IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 15 May 2023, accepted 3 July 2023, date of publication 12 July 2023, date of current version 24 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3294570

RESEARCH ARTICLE

Lightweight Biomedical Image Encryption Approach

MANJIT KAUR[1], (Senior Member, IEEE), AHMAD ALI ALZUBI[2], DILBAG SINGH[3], (Senior Member, IEEE), VIJAY KUMAR[4], AND HEUNG-NO LEE[5], (Senior Member, IEEE)

[1]School of Computer Science and Artificial Intelligence, SR University, Warangal, Telangana 506371, India
[2]Department of Computer Science, Community College, King Saud University, Riyadh 11362, Saudi Arabia
[3]Center of Biomedical Imaging, Department of Radiology, New York University Grossman School of Medicine, New York, NY 10016, USA
[4]Department of Information Technology, Dr. B. R. Ambedkar National Institute of Technology, Jalandhar, Punjab 144008, India
[5]School of Electrical Engineering and Computer Science, Gwangju Institute of Science and Technology, Gwangju 61005, South Korea

Corresponding author: Heung-No Lee (heungno@gist.ac.kr)

This work was supported in part by the National Research Foundation of Korea (NRF) funded by the Korean Government (MSIP) under Grant NRF-2021R1A2B5B03002118; in part by the Ministry of Science and ICT (MSIT), South Korea, under the Information Technology Research Center (ITRC) Support Program Supervised by the Institute of Information and Communications Technology Planning and Evaluation (IITP) under Grant IITP-2023-2021-0-01835; and in part by King Saud University, Riyadh, Saudi Arabia, Researchers Supporting under Project RSP2023R395.

ABSTRACT This paper proposes a lightweight image encryption approach for medical Internet of Things (MIoT) networks using compressive sensing and a modified seven-dimensional (*MSD*) hyperchaotic map. Initially, 7D hyperchaotic map is modified to generate more secure and complex secret keys. SHA-512 is used to create the initial conditions for *MSD*, which ensures its sensitivity towards input images. Using nonsubsampled contourlet transform (NSCT), further improvements in the compressive sensing are achieved, and then the measurement matrices are generated using the secret keys obtained from *MSD*. Finally, to generate encrypted images, the diffusion and permutation are carried out row and column-wise on compressed images using secret keys obtained from *MSD*. The comparative analyses verify the performance of the proposed lightweight encryption approach in terms of robustness, security, and statistical analysis.

INDEX TERMS Lightweight image encryption, Medical Internet of Things (MIoT), compressive sensing, hyperchaotic map, modified seven-dimensional (MSD), SHA-512, nonsubsampled contourlet transform (NSCT), measurement matrices, diffusion, permutation, robustness, security, statistical analysis.

I. INTRODUCTION

Nowadays, secure data transmission over the Internet is a challenging issue due to the recent progress in digital technologies and the Internet. This situation is even worse for medical data transmission. The unauthorized access to medical information over the Internet led to the desecration of patients' rights [1]. Patient data such as laboratory reports, ECG reports, and medical prescriptions are stored and transmitted in digital form. The digital form of patient's medical data is convenient for both patient and doctor. According to the literature, more than 90% medical images of patients are processed and stored in electronic health records [2]. Secure medical data is required to ensure privacy and protection from manipulation. Recently, Internet of Things (IoT) systems are widely used in medical imaging to easily transfer the patient's data to a remote site for medical diagnosis. However, the manipulation and exploitation of medical data are very easy in the IoT environment. To fix this problem, some information security policies are integrated with IoT systems to obtain security and privacy of medical data [3].

Steganography and encryption approaches are utilized to hide sensitive patient diagnostic information over an IoT environment. In an IoT environment, medical data should be encrypted through medical sensors. Thereafter, the medical practitioners decrypt the encrypted patient's data, and

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

decrypted patient's data was used for diagnosis. Besides this, the medical practitioners can utilize a cloud server to accomplish patients' supplementary diagnoses using deep learning techniques. The cloud server uses the encrypted patient's data for supplementary diagnosis [2], [4]. However, the traditional encryption techniques are unable to provide direct encryption on transmitted data [5], [6]. To fix this problem, the encryption technique is required to secure the patient's data over the IoT environment.

The main contributions of this paper are as follows:

1) A secure lightweight medical image encryption approach is designed using compressive sensing and a modified seven-dimensional (*MSD*) hyperchaotic map.
2) *MSD* is designed by modifying 7D hyperchaotic map [7] to make it more dynamic and complex. The initial conditions for *MSD* are generated using SHA-512 which assures its sensitivity towards input images.
3) Compressive sensing is further improved by using Nonsubsampled contourlet transform (NSCT) and measurement matrices are generated using the secret keys obtained from *MSD*.
4) To generate encrypted images, the diffusion and permutation are carried out row and column-wise on compressed images using secret keys obtained from *MSD*.

The remaining paper is organized as follows: The review of existing literature is presented in Section II. The proposed encryption approach for medical images is illustrated in Section III. Section IV presents the performance analysis. The concluding remarks are drawn in Section V.

II. RELATED WORK

Tao et al. [3] proposed a secure IoT-based healthcare system to handle the security issues associated with conventional techniques. They implemented a KATAN secret cipher algorithm on FPGA hardware platform. However, their proposed system requires slightly more computational time than the other schemes. Rezaeibagha et al. [4] presented an IoT-based wearable monitoring system for secure data analysis. An authenticated additive homomorphic encryption was proposed for secure communication. The computational time of the proposed system is lower than the existing schemes. Khari et al. [8] developed a Galois cryptography scheme (GCS) to secure data in an IoT environment. The matrix XOR steganography was utilized in their scheme to enhance security. Adaptive Firefly algorithm was used to optimize the image block. Their scheme attained better embedding efficiency than the existing schemes. Xiang et al. [9] developed an image importance-based visual security index by utilizing the texture and contrast. An Image importance-based polling strategy (IPS) was used to combine the texture features and contrast. This scheme has better performance than the existing approaches. Itier et al. [10] developed a JPEG crypto-compressed technique (CCT) using the information about the secret key and original image. The proposed technique is robust towards multiple recompressions. Visual secret sharing schemes (VSS) are also used for encrypting the multiple images [11]. Muhammad et al. [12] proposed a secure IoT system for image encryption. A probabilistic lightweight algorithm (PLA) was utilized for the encryption of keyframes. The chaotic map was used to generate the pseudorandom key. This approach not only reduces the transmission cost but also improves the storage capacity. However, the performance of this approach can be further improved by utilizing the dynamic keys. Lee and Chiu [13] developed a natural image-based VSS scheme for encryption. The diverse media was used for sharing digital images. Due to the diversity of media, interceptors are unable to intercept shares. They extracted the features from natural share. This scheme not only reduces the transmission risk but also increases user-friendliness. Xiang et al. [14] proposed a visual security index (VSI) to compute the visual analysis of encrypted images. They used a multi-threshold approach for the detection of a skeleton of an encrypted image. The adaptive weights were used to determine the contributions of texture and edge similarities. Bao et al. [15] developed a lossless secret image sharing scheme (LSS). It is able to identify the fake share for real-life applications. This scheme is able to withstand the different attacks. Li et al. [16] proposed a secure transmission system that uses the concepts of compressed sensing (CS) for IoT environments. They used compressed sensing and reconstruction mechanism for efficient image encryption. The proposed system provides not only low computational cost but also low power consumption. Beugnon et al. [17] presented a secret 3-D object sharing scheme to protect the actual content of an image. The geometrical distortions were protected through the proposed sharing mechanism. The degradation level mentioned in this scheme was used to control the geometric distraction in the encrypted image. Kamal et al. [18] implemented an image splitting technique and logistic map (ISTLM) to secure the medical images. The blocks of the image were scrambled by utilizing random permutation, rotation, and zigzag patterns. Using the logistic chaotic map, secret keys were generated that were used to diffuse scrambled blocks. Akkasaligar et al. [19] utilized dual hyperchaotic map and DNA cryptography (DDNA) to implement the medical image encryption technique. In this technique, encryption was carried out on the selective pixels to reduce the complexity. Liu et al. [20] designed an attribute-based encryption approach using the symmetric key. The convergence key was utilized to encrypt medical data.

