IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 19, 2021, accepted December 15, 2021, date of publication December 27, 2021,
date of current version January 4, 2022.

Digital Object Identifier 10.1109/ACCESS.2021.3138718

A Robust Chaos-Based Technique for Medical Image Encryption

IBRAHIM YASSER, ABEER T. KHALIL, MOHAMED A. MOHAMED, AHMED S. SAMRA, AND FAHMI KHALIFA, (Senior Member, IEEE)
Electronics and Communications Engineering Department, Faculty of Engineering, Mansoura University, Mansoura 35516, Egypt
Corresponding author: Fahmi Khalifa (fahmikhalifa@mans.edu.eg)

ABSTRACT Transmission and storage of medical data using cloud-based Internet-of-health-systems (IoHS) necessitate important prerequisites, such as secrecy, legitimacy, and integrity. This paper recommends a novel hybrid encryption/decryption scheme that can be applied in e-healthcare, or IoHS, for the protection of medical images. The proposed system explores innovative perturbation algorithms that utilize novel chaotic maps. The proposed perturbation-based data encryption is employed in both rounds of confusion and diffusion to cope the drawbacks of traditional chaos-based confusion and diffusion architectures. Particularly, (i) the new maps parameters and chaotic sequences are used to control the permutation and diffusion properties of the scheme, and (2) the derived properties control pixel shuffling and operations of substitution. Different techniques and tests are used to analyzed the chaotic behaviors of the proposed system, including the bifurcation diagram, Lyapunov exponents, as well as the NIST and DIEHARD tests. Moreover, evaluation using various test images indicated that the proposed cryptosystem is fast, have high efficiency, showed high robustness and protection of medical images, and documented the good ability to withstand a variety of cyber-attacks. Furthermore, quantitative results using benchmark color and greyscale images prove the high security levels, sensitivity, and low residual intelligibility with high quality recovered data of our technique than several typical and state-of-the-art encryption schemes. This has been documented using statistical and security analysis metrics, such as number of pixels change rate (NPCR, 99.814%), unified average changing intensity (UACI, 33.694%), peak signal-to-noise-ratio (PSNR, 7.723), and Shannon entropy (7.998).

INDEX TERMS Chaotic maps, cryptography, medical image encryption, randomness tests, security analysis.

I. INTRODUCTION

In the era of exponential growth of communications technologies, security of data, in particular medical data, is of great interest. Cloud-based Internet-of-heath systems (IoHS) are being increasingly used to store patients data to make them remotely accessible at different facilities/locations. The stored and/or transferred data include sensitive identifiable information (e.g., names, address and the other health records) in addition to medical scans (i.e., medical images and physician reports). Non-authorized access to such data is catastrophic and thus, the security of patient data is of immense importance [1]. Storage and/or transfer of medical images not only requires secrecy, but also legitimacy and integrity as prerequisites [2]. Fortunately, cryptography algorithms can be exploited to ensure the required security prerequisites, by medical image scrambling to fulfill encryption. Validness and uprightness of a given cryptosystem are eventually assessed using various computerized marks.

Early image encryption methods are primarily based on off-the-shelf data encryption technologies [3], [4], e.g., data encryption standard (DES), advanced encryption standard (AES) [5], etc. However, those approaches are shown to be low in efficiency and anti-attack capabilities [4], [6]. To increase encryption efficacy, other advanced methods have been introduced in literature. Examples of the developed and utilized methods include the one-time keys methods (e.g. [7]), bit-level permutation techniques (e.g., [8]), and deoxyribonucleic acid (DNA) rule-based schemes (e.g., [9]–[12]). However, one-time keys-based methods do not have additional input parameters to control the encryption process other than the plain image and the input key, which limits wide applicability range. Recent advanced schemes utilized novel theories, such as chaotic maps

The associate editor coordinating the review of this manuscript and approving it for publication was Lo'ai A. Tawalbeh.

