. Peak signal to noise ratio (PSNR) is utilized to quantify the quality of decrypted images [51]. It can be computed as

$$\text{PSNR} = 10 \times \log_{10} \frac{255^2}{\text{MSE}}. \quad (3)$$

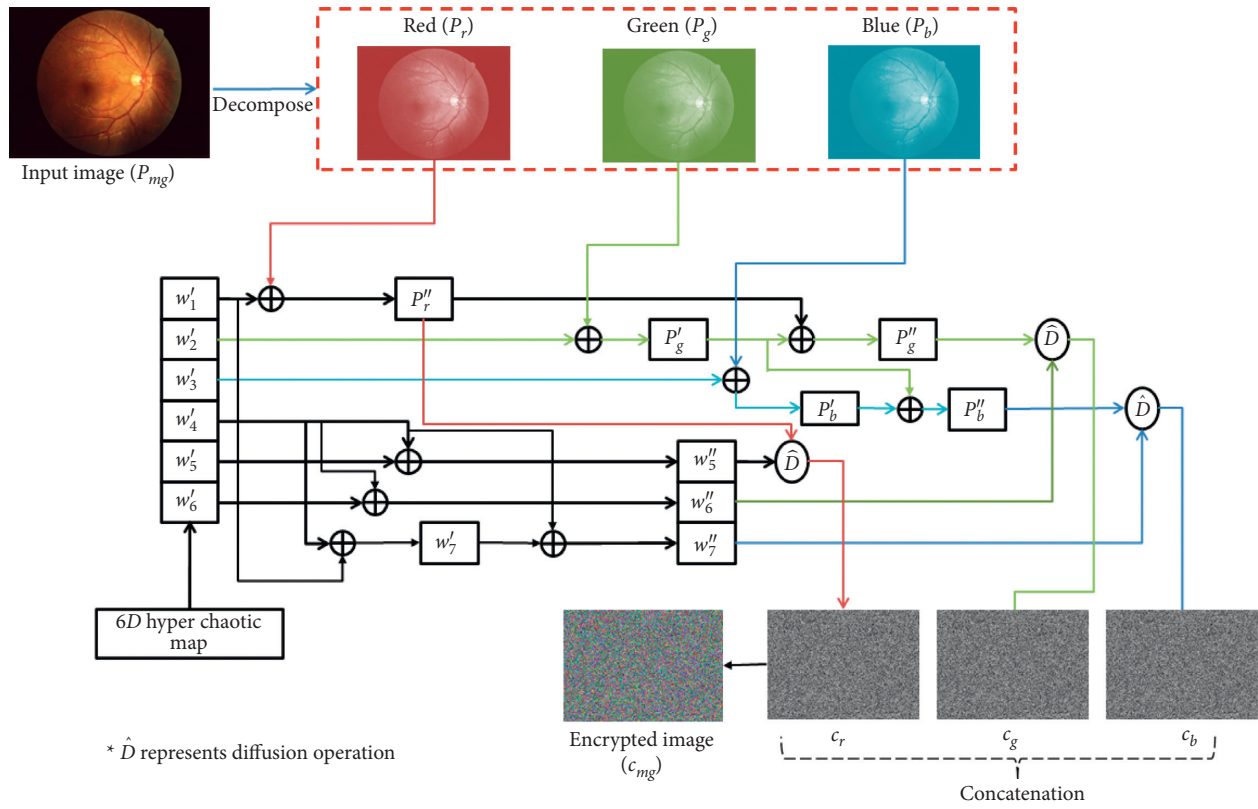


FIGURE 1: Proposed encryption scheme.