Zeng et al. [21] proposed attribute-based encryption to provide fine-grained access control to achieve user privacy and data confidentiality. This approach was used with public traceability for real-time implementation. Lin et al. [22] utilized a memristive coupled neural network on one multistable memristor synapse and two sub-neural networks. Hyperchaotic attractors with higher complexity were achieved that have also improved the attractor positions by switching their initial states. Masood et al. [23] applied XOR operations and random shuffling (XRF) to encrypt the medical images. Henon chaotic map was used to perform the confusion process. Chen's chaotic system and Brownian motion were utilized to implement the diffusion process. To resolve the issues associated with different techniques, a novel encryption technique is required to store and transmit the patient's data securely and efficiently.

III. PRELIMINARIES

Compressive sensing and hyperchaotic seven-dimensional map are discussed in this section.

A. COMPRESSIVE SENSING

In this paper, $2D$ compressive sensing is used which evaluates the sparse signal s_g from two directions linearly to minimize the size of a image. Initially, Φ domain is used to evaluate s_g. For a $2D$ signal x having size $R \times C$, x can decomposed to Φ domain to evaluate s_g as:

$$x = \Phi s_g \tag{1}$$

Here, s_g represent the transform coefficients matrix of x. It provides maximum size as $R1 \times C$ ($R1 \ll R$). Φ represents a $R \times C$ orthogonal matrix. Two $R \times C$ measurement matrices ϕ_1 and ϕ_2 are implemented on s_g from two directions and $R1 \times C1$ measurement signal matrix y can be computed as:

$$y = \phi_2 s_g \phi_1^T \tag{2}$$

Finally, x can be reevaluated from y by optimizing l_0-norm as:

$$min||s||_0 \ s.t. y = \phi_2 s_g \phi_1^T \tag{3}$$

Here, $|| \cdot ||_0$ shows l_0-norm.

In this paper, an input image is decomposed into Nonsubsampled contourlet transform (NSCT) [24], and utilize the circular matrices to evaluate the signal from both directions.

B. 7D HYPERCHAOTIC

A 7D hyperchaotic map (7DHCM) is implemented by Yang et al. [7]. Two linear and one nonlinear feedback controller are used in 7DHCM to make its behavior complex. It generates five positive Lyapunov exponents which make it better than other chaotic maps. It contains a large number of attributes (state variables and constants) under unique equilibria. It further improves the keyspace and makes the brute-force attacks infeasible. Therefore, it can be used in secure communication. 7DHCM map can be defined as

$$\left.\begin{aligned} d_1' &= l(d_2 - d_1) + d_4 + ed_6, \\ d_2' &= qd_1 - d_2 - d_1 d_3 + d_5, \\ d_3' &= -Td_3 + d_1 d_2, \\ d_4' &= td_4 - d_1 d_3, \\ d_5' &= -ad_2 + d_6, \\ d_6' &= p_1 d_1 + p_2 d_2, \\ d_7' &= hd_7 + md_4, \end{aligned}\right\} \tag{4}$$

where d_1 to d_7 represent the initial state variables of 7DHCM. m denotes the coupling attribute. l, T, and q represent the constant attributes. e, t, a, p_1, p_2, and h denote the control attributes.

IV. PROPOSED APPROACH

The proposed lightweight image encryption approach is illustrated in Fig. 1 and Algo. 1.

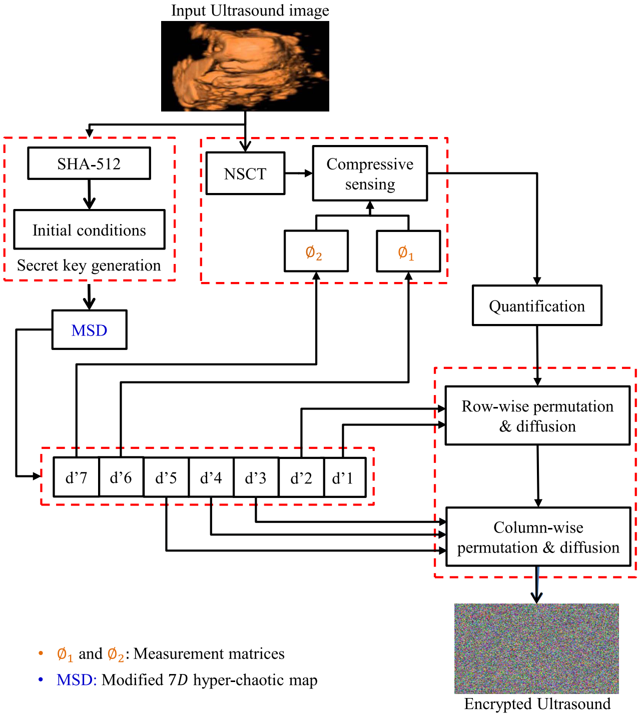

FIGURE 1. Diagrammatic flow of *MSD*-based lightweight encryption approach.

Algorithm 1 *MSD*-Based Lightweight Encryption

```
Read an image $I_m$ of size $R \times C$.
Initial conditions of $MSD$ are obtained using
    SHA-512 based on plain image (see Section IV-B).
Initial conditions are supplied to $MSD$ (using Eq. 5) to
    obtain the secret keys such as $d_1'$ to $d_7'$.
Apply compression and encryption on $I_m$ using $2D$
    compressive sensing. To obtain the measurement
    matrix, $d_6'$ and $d_7'$ are utilized. The process of
    compression is presented in Section IV-C. The
    resultant compressed image is $I$.
$I$ is permutated and diffused row-wise using secret
    keys $d_1$ and $d_2$ (see Algo. 2 and section IV-D).
    It generates a permutated and diffused image $I_r$.
$I_r$ is then permutated and diffused column-wise using
    secret keys $d_3$, $d_4$, and $d_5$ (see Algo. 3 and
    Section IV-E). It generates the final encrypted
    image $I_c$.
```