(e.g., [13]–[17]), and quantum maps and harmonics (e.g., [18], [19]). More specifically, chaos theory-based methods have attracted researcher attentions due to their inherent advantages over conventional non-chaotic counterpart. Particularly, they are quicker, easier to enforce, and have greater key space, i.e., a wide encryption values' variety [20], [21]. Additional attractive characteristics include initial value-dependency, unpredictability, pseudorandomness, and ergodicity. Those characteristics make chaotic systems more desirable as they have great encryption potentials similar to ideal cryptosystems [16].

Since the introduction of chaotic system by Lorenz in [22], various chaotic-based research have been developed to meet the demand for effective, secure, and storage/ transmission of digital data. Schemes for both greyscale and color images have been introduced in different applications with the ultimate goal of high robustness and reduced security breach risks. Earlier chaos-based encryption schemes employ only a single-level security by employing a single chaotic map, i.e., one-dimensional (1D) systems. Despite their realistic realizability and straightforward deployment, they have limited control parameters, and suffer from the lack of restricted chaotic ranges and vulnerability to attacks [23]. For more efficient encryption, variant of high dimensional schemes have been proposed in literature with excellent chaotic features and more complexity and unpredictability due to the higher number of controlling variables [16]. A review of the recent literature-related work will be provided in the next section.

II. RELATED WORK

In literature, various chaotic-based research work have been developed to enhance schemes' robustness and to reduces security breach risks. Zahmoul *et al.* [24] introduced a modified beta-chaotic map to produce various sequences in permutation, diffusion, and substitution. The results showed the capability of the scheme to enhance encryption efficiency. Yayuz *et al.* [25] proposed a two-map-based scheme to properly apply the concepts of chaos and diffusion to images of some entropy. Resistance to differential attacks is improved by employing additional exclusive or circular rotation of the cipher pixels' values. Despite the effort to achieve a more ideal effect, their system exhibits a high computational cost. Wang *et al.* [26] integrated two sine maps to enhance the 1D chaotic map and to overcome the chosen plain-text attacks. However, their scheme used limited key space and thus is still not secure. A hybrid framework by Parvaz and Zarebnia [27] combined logistic, sine and tent maps. Although, they have shown that their algorithm is secure and realistic, the encryption capabilities were not satisfactory. Wu *et al.* [28] suggested a two-dimensional (2D) Hénon-Sine map (2D-HSM) in combination with DNA approach. Diffusion was achieved by the DNA and 2D-HSM to overwrite image pixels. A chaotic cipher approach by Amina and Mohamed [29] is proposed and customized in medical images application. Their method included modules that could be interactive: chaotic confusion and pixel diffusion. Similar to [28], an encryption scheme by Lou and Ge [30] utilized the DNA method for diffusion of the image pixels and permuted using a 2D-HSM.

Color-based encryption has been the area of extensive research in recent years. For example, Liu *et al.* [31] proposed an image encryption algorithm for color images based on the recent Chebyshev-Sine 2D map. It achieved a desired effect after two rounds by an exclusive OR (XOR) avalanche operation. Another color-based encryption algorithm that uses a hyperchaotic system and blocks permutation was proposed by Cheng *et al.* [32]. It was realized by mixing the components red (R), green (G) and blue (B) to strengthen the dependence of each element. Wang *et al.* [33] proposed an encryption system for color image based on the Lorenz system and DNA permutation. It used chaotic pseudo-random sequences depending on plain text images and secret keys. In addition, the DNA permutation subtraction operations can completely break the bit planes of the plain-text image. A symmetric plaintext-related encryption system for color image was developed by Huang *et al.* [34]. They combined the permutation and diffusion stages into a single inseparable process, termed as "permutation-diffusion-simultaneous operation (PDSO). A minimal encryption round algorithm was developed by Khan and Masood [35] using several chaotic maps. The multiple chaotic map provided projected encryption scheme with confusion and diffusion capability. Wang *et al.* [36] proposed encryption algorithm, an improved model of customized globally coupled map lattices (CGCML) chaos. The hash function SHA-256 was used to generate initial values that establish the relationship between plain images and CGCML cipher images. Younas and Khan [37] proposed a new structure called reverse left almost semigroup (LA-semigroup) by applying confusion to the diffusion characteristics with discrete and continuous chaotic structures. A cyclic redundancy check (CRC) and a nine-palace map encryption algorithm for color image chaos was introduced by Xiong *et al.* [38]. The pixel data of the plain image have been moved and reshaped based on the nine-palace map theory. A binary sequence of the three RGB channels is constructed and the CRC code generation algorithm is then employed to cyclically shift the sequence.