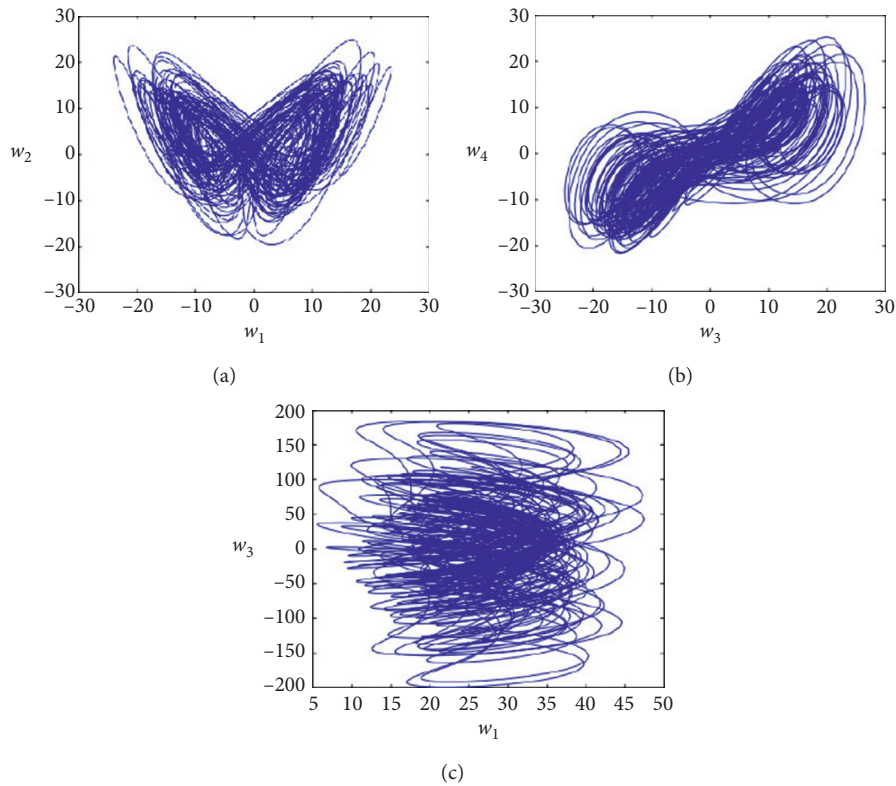


FIGURE 2: Chaotic attractors of SHM: (a) $w_1 - w_2$ plane, (b) $w_3 - w_4$ plane, and (c) $w_1 - w_3$ plane.

```

Input: plain image ( $P_{mg}$ )
Output: encrypted image ( $C_{mg}$ )
/* Decompose  $P_{mg}$  into red ( $P_r$ ), green ( $P_g$ ), and blue ( $P_b$ ) matrices.* /
 $P_r = P_{mg}(:, :, 1)$ 
 $P_g = P_{mg}(:, :, 2)$ 
 $P_b = P_{mg}(:, :, 3)$ 
obtain secret key  $w'_i$ , with  $i = 1, \dots, 7$  utilizing equations (1) and (2)
//Diffuse color channels using  $w'_1, w'_2$ , and  $w'_3$ 
 $P'_r = \text{mod}(P_r \oplus w'_1, 256)$ 
 $P'_g = \text{mod}(P_g \oplus w'_2, 256)$ 
 $P'_g = \text{mod}(P'_g \oplus P'_r, 256)$ 
 $P'_b = \text{mod}(P_b \oplus w'_3, 256)$ 
 $P_b = \text{mod}(P'_b \oplus P'_g, 256)$ 
//Modify keys  $w'_5, w'_6$ , and  $w'_7$  by considering  $w'_4$ 
 $w_5 = w'_5 \oplus w'_4$ 
 $w_6 = w'_6 \oplus w'_4$ 
 $w_7 = w'_7 \oplus w'_4$ 
//Diffuse  $P_r, P_g$ , and  $P_b$  utilizing  $w_5, w_6$ , and  $w_7$ 
 $C_r = \text{mod}(w_5 \times P_r + (1 - E_f) \times w_5, 256)$ 
 $C_g = \text{mod}(w_6 \times P_g + (1 - E_f) \times w_6, 256)$ 
 $C_b = \text{mod}(w_7 \times P_b + (1 - E_f) \times w_7, 256)$ 
//Obtain an encrypted image by concatenating scrambled channels
 $C_{mg} = \text{cat}(C_r, C_g, C_b)$ 
return  $C_{mg}$ 

```

ALGORITHM 1: Proposed encryption algorithm for medical images.

```

Input: keys  $w_1, w_2, w_3, w_4, w_5, w_6, w_7, \lambda_1, \lambda_1, b, v, f, u_1, u_2, z, p$ , and  $E_f$ 
Output:  $D_{mg}$ 
//Decompose  $C_{mg}$  to red  $C_r$ , green  $C_g$ , and blue  $C_b$  channels
 $C_r = C_{mg}(:, :, 1)$ 
 $C_g = C_{mg}(:, :, 2)$ 
 $C_b = C_{mg}(:, :, 3)$ 
obtain keys  $w'_1, w'_2, w'_3, w'_4, w'_5, w'_6$ , and  $w'_7$  using equations (1) and (2)
//modify keys  $w'_5, w'_6$ , and  $w'_7$  by  $w'_4$ 
 $w'_5 = w'_5 \oplus w'_4$ 
 $w'_6 = w'_6 \oplus w'_4$ 
 $w'_7 = w'_7 \oplus w'_4$  //Decrypt  $C_r, C_g$ , and  $C_b$  by  $w'_5, w'_6$ , and  $w'_7$ 
 $P_r = (C_r - (1 - E_f) \times w'_5) / E_f$ 
 $P_g = (C_g - (1 - E_f) \times w'_6) / E_f$ 
 $P_b = (C_b - (1 - E_f) \times w'_7) / E_f$ 
//Decrypt  $P'_r, P'_g$ , and  $P'_b$  by considering  $w'_1, w'_2$ , and  $w'_3$ 
 $P_r = P'_r \oplus w'_1$ 
 $P'_g = P'_g \oplus P'_r$ 
 $P_g = P'_g \oplus w'_2$ 
 $P_b = P'_b \oplus P'_g$ 
 $P_b = P'_b \oplus w'_3$ 
//Obtain original image by concatenating the decrypted channels
 $D_{mg} = \text{cat}(P_r, P_g, P_b)$ 
return  $D_{mg}$ 

```

ALGORITHM 2: Decryption algorithm.

Here, mean squared error (MSE) can be computed as

$$\text{MSE} = \frac{1}{mn} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [P_{mg}(i, j) - C_{mg}(i, j)]^2. \quad (4)$$

Here, P_{mg} shows input image. C_{mg} shows encrypted image. (i, j) denotes pixel coordinates. $mandn$ shows size of the input image.