A. MODIFIED 7D HYPERCHAOTIC MAP

The states d_5' and d_6' of 7DHCM do not depend on the its initial states (see Eq. 4). To create better chaotic sequences, it is must that the states should depend on their initial states. Therefore, to improve the complexity of 7DHCM, we have modified the states d_5' and d_6' of Eq. 4. Hence, the modified 7DHCM (MSD) map is defined as

$$\left.\begin{aligned} d_1' &= l(d_2 - d_1) + d_4 + ed_6, \\ d_2' &= qd_1 - d_2 - d_1d_3 + d_5, \\ d_3' &= -Td_3 + d_1d_2, \\ d_4' &= td_4 - d_1d_3, \\ d_5' &= -ad_5 + d_6, \\ d_6' &= p_1d_1 + p_2d_2 - d_6, \\ d_7' &= hd_7 + md_4, \end{aligned}\right\} \tag{5}$$

The hyperchaotic behavior of *MSD* is shown in Fig. 2 with attributes $l = 10$, $m = 1$, $a = 9.9$, $T = 8/3$, $e = 1$, $p_1 = 1$, $q = 28$, $t = 2$, $p_2 = 2$, and $h = 1$. The Lyapunov exponents (*LEs*) of *MSD* map are obtained as $L\epsilon_1 = 1.0000$, $L\epsilon_2 = 0.4128$, $L\epsilon_3 = 0.2255$, $L\epsilon_4 = 0.1360$, $L\epsilon_5 = 0.0880$, $L\epsilon_6 = 0.0000$, and $L\epsilon_7 = -12.5289$. Their corresponding eigenvalues (G) are $G_1 = -22.06230$, $G_2 = -2.6667$, $G_3 = 1$, $G_4 = 2$, $G_5 = 11.4755$, and $\epsilon_{6,7} = 0.037 \pm 0.3850i$. It is evident that *MSD* achieves hyper chaotic attractors with 5 non-negative *LEs* and only 1 equilibrium.

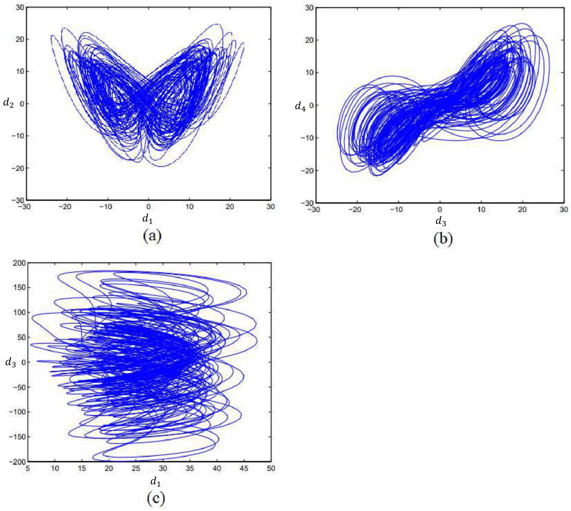

FIGURE 2. The chaotic attractors of *MSD*: (a) $d_1 - d_2$ plane, (b) $d_3 - d_4$ plane, and $d_1 - d_3$ plane.

B. SECRET KEY GENERATION

To generate the secret keys, we need to calculate the initial conditions of *MSD* (Eq. 5). In this work, SHA-512 is used to create the initial conditions. Because SHA-512 calculates the key from the input image, thus generated initial conditions become sensitive towards the plain image. So, a small change to the plain image will also change the initial conditions. Hence, it will provide more security to images. The initial conditions can be generated as follows: i.

1) Apply SHA-512 on then input image to generate 512-bit secret key ρ. Divide ρ into 8-bit blocks and convert to 64 decimal numbers such as $\rho_1, \rho_2, \ldots,$ and ρ_{64}.

2) The control and constant parameters of *MSD* are obtained as

$$\left.\begin{aligned} m &= \frac{1}{256}(\rho_1 \oplus \rho_2 \oplus \rho_3 \oplus \rho_4) \\ l &= \frac{1}{256}(\rho_5 \oplus \rho_6 \oplus \rho_7 \oplus \rho_8) \\ T &= \frac{1}{256}(\rho_9 \oplus \rho_{10} \oplus \rho_{11} \oplus \rho_{12}) \\ q &= \frac{1}{256}(\rho_{13} \oplus \rho_{14} \oplus \rho_{15} \oplus \rho_{16}) \\ e &= \frac{1}{256}(\rho_{17} \oplus \rho_{18} \oplus \rho_{19} \oplus \rho_{20}) \\ t &= \frac{1}{256}(\rho_{21} \oplus \rho_{22} \oplus \rho_{23} \oplus \rho_{24}) \\ a &= \frac{1}{256}(\rho_{25} \oplus \rho_{26} \oplus \rho_{27} \oplus \rho_{28}) \\ p_1 &= \frac{1}{256}(\rho_{29} \oplus \rho_{30} \oplus \rho_{31} \oplus \rho_{32}) \\ p_2 &= \frac{1}{256}(\rho_{33} \oplus \rho_{34} \oplus \rho_{35} \oplus \rho_{36}) \\ h &= \frac{1}{256}(\rho_{37} \oplus \rho_{38} \oplus \rho_{39} \oplus \rho_{40}) \end{aligned}\right\} \tag{6}$$

3) The initial states of *MSD* can be obtained as

$$\left.\begin{aligned} d_1 &= \frac{1}{256}(\rho_{40} \oplus \rho_{41} \oplus \rho_{42} \oplus \rho_{43}) \\ d_2 &= \frac{1}{256}(\rho_{43} \oplus \rho_{44} \oplus \rho_{45} \oplus \rho_{46}) \\ d_3 &= \frac{1}{256}(\rho_{46} \oplus \rho_{47} \oplus \rho_{48} \oplus \rho_{49}) \\ d_4 &= \frac{1}{256}(\rho_{49} \oplus \rho_{50} \oplus \rho_{51} \oplus \rho_{52}) \\ d_5 &= \frac{1}{256}(\rho_{53} \oplus \rho_{54} \oplus \rho_{55} \oplus \rho_{56}) \\ d_6 &= \frac{1}{256}(\rho_{57} \oplus \rho_{58} \oplus \rho_{59} \oplus \rho_{60}) \\ d_7 &= \frac{1}{256}(\rho_{61} \oplus \rho_{62} \oplus \rho_{63} \oplus \rho_{64}) \end{aligned}\right\} \tag{7}$$

where $\oplus$ represents the bit-xor operator.

C. COMPRESSION PROCESS

The compression of plain image I_m of size $R \times C$ is carried out as follows:

Step 1: Apply Nonsubsampled contourlet transform (NSCT) to I_m to obtain the sparse image. It generates the sparse coefficient matrix I_m' with the same size as I_m.

Step 2: In compressive sensing, measurement matrices, i.e., ϕ_1 and ϕ_2 are generated in circular form. These matrices are constructed using the chaotic sequences d_6' and d_7' of *MSD*. To minimize the transient effect, the initial 100 values of d_6' and d_7' are neglected. Thereafter, the obtained chaotic sequences $D_6 = [d_{6_1}, d_{6_2}, \ldots, d_{6_C}]$ and $D_7 = [d_{7_1}, d_{7_2}, \ldots, d_{7_C}]$.