In summary, various algorithms and techniques have been developed and introduced for efficient data security, each of which has its advantages, disadvantage, and application domain. Time complexity, dynamical behavior, computational overhead, robustness to attacks, and security are the main criteria used for evaluation and choice. Since in the IoHS patients data are stored on the cloud to be accessible at different facilities, its security is of immense importance.

The work presented in this paper proposes an improved encryption algorithm that can be applied and utilized in a secure e-healthcare system for the security of medical data, see Fig. 1. The main objective is to develop a user-friendly data encryption scheme with low residual consistency, key sensitivity, and good quality of the data retrieved by chaotic maps. To achieve our goal, two novel 2D modification models

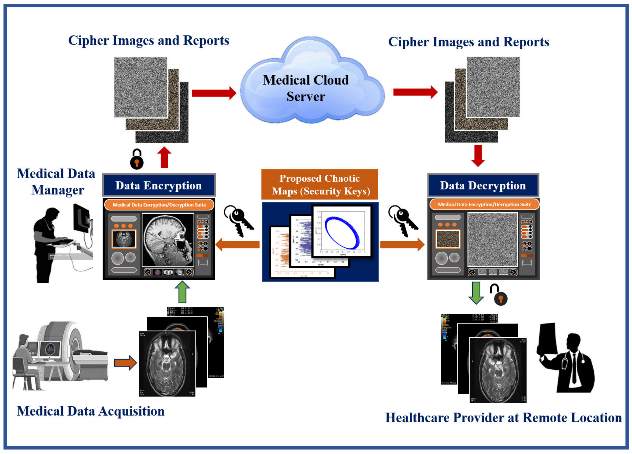
Cipher Images and Reports
Medical Cloud Server
Cipher Images and Reports
Medical Data Manager
Data Encryption
Medical Data Encryption/Decryption Suite
Proposed Chaotic Maps (Security Keys)
Data Decryption
Medical Data Encryption/Decryption Suite
Medical Data Acquisition
Healthcare Provider at Remote Location

FIGURE 1. Schematic illustration of a generic secure cloud-based internet-of-heath systems (IoHS).

are proposed that generate random chaotic sequence matrices, for which chaotic behaviours have been analyze and validated using the bifurcation diagram and Lyapunov exponent. To test the applications of the proposed maps, a novel image encryption algorithm consisting of a two-run confusion-diffusion architecture is proposed. The proposed system incorporates other input parameters besides the plain image and the secret key, to permit controlling the encrypted data values without affecting the secret keys. Therefore, the suggested algorithm breaks the limitation of those based on one-time keys scheme. Moreover, our algorithm can encrypt many images securely and speedily using the same key. Experimental results and security review indicate that the proposed maps could encrypt digital images with high protection and a good ability to withstand a variety of attacks. Moreover, dynamic analysis and sample entropy algorithm show that the proposed map is hyperchaotic overall with high complexity and high sensitivity.

The reminder of this manuscript is sectioned as follows. In Section III, details of proposed chaotic maps characteristics and behaviours are given. This is followed by details of the proposed image encryption/decryption system and its full description in Section IV. Simulation experiments and extensive quantitative and qualitative evaluations of the proposed cryptosystem as well as comparison with state-of-the-art (SOTA) techniques are presented using both medical and benchmark images in Section V. Finally, the concluding remarks are given in Section VI.

III. PROPOSED CHAOTIC MAPS

Modern cryptography-related research work is increasingly adopting chaos algorithms due to their inherent characteristics/attributes, including: (i) high sensitivity to the initial conditions and control parameters, (ii) unpredictability of the orbital evolution, and (iii) high encryption rate due to the simplicity of the hard and software implementation [39].