Table 1 shows the performance evaluation of the proposed SDHM in terms of PSNR among decrypted and actual

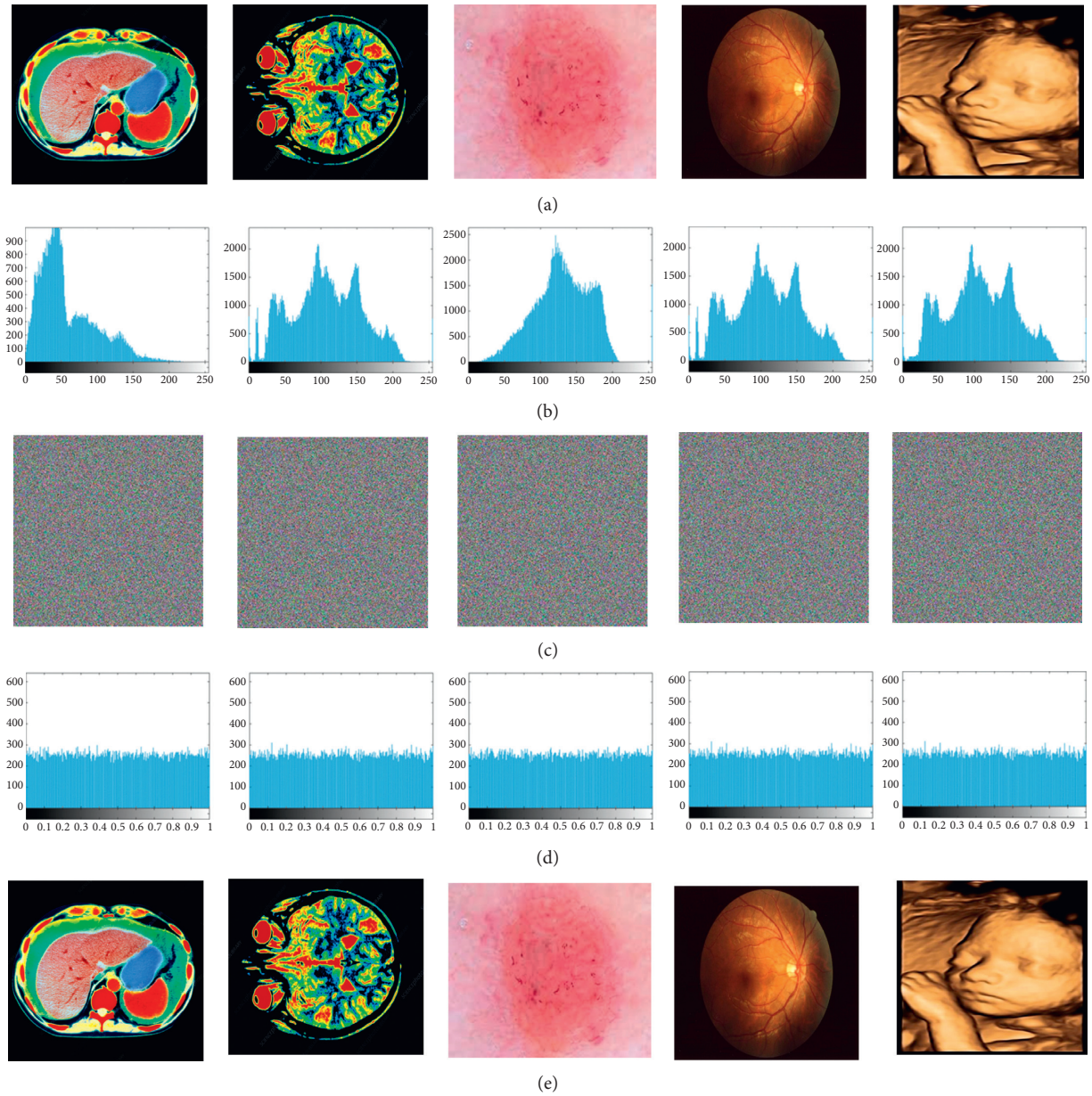


FIGURE 3: Visual analysis. (a) Plain medical images. (b) Histograms of plain images. (c) Encrypted medical images. (d) Histograms of encrypted images. (e) Decrypted images.

TABLE 1: Performance evaluation of color image in terms of PSNR between actual and decrypted images.

Technique	CTA	BMRI	DM	FS	US
CGAN [27]	56.62	47.31	40.16	51.86	50.59
VMKS [29]	56.52	43.77	47.51	52.99	52.81
PEC [30]	44.37	50.18	59.02	57.04	54.18
JJL [31]	58.21	52.55	51.12	59.32	53.92
SET [32]	57.12	56.94	43.53	57.02	57.41
SHE [33]	56.76	48.92	45.59	59.22	51.25
Proposed	59.41	58.14	60.22	60.52	58.65

images. PSNR among decrypted and actual images is desirable to be maximum. It is clearly found that the proposed SDHM achieves remarkably better PSNR values than the

existing models. The proposed SDHM shows an average improvement in terms of PSNR as 3.4587%. Bold values indicate the high performance.

TABLE 2: Performance evaluation of color image in terms of PSNR between actual and encrypted images.