Consider the obtained secret keys are the actual row vectors $\phi_1'(1, N) = D_6$ and $\phi_2'(1, N) = D_7$. The first element of ϕ_1' and ϕ_2' is modified to minimize the correlation between the column vectors. ϕ_1 and ϕ_2 can be obtained as:

$$\left.\begin{aligned} \phi_1'(i,1) &= \alpha_1' \cdot \phi_1'(i-1, C) \\ \phi_1'(i, 2:C) &= \phi_1'(i-1, 1:C-1) \end{aligned}\right\} \tag{8}$$

$$\left.\begin{aligned} \phi_2'(i,1) &= \alpha_2' \cdot \phi_2'(i-1, C) \\ \phi_2'(i, 2:C) &= \phi_2'(i-1, 1:C-1) \end{aligned}\right\} \tag{9}$$

$$\left.\begin{aligned} \phi_1 &= \sqrt{2/R1\phi_1'} \\ \phi_2 &= \sqrt{2/R1\phi_2'} \end{aligned}\right\} \tag{10}$$

Here, $\alpha_1 > 1$ and $\alpha_2 > 1$. $\sqrt{2/R1}$ denotes the normalization factor. The size of ϕ_1 and ϕ_1 is $R1 \times C$ ($R1 = CR \times R$). Here, CR represents the compression ratio of I_m. To calculate the CR see [25].

Step 3: Compress and encrypt the I_m' using 2D-compressive sensing (described in Section III-A) by utilizing ϕ_1 and ϕ_2. The resultant image is I_m'' of size $R1 \times C1$.

Step 4: I_m'' values are then quantized by mapping all elements into integer values. The range of integer is set from 0 to 255. The obtained resultant matrix is I.

$$I = round\left(\frac{255 \times (I_m'' - V_{min})}{V_{max} - V_{min}}\right) \tag{11}$$

Here, V_{max} and V_{min} are the maximum and minimum values of I_m'', respectively. $round(V)$ calculates the nearest integer to V.

D. ROW-WISE PERMUTATION AND DIFFUSION

The row-wise permutation and diffusion on I are described in the Algo. 2. For row-wise, two key streams d_1 and d_2 are used to carry out the permutation and diffusion on each row, respectively. To perform permutation, d_1 of size $3 \times R1$ comprises three index values (see line 3). Based on these index values, each row is shuffled three times. The line 4 shows the shuffled row r_1 which generates from $ndex(1)$ and row of I. Thereafter, r_2 is obtained by shuffling the r_1 using $ndex(2)$. Then, the final permutated row r_3 is gotten by the shuffling the r_2 using $ndex(3)$. For diffusion, bitxor operation is applied on d_2 of size N and final permutated row r_3. It produces a permutated and diffused row r_4 (see line 7). Now, for the next row, r_4 is considered as a keystream. It provides sensitivity and security to the proposed approach. For each row of I, we repeat the same steps. The final output of row-wise permutation and diffusion is I_r.

Algorithm 2 Row-Wise Permutation and Diffusion

```
Input: Compressed image $I$ and chaotic
        sequences$\{d_1, d_2\}$
Output: row-wise permutated and diffused image $I_r$
1  initialize $z = 1$;
2  for $i = 1$ to $R1$ do
3      $ndex = d_1(z : z + 2)$;
4      $r_1 = [I(i, ndex(1) : -1 : 1), I(i, end : -1 :$
         $ndex(1) + 1)]$;
5      $r_2 = [r_1(ndex(2) : -1 : 1), r_1(end : -1 :$
         $ndex(2) + 1)]$;
6      $r_3 = [r_2(ndex(3) : -1 : 1), r_2(end : -1 :$
         $ndex(3) + 1)]$;
7      $r_4 = bitxor(r_3, d_2)$;
8      $d_2 = r_4$;
9      $I_r(i, :) = r_4$;
10     $z = z + 3$;
```

E. COLUMN-WISE PERMUTATION AND DIFFUSION

The column-wise permutation and diffusion is demonstrated in Algo. 3. In this, three key streams such as d_3, d_4, and d_5 are used. d_3 of size $3 \times C1$ is used to perform the permutation on each column. $ndex$ contains three values of d_3 (see line 4). c_1 is obtained by shuffling j^{th} column of I_r using $ndex(1)$ (see line5). c_2 is come after shuffling the c_1 using $ndex(2)$. The final permutated column is obtained by shuffling c_2 using $ndex(3)$ (see line 7). c_3 is diffused using bitxor operation with d_4 (see line 8). The same process is repeated for each column. The final encrypted image obtained after row-wise and column-wise operations is I_c.

Algorithm 3 Column-Wise Permutation and Diffusion

```
Input: permuated and confused image $I_r$ and chaotic
        sequences$\{d_3, d_4, d_5\}$
Output: column-wise permutated and diffused image
         $I_c$
1  initialize $z_1 = 1$;
2  $d_4 = bitxor(d_4, d_5)$;
3  for $j = 1$ to $C1$ do
4      $ndex = d_3(z_1 : z_1 + 2)$;
5      $c_1 = [I_r(ndex(1) : -1 : 1, j), I_r(end : -1 :$
         $ndex(1) + 1, j)]$;
6      $c_2 = [c_1(ndex(2) : -1 : 1), c_1(end : -1 :$
         $ndex(2) + 1)]$;
7      $c_3 = [c_2(ndex(3) : -1 : 1), c_2(end : -1 :$
         $ndex(3) + 1)]$;
8      $c_4 = bitxor(c_3, d_4)$;
9      $d_4 = c_4$;
10     $I_c(:, j) = c_4$;
11     $z_1 = z_1 + 3$;
```

V. PERFORMANCE ANALYSIS

The proposed lightweight image encryption approaches implemented on MATLAB 2020a software with core i7, 2GB graphics card, and 16 GB RAM. The four different biomedical images of size 256 × 256 i.e., computed tomography (CT), brain magnetic resonance imaging (MRI), dermoscopic (DSC), and ultrasound (USC) are considered for testing. For comparative analyses, seven competitive approaches are taken such as GCS [8], IPS [9], CCT [10], PLA [12], VSS [13], LSS [15], and CS [16].

A. VISUAL ANALYSIS

The image encryption approach is considered to be effective when it generates a random-like encrypted image. A random-like encrypted image should not contain any pixel pattern like input biomedical. Histograms are utilized to analyze the pixel distribution.Figure 3 illustrates the visual analysis of the proposed lightweight encryption approach for MIoT. Fig. 3 (a) shows the input CT, MRI, DSC, and USC images. From Fig. 3 (b), it is found that the histograms of input biomedical images contain pixel pattern's details. The resultant encrypted images of the *MSD* based hyperchaotic map are demonstrated in Fig. 3 (c). It is observed that these encrypted images are completely random. Corresponding histograms are presented in Fig. 3 (d). It is observed that the obtained histograms are uniform and do not provide any kind of information about the intensity of pixels. Hence, the attackers are unable to extract any statistical information from encrypted images. The decrypted images corresponding to encrypted images are depicted in Fig. 3 (e). It is found that the decrypted images are like input biomedical images.