In this work, we propose two novel 2D chaotic maps for a robust medical images and/or data encryption pipeline. The proposed framework is a discrete-time, nonlinear approach with unique dynamical chaotic behavior. Because of chaos inherent unrepeatability and ergodicity proprieties, searches at higher speeds can be performed compared with probability distribution-based algorithms, i.e., stochastic search methods [40]. Among different possible maps, two novel maps are proposed and investigated for medical image encryption. The chaotic characteristics and behaviours will be analyzed using Lyapunov and bifurcation analysis.

By definition, a chaotic map is any function that exhibit chaotic behavior. The chaotic nature of the proposed maps defining the mapping of a given point (x_n, y_n) to a new position (x_{n+1}, y_{n+1}) is controlled mathematically by:

$$\begin{aligned} y_{n+1} &= y_n - r * \tanh x_n \\ x_{n+1} &= \sin x_n + \cos y_n \qquad (1) \\ y_{n+1} &= b * x_n^2 \\ x_{n+1} &= x_n + {y_n}^2 - a * r \qquad (2) \end{aligned}$$

The first proposed map, Eq. (1), represents a novel 2D financial model and is shown in Fig. 2 (a). Namely, it represents a new non-linear dynamic model, where (x_n, y_n) mapping is controlled by the r parameter during an iterative process, determined by n. On the other hand, the second proposed map (Fig. 2 (d)) is considered as a novel extension of the well-known logistic map, and its chaotic nature is close to the Henon map mathematical expression, but with three control parameters a, b, and r. The generation of the such maps starts by selecting one of the models defined by Eqs. (1) or (2) and setting initial system parameters (n, the upper and lower limits, the number of dimensions, and the fitness function). Then, maps initial positions x_0, and y_0 are randomly initialized. Finally, an iterative process of n times is followed to update x_{n+1} and y_{n+1}.

Each of the proposed maps has an extraordinary signature as shown in Fig. 2, which can be a special attraction feature. In addition, the dynamic behaviours of maps are characterized by a discontinuous motion and non-smooth orbits. The proposed scheme uses an iterative process to encode a series of bytes, which is a 1D converted version of the original two-dimensional image. The proposed chaotic functions are used as described in Eqs. (1) or (2). One is used for changing the pixels positions while the other is used to change the pixel density values. Together, these functions include the mergers and acquisitions required for encryption, and the algorithm is supported by some logical processes for increasing safety and reduce encryption time.

In order to investigate the chaotic behaviors of the proposed maps, bifurcation and Lyapunov diagrams are exploited. Figures 2(b) and (c) depict the bifurcation and Lyapunov exponent, respectively, for the first map. As demonstrated in this figure, the map has multiple convergence regions (e.g., at $r \in [0.0, 4.0]$, $r \in [6.7, 8.0]$ and so on) and also multiple bifurcation regions (e.g., at $r \in [8.0, 8.5]$ and so on). The chaos regions are at $r \in [5.3, 6.7]$, $r \in [8.5, 9.2]$, $r \in [9.9, 13.0]$, $r \in [14.3, 19.2]$, and so on, despite the small