Technique	CTA	BMRI	DM	FS	US
CGAN [27]	6.18	4.25	2.44	3.73	4.27
VMKS [29]	4.32	5.12	2.17	2.42	5.27
PEC [30]	4.57	4.55	6.58	3.61	4.04
JJL [31]	1.64	3.45	5.99	3.55	1.75
SET [32]	5.05	6.92	4.61	4.32	4.44
SHE [33]	3.29	4.94	5.31	2.08	4.89
Proposed	1.44	2.25	1.97	1.88	1.55

TABLE 3: Performance evaluation of color image in terms of entropy.

Technique	CTA	BMRI	DM	FS	US
CGAN [27]	7.76	7.26	7.54	7.6	7.05
VMKS [29]	7.51	7.59	7.45	7.39	7.19
PEC [30]	7.21	7.72	7.5	7.07	7.31
JJL [31]	7.65	7.37	7.03	7.43	7.12
SET [32]	7.6	7.7	7.52	7.53	7.56
SHE [33]	7.16	7.53	7.55	7.14	7.12
Proposed	7.59	7.53	7.38	7.43	7.39

Table 2 demonstrates the performance evaluation of the proposed SDHM in terms of PSNR among encrypted and actual images. PSNR among encrypted and actual images is desirable to be minimum. It is clearly observed that the proposed SDHM obtains remarkably minimum PSNR values than the existing models. The proposed SDHM shows an average reduction in terms of PSNR as 1.6478%.

4.1.2. Entropy. Entropy is a well-known measure which indicates the degree of randomness in the image [52]. Entropy values of encrypted images are desirable to be 8. Entropy (m) of an image can be computed as

$$m = \sum_{i=0}^{m-1} p(m_i) \log_2 \frac{1}{p(m_i)}. \quad (5)$$

Here, m_i shows the probability values of corresponding pixels.

Table 3 shows the performance evaluation of the proposed SDHM in terms of entropy of encrypted images and it should be maximum. It is clearly observed that the proposed SDHM attains remarkably better entropy values than the existing models. The proposed SDHM shows an average improvement in terms of entropy as 0.8978%.

4.1.3. Correlation Coefficient. The attackers sometimes explore the relation among the adjacent pixels of an image for statistical attacks. Actually, the adjacent pixels of the plain image are highly correlated to each other in all three directions such as horizontally (H_C), vertically (V_C), and diagonally (D_C) [53]. This relation should be minimum so that no statistical information should be disclosed to the

attackers. The relation among the adjacent pixels can be calculated as follows:

$$r = \frac{\sum(x_i - \mu_x)(y_i - \mu_y)}{\sqrt{\sum(x_i - \mu_x)^2(y_i - \mu_y)^2}} \quad (6)$$

Here, r is the correlation coefficient. x and y represent the adjacent pixels. μ_x and μ_y are the means of x and y , respectively. For this experiment, we randomly selected 3000 pairs of adjacent pixels (x, y) from plain and encrypted images. US image is taken for this test.

Figure 4 shows the inter-pixel correlation of US image. Horizontal (H_C), vertical (V_C), and diagonal (D_C) correlations between the pixels of plain red channel are presented in Figures 4(a), 4(b), and 4(c). Here, it shows that pixels of plain image are highly correlated. Figures 4(d), 4(e), and 4(f) show H_C , V_C , and D_C among the pixels of encrypted red channel. Here, it can be seen that pixels are random in nature and show no relation among the pixels.

The inter-pixel correlation of green channel is shown in Figure 5. H_C , V_C , and D_C between the pixels of plain green channel are shown in Figures 5(a), 5(b), and 5(c), respectively. Figures 5(d), 5(e), and 5(f) show H_C , V_C , and D_C among the pixels of encrypted green channel. It can be seen that pixels are loosely correlated to each other. Similarly, Figure 6 shows the correlation among the pixels of plain and encrypted blue channels. Figures 6(a)–6(c) show the relation between the pixels of plain blue channel. Figures 6(d)–6(f) show the relation among the pixels of encrypted green channel. It can be observed that pixels are not correlated to each other. Table 4 shows H_C , V_C , and D_C among the adjacent pixels