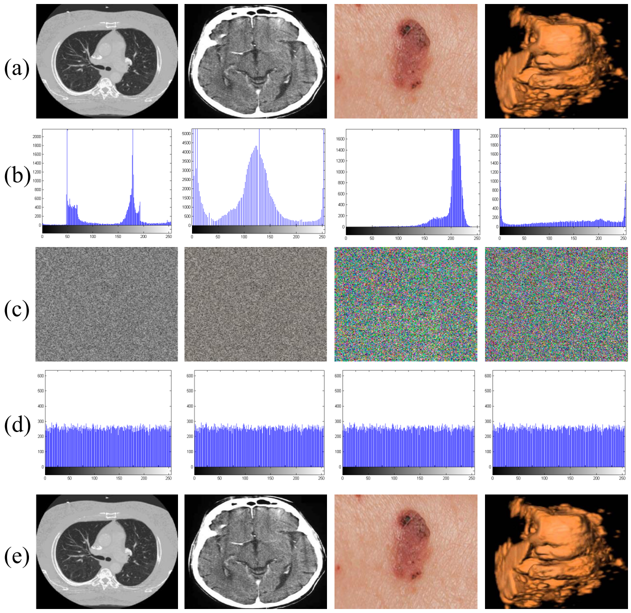

FIGURE 3. Visual analyses: Row (a) Biomedical images, (b) Histograms of respective biomedical images, (c) Encrypted biomedical images, (d) Histograms of encrypted biomedical images, and (e) Decrypted biomedical images.

B. SECURITY ANALYSES

1) STATISTICAL ANALYSES

The statistical analysis of the proposed approach is performed using correlation coefficient, histogram analysis, and entropy.

Entropy is utilized to check the randomness of encrypted images [26]. Entropy can be calculated globally as well as locally. The global entropy (GE) evaluates the randomness of the complete image at once. But the evaluation of local entropy (LE) is different than the GE [27]. To evaluate the LE, firstly, an image is decomposed into blocks (I_b) that contain the fixed amount of pixels (F_p). Then, each block's entropy is evaluated. Thereafter, the local entropy is computed by taking the average of all blocks.

The local and global entropies of the resultant encrypted images are shown in Table 1. Both global and local entropies are found to be close to the ideal value, which is 8. Hence, the encrypted images are completely noisy.

TABLE 1. Global and local entropies of the proposed encryption approach (in bits).

Images	GE	LE No. of pixels $F_p = 1936$	
		$I_b = 30$	$I_b = 40$
CT	7.9997	7.9051	7.9035
MRI	7.9996	7.9062	7.9057
DSC	7.9995	7.9048	7.9039
USC	7.9998	7.9065	7.9055

Histogram analyses are used to show each pixel's intensity distribution of the encrypted images. From Fig. 3 (m)-(p), it can be seen that each pixel of the encrypted image approaches toward 255 value. Hence, the encrypted image' pixels are uniformly distributed. The uniform distribution of histograms can be proved by using the chi-square test [28]. χ^2 value at 0.05 level of significance (χ^2(0.05,255)) is 293.25 [29]. Table 2 depicts the computed χ^2 values of input and encrypted images. χ^2 values of encrypted images are significantly lesser as compared to the theoretical value, i.e., 294. A histogram of encrypted images shows an even distribution.

TABLE 2. χ^2 test of the proposed approach.

Image	χ^2 of Input Image	χ^2 of Encrypted Image
CT	55,456	280.17
MRI	60,600	266.34
DSC	345,140	290.56
USC	72,250	285.33

Attackers can use the correlation information among the adjacent pixels to exploit the encryption approach. Therefore, it is necessary to reduce the correlation among the pixels of an encrypted image. The correlation coefficient including diagonal (D), vertical (V), and horizontal (H) directions of the input biomedical images and encrypted images is shown in Table 3. The correlation values of the input biomedical images approach toward 1 horizontally, vertically, and diagonally. It implies that images are highly correlated horizontally, vertically, and diagonally. This relation is reduced to approximately 0 by the proposed approach. It can be analyzed that the correlation of all encrypted images is near to 0 horizontally, vertically, and diagonally. Hence, the adjacent pixels of the encrypted images are not correlated with each other. Thus, the attackers cannot exploit the statistical information of the encrypted images to break the proposed approach.

TABLE 3. Correlation coefficient analysis of input biomedical images.

Image	Plain images			Encrypted images		
	H	V	D	H	V	D
CT	0.9651	0.8266	0.9921	0.0038	0.0013	-0.0211
MRI	0.9616	0.8444	0.9638	-0.0142	0.0010	0.0007
DSC	0.9641	0.7830	0.9845	0.0003	-0.0012	0.0031
USC	0.9671	0.9817	0.9741	-0.0016	0.0076	0.0009

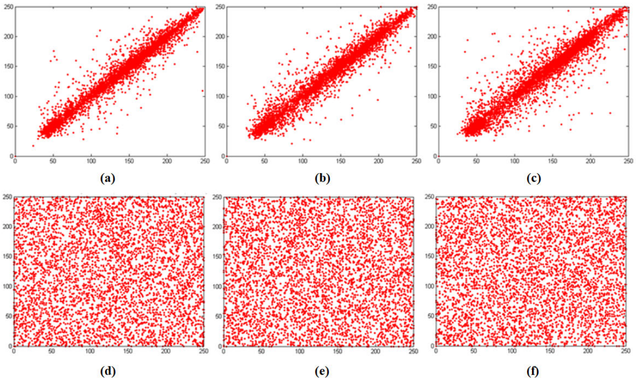

FIGURE 4. Correlation coefficient analyses of red channel of DSC image: (a) Horizontal, (b) Vertical, and (c) Diagonal correlations of actual DSC, and (d) Horizontal, (e) Vertical, and (f) Diagonal correlations of encrypted DSC.

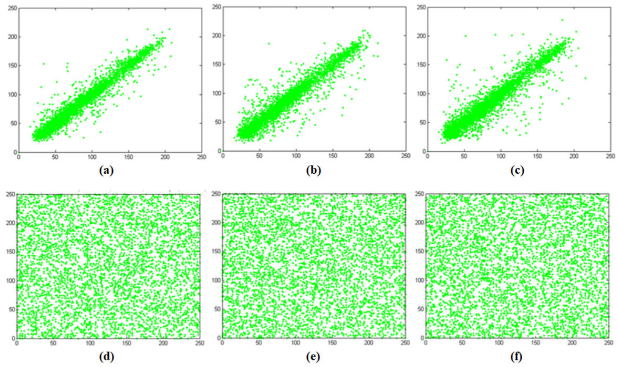

FIGURE 5. Correlation coefficient analyses of green channel of DSC image: (a) Horizontal, (b) Vertical, and (c) Diagonal correlations of actual DSC, and (d) Horizontal, (e) Vertical, and (f) Diagonal correlations of encrypted DSC.

Figure 4 shows that input and encrypted red channels images of DSC image correlations horizontally, vertically, and diagonally. Figures 5 and 6 show the input and encrypted green and blue channels' horizontal, vertical, and diagonal correlations, respectively. Figures 4, 5, and 6 (a)-(c) show the adjacent pixels of input channels are highly correlated. Figures 4, 5 and 6 (d)-(f) show the adjacent pixels of encrypted red, green, and blue channels horizontally, vertically, and diagonally, respectively. It is found that the adjacent pixels are loosely related with each other. Hence, no significant statistical information can be deduced from the encrypted images.