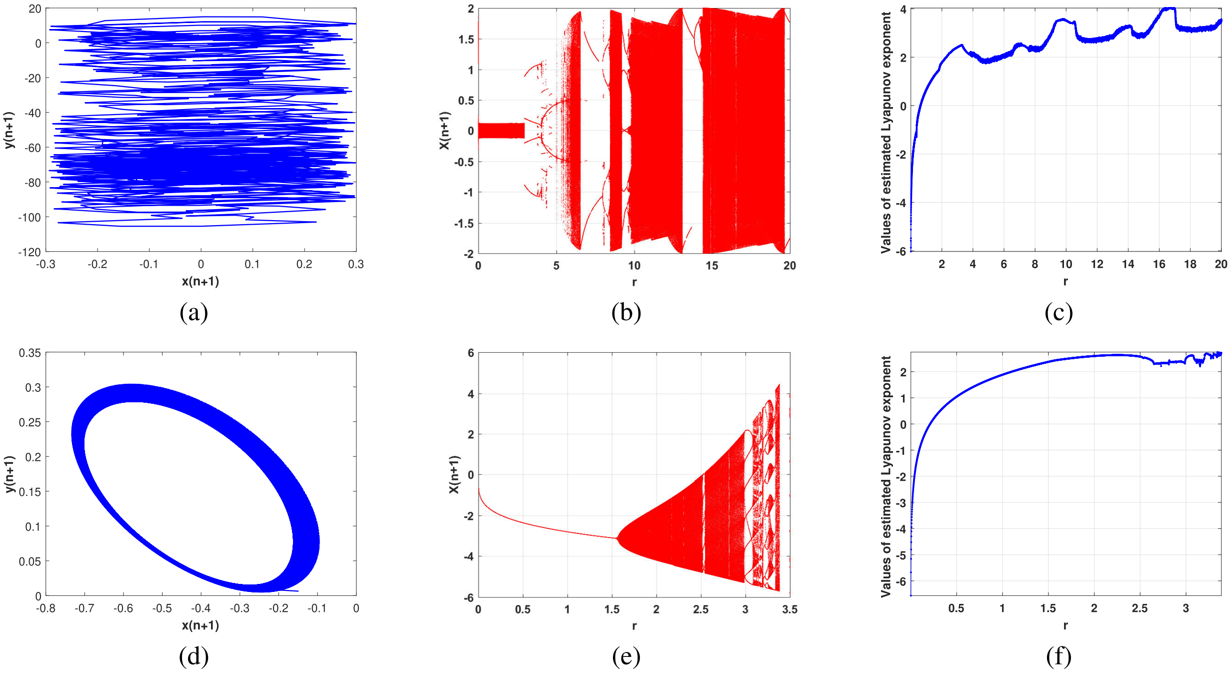

FIGURE 2. 2D-(x, y) phase plots of the proposed maps and their respective bifurcation (b,e) and Lyapunov exponent (c,f) diagrams. The map in (a) is obtained by Eq. (1) with $r = 17.0$; and that in (d) is obtained by Eq. (2), $a = 0.5$, $b = 0.3$, and $r = 2.35$. Simulated maps are obtained with $x_0 = y_0 = 0.1$, and the # of iteration n is 1000.

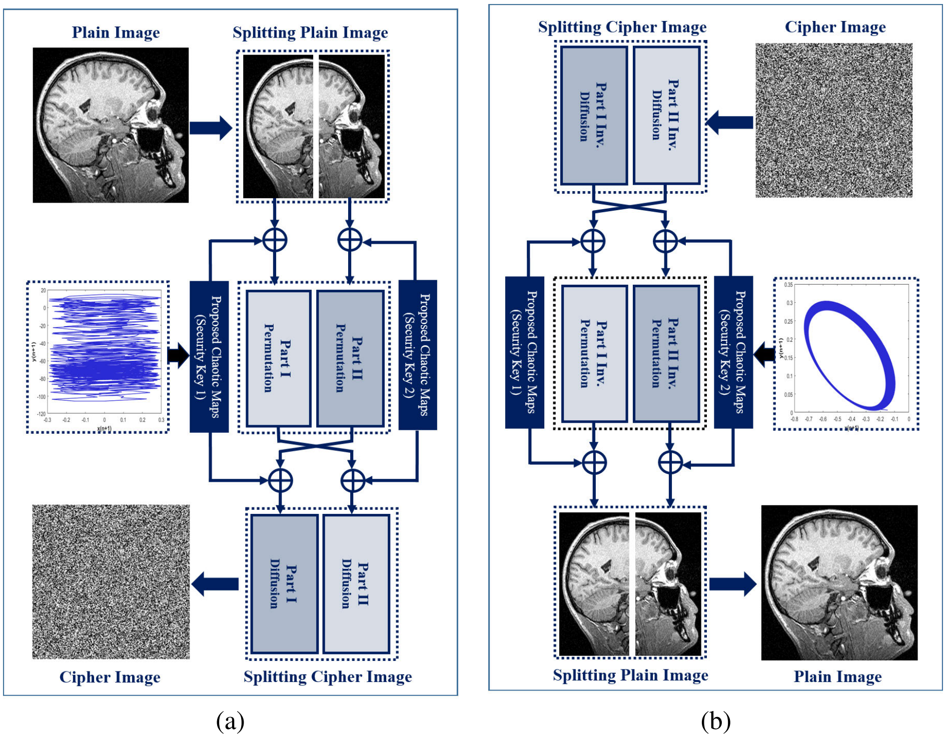

FIGURE 3. Flow diagram illustrating the (a) encryption and (b) decryption stages of the proposed scheme.