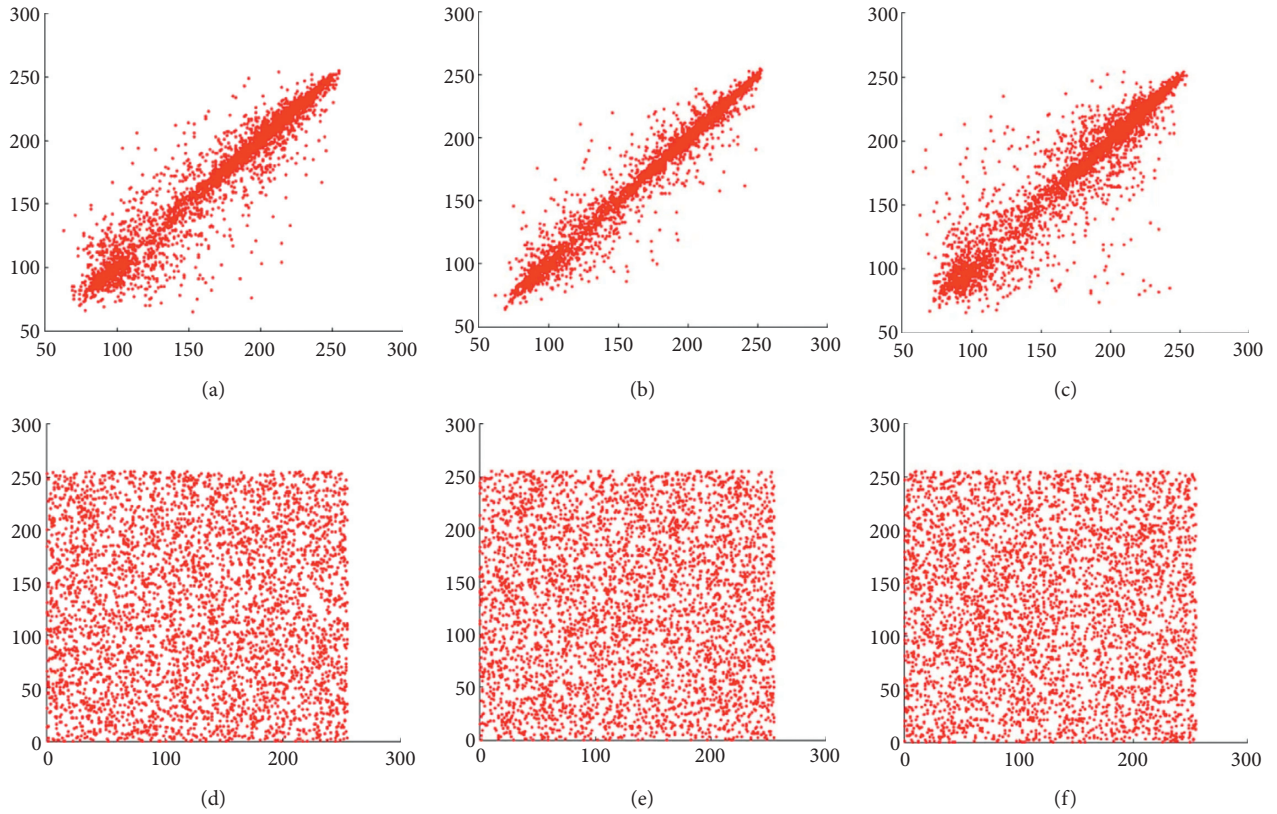


FIGURE 4: Correlation analysis of red channel of US image: (a) H_C , (b) V_C , and (c) D_C among the pixels of plain red channel and (d) H_C , (e) V_C , and (f) D_C among the pixels of encrypted red channel.

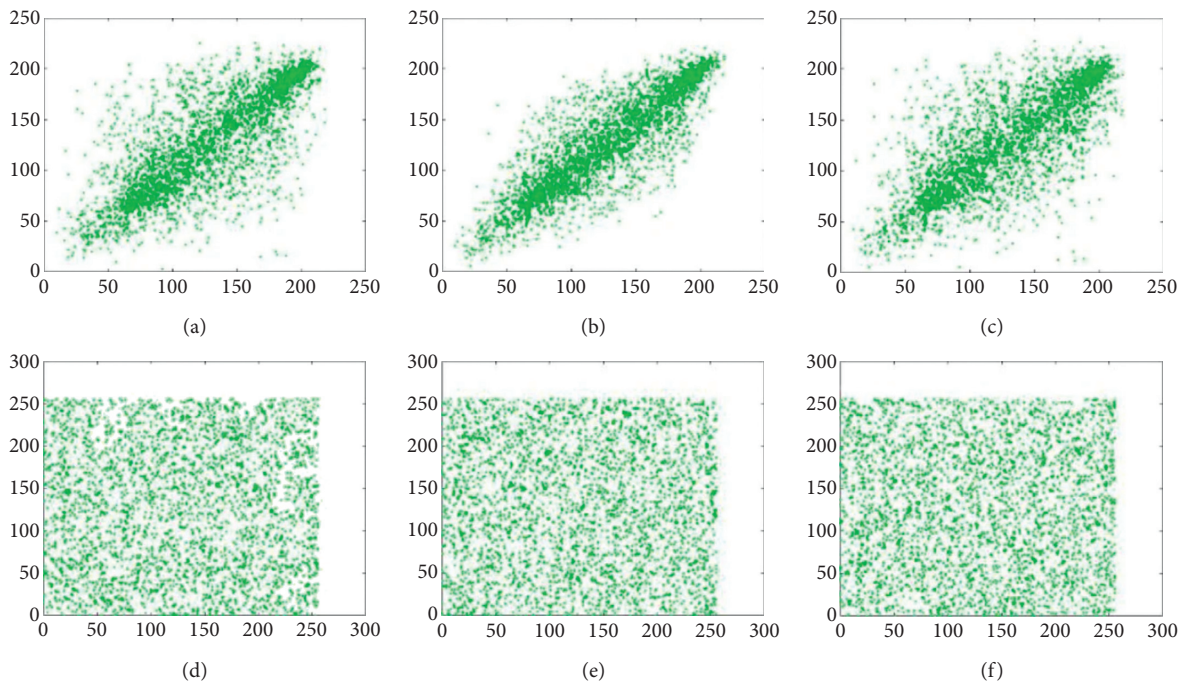


FIGURE 5: Correlation analysis of green channel of US image: (a) H_C , (b) V_C , and (c) D_C among the pixels of plain green channel and (d) H_C , (e) V_C , and (f) D_C among the pixels of encrypted green channel.