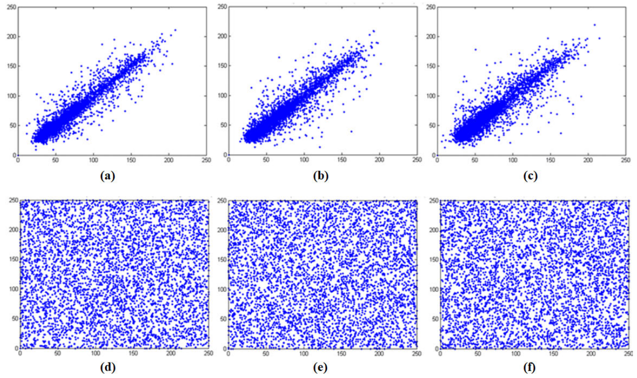

FIGURE 6. Correlation coefficient analyses of blue channel of DSC image: (a) Horizontal, (b) Vertical, and (c) Diagonal correlations of actual DSC, and (d) Horizontal, (e) Vertical, and (f) Diagonal correlations of encrypted DSC.

2) KEY SPACE ANALYSIS

Keyspace is a significant metric to be analyzed to prevent a brute force attack. An attacker uses approximately half of all possible keys in the keyspace analysis to determine the secret key, so the large keyspace is advantageous to resist the brute force attack. Researchers have found that any encryption algorithm can avoid the brute-force attack if the keyspace is more than $2^{100} \approx 10^{30}$.

In the proposed approach, secret keys are generated using *MSD*. It requires 7 initial state variables d_1 to d_7 and 10 control variables l, m, a, T, e, p_1, q, t, p_2, and h to compute the secret keys. Now, we can consider that the initial control and state variables are double precision values (i.e., 10^{-16}). It indicates that d_1 can have more than 10^{16} different values. It is also true for all other state as well control attributes. Thus, the key space of the *MSD* map is approx. 10^{272}. It is a quite large key space. Hence, the *MSD* map cannot be broken through brute-force attack.

3) ANALYSIS OF DIFFERENTIAL ATTACK

An analysis of differential attacks is performed to evaluate the sensitivity of the proposed model to input biomedical images using Unified averaged changed intensity (UACI) and Number of changing pixel rates (NPCR). The maximum value of UACI and NPCR are required to handle the differential attacks. Wu et al. [30] found the critical NPCR and UACI values with two significance levels, i.e., 0.05 and 0.01. Based on significance level 0.05, the critical value of UACI is 33.6447% while the NPCR is 99.5693% for 8-bit images. Similarly, at 0.01 level of significance, the critical value of UACI is 33.2255% and NPCR is 99.5527%. Tables 4 and 5 show that the computed NPCR and UACI values are better than their corresponding critical values. Therefore, the proposed lightweight image encryption approach can efficiently resist differential attacks.

TABLE 4. Theoretical NPCR analysis of the proposed lightweight image encryption approach.

Image	Actual	Theoretical $NPCR$	
		$N^*_{0.01}$=99.5527	$N^*_{0.05}$=99.5693
CT	99.69	✓	✓
MRI	99.59	✓	✓
DSC	99.64	✓	✓
USC	99.67	✓	✓

TABLE 5. Theoretical UACI analysis of the proposed lightweight image encryption approach.

Image	Actual	Theoretical $UACI$	
		$U^{*-}_{0.01}$/ $U^{*+}_{0.01}$ 33.2255/33.7016	$U^{*-}_{0.05}$/ $U^{*+}_{0.05}$ 33.2824/33.6447
CT	33.47	✓	✓
MRI	33.50	✓	✓
DSC	33.49	✓	✓
USC	33.42	✓	✓

The proposed approach is compared with the existing approaches in terms of NPCR and UACI. Tables 6 and 7 show the NPCR and UACI comparative analysis, respectively. The tables show that the proposed approach generates a dissimilar image if there is a tiny modification in the input biomedical image. Hence, the proposed approach is sensitive to small changes in the input biomedical images.

TABLE 6. NPCR analyses of the proposed lightweight encryption.

Techniques	CT	MRI	DSC	USC
GCS [8]	99.51	99.55	99.45	99.42
IPS [9]	99.40	99.44	99.47	99.48
CCT [10]	99.47	99.42	99.50	99.51
ISTLM [18]	99.49	99.50	99.45	99.46
DDNA [19]	99.52	99.47	99.40	99.42
XRF [23]	99.48	99.41	99.45	99.52
CS [16]	99.41	99.46	99.51	99.47
Proposed	99.69	99.59	99.64	99.67

TABLE 7. UACI analyses of the proposed lightweight encryption.

Techniques	CT	MRI	DSC	USC
GCS [8]	33.27	33.38	33.31	33.29
IPS [9]	33.28	33.30	33.23	33.34
CCT [10]	33.39	33.32	33.33	33.25
ISTLM [18]	33.24	33.23	33.32	33.22
DDNA [19]	33.36	33.26	33.35	33.31
XRF [23]	33.22	33.34	33.37	33.28
CS [16]	33.37	33.26	33.27	33.30
Proposed	33.47	33.50	33.49	33.42

4) KEY SENSITIVITY ANALYSIS

Key sensitive analysis is used to check the sensitiveness of the computed secret keys by using Eq. 4 to the initial values.

An image encryption approach needs to generate a entirely separate encrypted image even if tiny modification is made in control parameters. The sensitiveness of the *MSD* map towards initial values is shown in Fig. 7. One secret key (S_k) is obtained using initial states (d_1 to d_7) and constant parameters (l, m, a, T, e, p_1, q, t, p_2, and h). Suppose that the value of y_1 is changed little bit while all other initial values are similar. By utilizing these initial values, another secret key (S'_k) is generated. Then, USC image is encrypted using *MSD* with S_k and S'_k. It generates an encrypted image I_{mc} with S_k and another encrypted image I'_{mc} with S'_k. The difference between I_{mc} and I'_{mc} is shown in Table 8. The values of the table show that I_{mc} and I'_{mc} are identical encrypted images. Hence, the keys obtained using the *MSD* are sensitive to initial control parameters.