places of assembly and bifurcation, where chaotic behavior occurs. In Fig. 2(c), the Lyapunov exponent is depicted for the first map. As readily seen, the Lyapunov has a positive incentive in all estimates r despite a few plural and bifurcation ranges. After that, the proposed map demonstrates turbulent behavior in the rest of the range. The maximal Lyapunov exponent (MLE) of the first map is 4.0. Similarly, the bifurcation and Lyapunov diagrams are constructed for the second proposed map and are shown in Fig. 2(e) and 2(f), respectively. As Fig. 2(e) shows, the bifurcation graph of the second chaotic map has three distinct parts: (i) conversions area at $r \in [0, 1.51]$; (ii) the bifurcation region at $r \in [2.9, 3.1]$; and (iii) the local chaos region at $r \in [1.51, 2.9]$, and $r \in [3.1, 3.2]$ where the chaotic behaviour happens. Lyapunov diagram is depicted in Fig. 2(f), where Lyapunov exponents are less than zero at $r \in [0.0, 0.2]$. But Lyapunov exponents are positive and consequently tumultuous when $r \in [0.2, 3.4]$. Finally, the MLE of the second proposed map is 3.0.

IV. PROPOSED ENCRYPTION/DECRYPTION SCHEME

We propose a novel chaos-based image encryption/ decryption scheme. The core of the proposed algorithm employs an image splitting process, where the pixels of a given image I to be encrypted are divided into multiple portions (I_s, $s \geq 2$). Since we introduce two novel key maps, we choose $s = 2$, such that each image half is encoded using one of the proposed maps. Generally any number of splits can be used and different maps (or a combinations of the maps) can be used for encoding different image portions. The idea behind such process is that individual image portions/splits convey no valuable information, while in the same time an adequate set I_s will, at least partially, help to regenerate I. Although being an effective approach, the recovered image may suffer poor quality due to contrast and colors loss. To partially overcome such limitation, a new and fast scheme is proposed utilizing novel chaotic keys that have the advantage of less error chance in encryption/ decryption stages, thus can maintain the quality of the recovered image. Additionally, the proposed schemes have low execution-time and bandwidth requirements, while also keeping resist against attacks. To fully encrypt an image, two phases of permutation (i.e., confusion) and diffusion operations are employed. Both operations are designed in such a way that chaotic states and plain image data are used to change pixel positions and substitute pixel values, respectively, which leads to a noise-like cipher image. The encryption and decryption operations are fully described next and are schematized in Fig. 3.

A. ENCRYPTION PROCESS

Figure 3(a) depicts the flow diagram of our chaos-based medical image encryption algorithm. A given input plain image (size $H \times W \times D$), is converted into a 1D matrix by concatenating the image pixel values in a columns-wise manner. Here H and W are the height and width, respectively, and D is the image depth, i.e., $D = 1$ for greyscale images and $D = 3$ for color images. After that, the constructed 1D matrix is then split into two equal halves (P_1 and P_2 each of length $(H \times W \times D)/2$ for processing. In the coding system provided, the two proposed maps are utilized for the encryption of split parts. Suggested maps are given by Eqs. (1) and (2) where r, a, and b are the external parameters that determine the maps chaotic behavior and are used in the encryption system as a part of the keys. As previously mentioned, individual maps or their combinations can be used for encoding individual image splits.