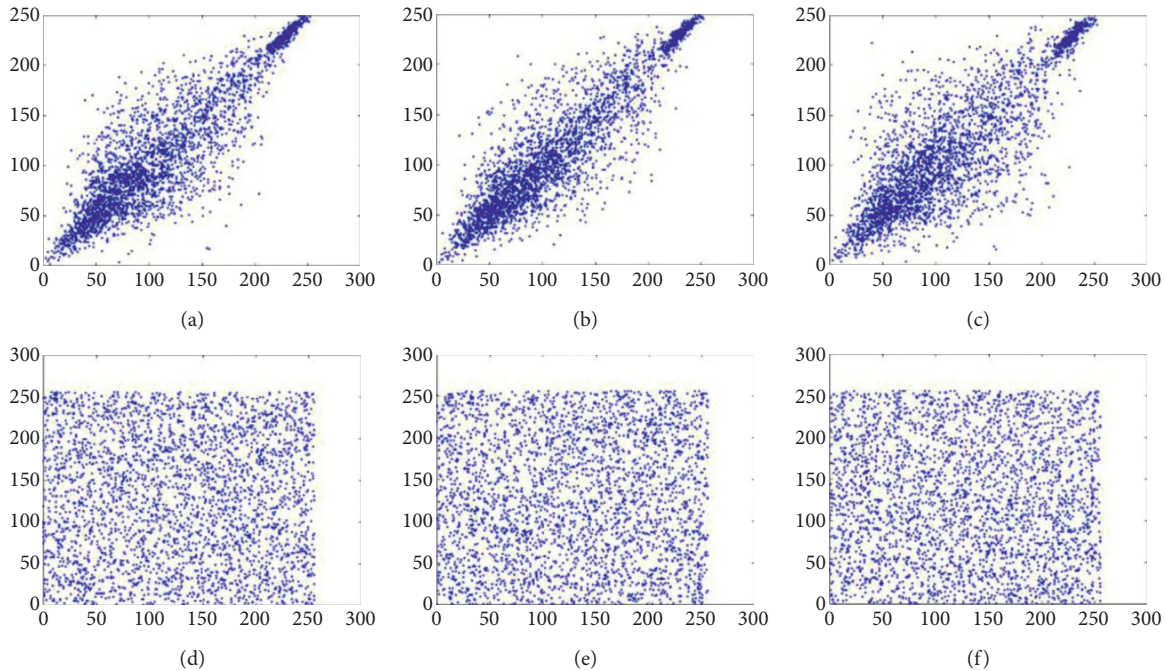


FIGURE 6: Correlation analysis of blue channel of US image: (a) H_C , (b) V_C , and (c) D_C among the pixels of plain blue channel and (d) H_C , (e) V_C , and (f) D_C among the pixels of encrypted blue channel.

TABLE 4: Correlation coefficient of encrypted medical images.

Technique	H_C	V_C	D_C
CTA	0.0076	0.0052	0.0049
BMRI	0.0051	0.0059	0.0045
DM	0.0021	0.0072	0.0015
FS	0.0065	0.0037	0.0032
US	0.0006	0.0027	0.0062

of encrypted medical images. From the values, it can be seen that there is no relation among the adjacent pixels of the encrypted medical images. Hence, attackers cannot discover any kind of statistical information to recover the information.

5. Conclusion

An efficient image encryption approach for medical images was proposed. Six-dimensional hyperchaotic map was utilized to obtain the secret keys. Firstly, plain medical image was divided into three channels such as red, green, and blue. Secret keys were used to diffuse these channels. Lastly, encrypted channels were concatenated and final encrypted medical image was obtained. Comparative analysis revealed that the proposed SDHM achieves remarkably good performance than the existing encryption models. The proposed SDHM has significantly increased the key size. Therefore, the proposed SDHM can resist various security attacks. Extensive experimental analysis revealed that the proposed SDHM outperforms the competitive models in terms of entropy, correlation coefficient, and PSNR by 1.7483%, 1.7483%, and 1.8325%, respectively.

In near future, we will utilize some soft-computing techniques to increase the size of secret keys. Additionally, more security attacks will be implemented to evaluate the performance of the proposed model.

Data Availability

The used datasets are freely available from the following: CT (<https://www.kaggle.com/kmader/siim-medical-images>); dermatology (<https://www.kaggle.com/sergio814/dermoscopy-images>); fundus (<https://www.kaggle.com/andrewmvd/ocular-disease-recognition-odir5k>); brain MRI (<https://www.kaggle.com/mateuszbeda/lgg-mri-segmentation>); ultrasound (<http://femomum.telecom-paristech.fr/download.html>).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

- [1] S. A. Banday, A. H. Mir, and S. Malik, "Multilevel medical image encryption for secure communication," in *Advances in Computational Techniques for Biomedical Image Analysis*, D. Koundal and S. Gupta, Eds., Academic Press, Cambridge, MA, USA, pp. 233–252, 2020.
- [2] B. Gupta, M. Tiwari, and S. S. Lamba, "Visibility improvement and mass segmentation of mammogram images using quantile separated histogram equalisation with local contrast enhancement," *CAAI Transactions on Intelligence Technology*, vol. 4, no. 2, pp. 73–79, 2019.
- [3] W. Cao, Y. Zhou, C. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Processing*, vol. 132, pp. 96–109, 2017.