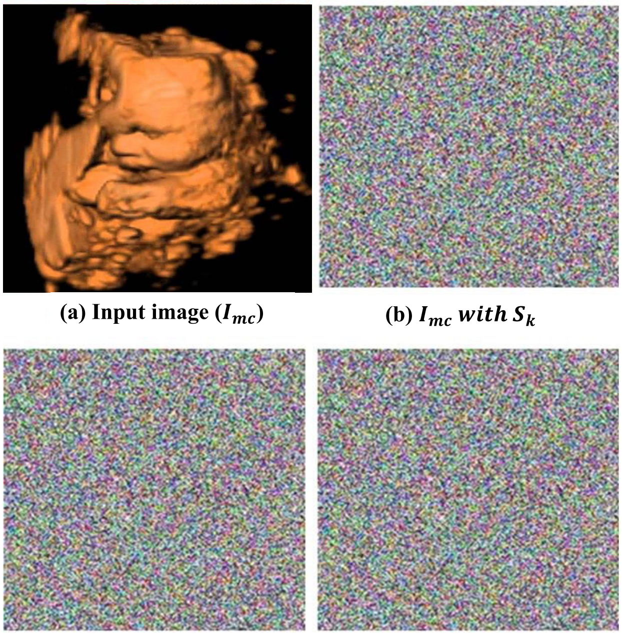
(a) Input image (I_{mc})
(b) I_{mc} with S_k
(c) I'_{mc} with S'_k
(b) $V = I_{mc} - I'_{mc}$

FIGURE 7. Key sensitivity: (a) Input ultrasound (USC) image, (b) encrypted USC using S_k, (c) encrypted USC using S_k', and (d) Subtraction of I_{mc} and I'_{mc}.

TABLE 8. Key sensitivity analysis.

	CT	MRI	DSC	USC
Difference	99.936	99.957	99.979	99.982

C. PEAK SIGNAL TO NOISE RATIO

Peak Signal to Noise Ratio (PSNR) is another measure to evaluate the performance of the image encryption techniques. Maximum PSNR between input I_m and decrypted D_m images states that the significant information of biomedical images is not lost. Thus, PSNR between input images and corresponding decrypted images is desirable to be maximum [31]. Also, an encryption technique is said to be efficient if the computed

PSNR between input and its respective encrypted image is minimum [32].

Table 9 shows that the PSNR between input and their respective encrypted images is minimum. Also, the PSNR between input images and their respective decrypted images is maximum. The comparative analysis between the proposed and competitive image encryption techniques in terms of PSNR between input and their respective decrypted images is shown in Table 10. It demonstrates that the proposed image encryption technique achieves significant PSNR in contrast to the existing techniques.

TABLE 9. PSNR analysis of input and encrypted images.

Images	Between I_m and I_{mc}	Between I_m and D_m
CT	-8.4021	79.2921
MRI	-7.5243	82.1515
DSC	-7.3982	80.4119
USC	-8.0301	83.6470

TABLE 10. Comparative analysis of the proposed technique in terms of PSNR.

Techniques	CT	MRI	DSC	USC
FDHC	52.90	53.49	48.81	57.41
LDCML	51.33	56.49	64.93	58.86
FDCC	50.28	61.83	64.52	53.15
LcLu	49.97	55.10	50.97	64.77
NSGALC	50.84	46.25	47.66	47.66
MOGA	46.49	56.25	49.38	55.12
ILMDE	64.85	49.55	54.19	59.48
PSOGA	53.21	50.97	65.57	46.66
Proposed	67.29	66.15	68.41	69.64

D. NOISE RESISTANCE ANALYSIS

This section evaluates the performance of the proposed image encryption technique against Gaussian attack. It is assumed that the transmission medium may introduce some noise in the encrypted image [33]. Thus, the encryption should have an ability to handle the noise attack in such a way that the decrypted images should contain some information about the input image. In this paper, we have added low, moderate, and high Gaussian noise in encrypted images (see Figure 8 (a)-(c)). The corresponding decrypted images are shown in Figure 8 (d)-(f). It shows that the decrypted images are recognizable even if we add a higher density of Gaussian noise in it (see Figure 8(f)).

E. OCCLUSION ATTACK ANALYSIS

During communication of images, some potential blocks of image may be lost due to malicious destruction or congestion in the network [34]. Occlusion attack is utilized to evaluate the performance of restoring input images from encrypted images even if some blocks or pixels of it has been occluded.

Figure 9 (a)-(c) shows the occlusion attack analysis of the proposed image encryption technique with low, moderate, and high occlusion attacks. It is found that the decrypted images are in a understandable form even if some blocks of encrypted images are occluded (see Figure 9 (e)-(f)).

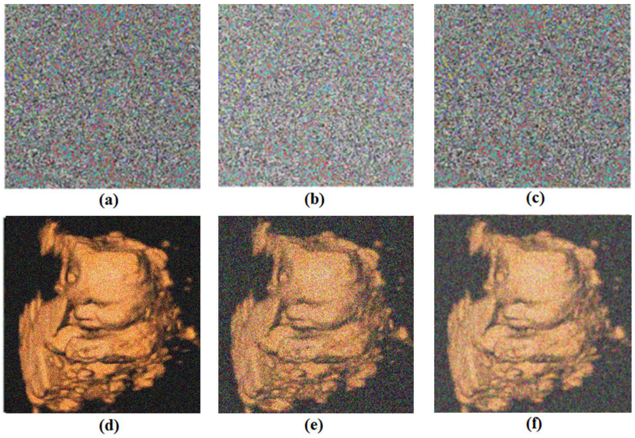

FIGURE 8. Guassian noise analyses: (a) Encrypted image with low Gaussian noise, (b) Encrypted image with moderate Gaussian noise, (c) Encrypted image with high Gaussian noise, (d) Decrypted image of (a), (e) Decrypted image of (b), and (f) Decrypted image of (c).

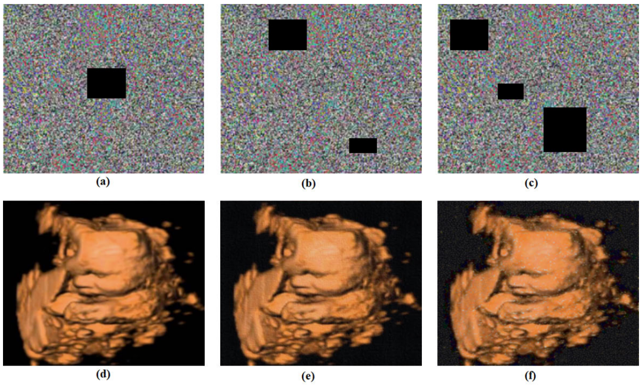

FIGURE 9. Occlusion attack analyses: (a) Encrypted image with low occluded area, (b) Encrypted image with moderate occluded area, (c) Encrypted image with high occluded area, (d) Decrypted image of (a), (e) Decrypted image of (b), and (f) Decrypted image of (c).

VI. CONCLUSION

In MIoT networks, a large amount of biomedical images are transmitted over Internet for their storage and analysis on cloud servers. Due to this, biomedical images are vulnerable to numerous security vulnerabilities. Hence, a lightweight biomedical image encryption approach was developed using *MSD* and compressive sensing. *MSD* was designed by modifying 7D hyperchaotic map to make it more dynamic and complex. The initial conditions for *MSD* were generated using SHA-512 which enforce the sensitivity of proposed approach to input images. Compressive sensing was improved by using NSCT and measurement matrices were generated using the secret keys obtained from *MSD*. Finally, to generate encrypted images, the diffusion and permutation were carried out row and column-wise on compressed images using secret keys obtained from *MSD*. The performance analysis proved that the proposed lightweight encryption achieved better performance in terms of robustness, security, and computational speed as compared to the existing approaches in terms of entropy, NPCR, UACI, and PSNR by 0.07%, 0.13%, 0.11%, and 2.35%, respectively.

CONFLICT OF INTEREST

The authors declare no conflict of interest regarding the publication of this paper.

REFERENCES

[1] Y. Ding, G. Wu, D. Chen, N. Zhang, L. Gong, M. Cao, and Z. Qin, "DeepEDN: A deep-learning-based image encryption and decryption network for Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 3, pp. 1504–1518, Feb. 2021.

[2] 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 Things J.*, vol. 6, no. 6, pp. 10177–10190, Dec. 2019.

[3] H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain, and T. Hayajneh, "Secured data collection with hardware-based ciphers for IoT-based healthcare," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 410–420, Feb. 2019.

[4] F. Rezaeibagha, Y. Mu, K. Huang, and L. Chen, "Secure and efficient data aggregation for IoT monitoring systems," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 8056–8063, May 2021.

[5] D. Wang, T. Song, L. Dong, and C. Yang, "Optimal contrast grayscale visual cryptography schemes with reversing," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2059–2072, Dec. 2013.

[6] B. Ferreira, J. Rodrigues, J. Leitão, and H. Domingos, "Practical privacy-preserving content-based retrieval in cloud image repositories," *IEEE Trans. Cloud Comput.*, vol. 7, no. 3, pp. 784–798, Jul. 2019.

[7] Q. Yang, D. Zhu, and L. Yang, "A new 7D hyperchaotic system with five positive Lyapunov exponents coined," *Int. J. Bifurcation Chaos*, vol. 28, no. 5, May 2018, Art. no. 1850057.

[8] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan, and B. Balusamy, "Securing data in Internet of Things (IoT) using cryptography and steganography techniques," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 50, no. 1, pp. 73–80, Jan. 2020.

[9] T. Xiang, Y. Yang, H. Liu, and S. Guo, "Visual security evaluation of perceptually encrypted images based on image importance," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 11, pp. 4129–4142, Nov. 2020.

[10] V. Itier, P. Puteaux, and W. Puech, "Recompression of JPEG crypto-compressed images without a key," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 30, no. 3, pp. 646–660, Mar. 2020.

[11] M. Sasaki and Y. Watanabe, "Visual secret sharing schemes encrypting multiple images," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 2, pp. 356–365, Feb. 2018.

[12] K. Muhammad, R. Hamza, J. Ahmad, J. Lloret, H. Wang, and S. W. Baik, "Secure surveillance framework for IoT systems using probabilistic image encryption," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3679–3689, Aug. 2018.

[13] K. Lee and P. Chiu, "Digital image sharing by diverse image media," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 1, pp. 88–98, Jan. 2014.

[14] T. Xiang, S. Guo, and X. Li, "Perceptual visual security index based on edge and texture similarities," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 5, pp. 951–963, May 2016.

[15] L. Bao, S. Yi, and Y. Zhou, "Combination of sharing matrix and image encryption for lossless (k, n)-secret image sharing," *IEEE Trans. Image Process.*, vol. 26, no. 12, pp. 5618–5631, Dec. 2017.

[16] L. Li, G. Wen, Z. Wang, and Y. Yang, "Efficient and secure image communication system based on compressed sensing for IoT monitoring applications," *IEEE Trans. Multimedia*, vol. 22, no. 1, pp. 82–95, Jan. 2020.

[17] S. Beugnon, W. Puech, and J. Pedeboy, "Format-compliant selective secret 3-D object sharing scheme," *IEEE Trans. Multimedia*, vol. 21, no. 9, pp. 2171–2183, Sep. 2019.

[18] 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, pp. 37855–37865, 2021.

[19] P. T. Akkasaligar and S. Biradar, "Selective medical image encryption using DNA cryptography," *Inf. Secur. J., A Global Perspective*, vol. 29, no. 2, pp. 91–101, Mar. 2020.

[20] X. Liu, X. Yang, Y. Luo, and Q. Zhang, "Verifiable multikeyword search encryption scheme with anonymous key generation for medical Internet of Things," *IEEE Internet Things J.*, vol. 9, no. 22, pp. 22315–22326, Nov. 2022.

[21] P. Zeng, Z. Zhang, R. Lu, and K. R. Choo, "Efficient policy-hiding and large universe attribute-based encryption with public traceability for Internet of Medical Things," *IEEE Internet Things J.*, vol. 8, no. 13, pp. 10963–10972, Jul. 2021.

[22] H. Lin, C. Wang, L. Cui, Y. Sun, C. Xu, and F. Yu, "Brain-like initial-boosted hyperchaos and application in biomedical image encryption," *IEEE Trans. Ind. Informat.*, vol. 18, no. 12, pp. 8839–8850, Dec. 2022.

[23] F. Masood, M. Driss, W. Boulila, J. Ahmad, S. U. Rehman, S. U. Jan, A. Qayyum, and W. J. Buchanan, "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations," *Wireless Pers. Commun.*, vol. 127, pp. 1–28, May 2021.

[24] A. L. Da Cunha, J. Zhou, and M. N. Do, "The nonsubsampled contourlet transform: Theory, design, and applications," *IEEE Trans. Image Process.*, vol. 15, no. 10, pp. 3089–3101, Oct. 2006.

[25] Q. Xu, K. Sun, C. Cao, and C. Zhu, "A fast image encryption algorithm based on compressive sensing and hyperchaotic map," *Opt. Lasers Eng.*, vol. 121, pp. 203–214, Oct. 2019.

[26] S. M. Wadi and N. Zainal, "Decomposition by binary codes-based speedy image encryption algorithm for multiple applications," *IET Image Process.*, vol. 9, no. 5, pp. 413–423, May 2015.

[27] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.

[28] X. Zhang, X. Fan, J. Wang, and Z. Zhao, "A chaos-based image encryption scheme using 2D rectangular transform and dependent substitution," *Multimedia Tools Appl.*, vol. 75, no. 4, pp. 1745–1763, Feb. 2016.

[29] H. Liu, F. Wen, and A. Kadir, "Construction of a new 2D Chebyshev-Sine map and its application to color image encryption," *Multimedia Tools Appl.*, vol. 78, no. 12, pp. 15997–16010, Jun. 2019.

[30] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Select. Areas Telecommu.*, vol. 1, pp. 31–38, Apr. 2011.

[31] N. Rawat, B. Kim, and R. Kumar, "Fast digital image encryption based on compressive sensing using structurally random matrices and Arnold transform technique," *Optik*, vol. 127, no. 4, pp. 2282–2286, Feb. 2016.

[32] J. Chen, Z.-L. Zhu, L.-B. Zhang, Y. Zhang, and B.-Q. Yang, "Exploiting self-adaptive permutation–diffusion and DNA random encoding for secure and efficient image encryption," *Signal Process.*, vol. 142, pp. 340–353, Jan. 2018.

[33] M. Kaur, V. Kumar, and L. Li, "Color image encryption approach based on memetic differential evolution," *Neural Comput. Appl.*, vol. 31, no. 11, pp. 7975–7987, Nov. 2019.

[34] M. Kaur and V. Kumar, "Beta chaotic map based image encryption using genetic algorithm," *Int. J. Bifurcation Chaos*, vol. 28, no. 11, Oct. 2018, Art. no. 1850132.