- [4] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-Elyazeed, "Generalized double-humped logistic map-based medical image encryption," *Journal of Advanced Research*, vol. 10, pp. 85–98, 2018.
- [5] X. Chen and C.-J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping," *Saudi Journal of Biological Sciences*, vol. 24, no. 8, pp. 1821–1827, 2017.
- [6] A. Banik, Z. Shamsi, and D. S. Laiphrakpam, "An encryption scheme for securing multiple medical images," *Journal of Information Security and Applications*, vol. 49, Article ID 102398, 2019.
- [7] V. Sangavi and P. Thangavel, "An exotic multi-dimensional conceptualization for medical image encryption exerting rossler system and sine map," *Journal of Information Security and Applications*, vol. 55, Article ID 102626, 2020.
- [8] V. Lima, F. Madeiro, and J. Lima, "Encryption of 3d medical images based on a novel multiparameter cosine number transform," *Computers in Biology and Medicine*, vol. 121, Article ID 103772, 2020.
- [9] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Encryption and watermark-treated medical image against hacking disease—an immune convention in spatial and frequency domains," *Computer Methods and Programs in Biomedicine*, vol. 159, pp. 11–21, 2018.
- [10] J. Lima, F. Madeiro, and F. Sales, "Encryption of medical images based on the cosine number transform," *Signal Processing: Image Communication*, vol. 35, pp. 1–8, 2015.
- [11] S. Jeevitha and N. A. Prabha, "Novel medical image encryption using dwt block-based scrambling and edge maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3373–3388, 2021.
- [12] A. Banu S and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-dna-iwt combined approach," *Medical, & Biological Engineering & Computing*, vol. 58, no. 7, pp. 1445–1458, 2020.
- [13] D. Jiang, G. Hu, G. Qi, and N. Mazur, "A fully convolutional neural network-based regression approach for effective chemical composition analysis using near-infrared spectroscopy in cloud," *Journal of Artificial Intelligence and Technology*, vol. 1, no. 1, pp. 74–82, 2021.
- [14] A. Vengadapurvaja, G. Nisha, R. Aarthy, and N. Sasikaladevi, "An efficient homomorphic medical image encryption algorithm for cloud storage security," *Procedia Computer Science*, vol. 115, 2017.
- [15] D. Bouslimi, G. Coatrieux, and C. Roux, "A joint encryption/watermarking algorithm for verifying the reliability of medical images: application to echographic images," *Computer Methods and Programs in Biomedicine*, vol. 106, no. 1, pp. 47–54, 2012.
- [16] Y. Xu and T. T. Qiu, "Human activity recognition and embedded application based on convolutional neural network," *Journal of Artificial Intelligence and Technology*, vol. 1, no. 1, pp. 51–60, 2021.
- [17] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," *Optics and Lasers in Engineering*, vol. 110, pp. 24–32, 2018.
- [18] H. S. Basavegowda and G. Dagnew, "Deep learning approach for microarray cancer data classification," *CAAI Trans. Intell. Technol.* vol. 5, no. 1, pp. 22–33, 2020.
- [19] C. Thirumarai Selvi, J. Amudha, and R. Sudhakar, "A modified salp swarm algorithm (ssa) combined with a chaotic coupled map lattices (cml) approach for the secured encryption and compression of medical images during data transmission," *Biomedical Signal Processing and Control*, vol. 66, Article ID 102465, 2021.
- [20] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhleb, "A novel selective encryption scheme for medical images transmission based-on jpeg compression algorithm," *Procedia Computer Science*, vol. 112, pp. 369–376, 2017.
- [21] I. Ahmad and S. Shin, "A novel hybrid image encryption-compression scheme by combining chaos theory and number theory," *Signal Processing: Image Communication*, vol. 98, Article ID 116418, 2021.
- [22] G. Hu, S.-H. K. Chen, and N. Mazur, "Deep neural network-based speaker-aware information logging for augmentative and alternative communication," *Journal of Artificial Intelligence and Technology*, vol. 1, no. 2, pp. 138–143, 2021.
- [23] S. Ghosh, P. Shivakumara, P. Roy, U. Pal, and T. Lu, "Graphology based handwritten character analysis for human behaviour identification," *CAAI Trans. Intell. Technol.*, vol. 5, no. 1, pp. 55–65, 2020.
- [24] W. Cao, Y. Zhou, C. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Processing*, vol. 132, pp. 96–109, 2017.
- [25] X. Chen and S. Zou, "Improved wi-fi indoor positioning based on particle swarm optimization," *IEEE Sensors Journal*, vol. 17, no. 21, pp. 7143–7148, 2017.
- [26] H. Kwok and W. K. Tang, "A fast image encryption system based on chaotic maps with finite precision representation, Chaos," *Solitons & Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.
- [27] Y. Ding, G. Wu, D. Chen et al., "Deepedn: a deep-learning-based image encryption and decryption network for internet of medical things," *IEEE Internet of Things Journal*, vol. 8, no. 3, pp. 1504–1518, 2021.
- [28] A. Khedr and G. Gulak, "Securedmed: secure medical computation using gpu-accelerated homomorphic encryption scheme," *IEEE Journal of Biomedical and Health Informatics*, vol. 22, no. 2, pp. 597–606, 2018.
- [29] X. Liu, X. Yang, Y. Luo, and Q. Zhang, "Verifiable multi-keyword search encryption scheme with anonymous key generation for medical internet of things," *IEEE Internet of Things Journal*, page 2021.
- [30] X. Yi, A. Bouguettaya, D. Georgakopoulos, A. Song, and J. Willemsen, "Privacy protection for wireless medical sensor data," *IEEE Transactions on Dependable and Secure Computing*, vol. 13, no. 3, pp. 369–380, 2016.
- [31] S. Haddad, G. Coatrieux, A. Moreau-Gaudry, and M. Cozic, "Joint watermarking-encryption-jpeg-ls for medical image reliability control in encrypted and compressed domains," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 2556–2569, 2020.
- [32] H. Qiu, M. Qiu, M. Liu, and G. Memmi, "Secure health data sharing for medical cyber-physical systems for the healthcare 4.0," *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 9, pp. 2499–2505, 2020.
- [33] L. Jiang, L. Chen, T. Giannetsos, B. Luo, K. Liang, and J. Han, "Toward practical privacy-preserving processing over encrypted data in iot: an assistive healthcare use case," *IEEE Internet of Things Journal*, vol. 6, no. 6, Article ID 10177, 2019.
- [34] Y. Bao, W. Qiu, P. Tang, and X. Cheng, "Efficient, revocable and privacy-preserving fine-grained data sharing with keyword search for the cloud-assisted medical iot system," *IEEE Journal of Biomedical and Health Informatics*, p. 1, 2021.
- [35] Z. Wang, "Blind batch encryption-based protocol for secure and privacy-preserving medical services in smart connected

- health,” *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 9555–9562, 2019.
- [36] P. Zeng, Z. Zhang, R. Lu, and K.-K. R. Choo, “Efficient policy-hiding and large universe attribute-based encryption with public traceability for internet of medical things,” *IEEE Internet of Things Journal*, vol. 8, no. 13, Article ID 10963, 2021.
- [37] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, “A new image encryption algorithm for grey and color medical images,” *IEEE Access*, vol. 9, Article ID 37855, 2021.
- [38] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, “Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain,” *IEEE Access*, vol. 9, Article ID 59108, 2021.
- [39] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, “Dna chaos blend to secure medical privacy,” *IEEE Transactions on NanoBioscience*, vol. 16, no. 8, pp. 850–858, 2017.
- [40] S. Ibrahim, H. Alhumyani, M. Masud et al., “Framework for efficient medical image encryption using dynamic s-boxes and chaotic maps,” *IEEE Access*, vol. 8, Article ID 160433, 2020.
- [41] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, “Novel medical image encryption scheme based on chaos and dna encoding,” *IEEE Access*, vol. 7, Article ID 36667, 2019.
- [42] N. Wang, G. Di, X. Lv et al., “Galois field-based image encryption for remote transmission of tumor ultrasound images,” *IEEE Access*, vol. 7, Article ID 49945, 2019.
- [43] 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, Article ID 77145, 2018.
- [44] Q. Yang, D. Zhu, and L. Yang, “A new 7d hyperchaotic system with five positive lyapunov exponents coined,” *International Journal of Bifurcation and Chaos*, vol. 28, no. 05, Article ID 1850057, 2018.
- [45] S. Osterland and J. Weber, “Analytical analysis of single-stage pressure relief valves,” *International Journal of Hydro-mechatronics*, vol. 2, no. 1, pp. 32–53, 2019.
- [46] Kaggle, “siim-medical-images,” 2017, <https://www.kaggle.com/kmader/siim-medical-images>.
- [47] Kaggle, “lgg-mri-segmentation,” 2019, <https://www.kaggle.com/mateuszbudalgg-mri-segmentation>.
- [48] Kaggle, “dermoscopy-images,” 2019, <https://www.kaggle.com/sergio814/dermoscopy-images>.
- [49] Kaggle, “ocular-disease-recognition-odir5k,” 2020, <https://www.kaggle.com/andrewmvd/ocular-disease-recognition-odir5k>.
- [50] femonum.telecom-paristech, “Femonum telecom paristech,” 2018, <http://femonum.telecom-paristech.fr/download.html>.
- [51] M. Kaur and D. Singh, “Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption,” *Multidimensional Systems and Signal Processing*, vol. 32, no. 1, pp. 281–301, 2021.
- [52] M. Kaur, D. Singh, V. Kumar, B. Gupta, and A. A. Abd El-Latif, “Secure and energy efficient based e-health care framework for green internet of things,” *IEEE Transactions on Green Communications and Networking*, vol. 5, 2021.
- [53] M. Kaur, D. Singh, K. Sun, and U. Rawat, “Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5d chaotic map,” *Future Generation Computer Systems*, vol. 107, pp. 333–350, 2020.