For the **permutation process**, the proposed maps are used to create turbulent groups and then sort these numbers in an up or down order of the change key number. The chaotic sequences are sort into the network of records that are used to rearrange the original image to get the thinned image. When the arranged image is obtained, the relationship between the neighboring pixels is completely disrupted and the image cannot be fully recognized. In this way the permuted image is frail against attacking facts and a normal content attack is achieved [41]. Therefore, the dispersion method was used to improve the security. During the **diffusion process**, the provision step is implemented on the permutation halves/intermediate cipher images using the proposed chaotic maps (one for each half) to perform nonlinear transforms of the pixel values. In our algorithm, image pixel's position is considered as a random variable and its time-space probability density is governed by an advection-diffusion equation [42]. Pixel modifications is controlled by both the corresponding key stream element and the previous cipher-pixel value. Thus, any small change in a single pixel can spread out to all subsequent pixels [42]. In total, exact details of our encryption procedure is summarized in algorithm 1.

Algorithm 1 A Step-Wise Grey-Scale Image Encryption Scheme

The input is the plain image $\mathbf{P_i}$ (size $H \times W$) and the output is the encrypted image $\mathbf{C_i}$. leftmargin=10pt

1) **Convert** $\mathbf{P_i}$ into a 1D vector of pixels and **Split** it into P_1 and P_2 vector of size $H \times W/2$ each.
2) **Execute** Eqs. (1) and (2) to generate chaotic sequence.
3) **Iterate** Step (2) n times for scrambling P_{1p} and P_{2p} for P_1 and P_2, respectively.
4) **Compute** the next quantized chaotic pair for P_1 with the first chaotic sequence using the 1^{st} proposed map to scramble P_{1p}, and the 2^{nd} proposed map to scramble P_{2p} for P_2 with the second chaotic reiterate this step n times (when the scrambling of last row or the last column has been done, switch to the first row or the first column over again).
5) **Permute** S_{k_i} using the proposed maps for the secret key.
6) **Construct** the new vector of mistook pixels $S_{P_i} = S_{K_i}$ (index, size $=H \times W/2$).
7) **Adjust** and change S_{P_i} realizing that every component of level gray ranges in [0,255] utilizing the proposed chaotic maps interchangeably with the Step (2), and the accompanying condition: $S_{P_i}(t) = \text{mod}(\text{round}(10^{12} S_{P_i}(t)), 256)$, where $1 \leq t \leq H \times W/2$.
8) **Create** the diffused vector $S_{D_i} = S_{P_i} \oplus S_{K_i}$ ($\oplus$ is the bit-wise XOR)
9) **Combine** both encrypted halves and mix the combined image pixels.
10) **Create** the final matrix with cipher image C_i = reshape (S_{D_i}, H, W)

B. DECRYPTION PROCESS

Decoding, or decryption, process is simply the opposite procedure of the encryption stage. The schematic depiction of the our decryption stage appears in Fig. 3(b). Using the same mysterious keys, it tends to generate turbulent record sets and generate disordered vectors created in the encryption process. The decryption procedures starts with inverse diffusion and confusion, and ends with combination. Initially, we convert the encoded image C to a 2D matrix of size $H \times W$, and at mid point we create a diffuse inverted vector. Also, we get the standard alternating vector and reconfigure it in two parts (P_{1p}, P_{2p}). Finally, the inverse level for each partial area (P_1, P_2) using the disorganized recording arrangement and obtaining the original image P using a combination. Algorithm 2 summarizes the decryption stage.

```
Algorithm 2 Proposed Decryption Process
The input is the encrypted image $\mathbf{C_i}$ and the output is the plain image $\mathbf{P_i}$.
  1) Generate the deshuffled vector $S_P = S_D \oplus S_K$ ($\oplus$ is the bit-wise XOR operation).
  2) Generate each of the permutated vector $S_P = S_K$ (index)
  3) Obtain the permutation sub-bands($P_{1p}$,$P_{2p}$).
  4) Construct $P_1$,$P_2$ by reshaping vector components and utilizing the chaotic index sequence.
  5) Combine recovered halves, $P_1$,$P_2$, to get $\mathbf{P_i}$.
```

V. EXPERIMENTAL RESULTS

The proposed encryption/decryption pipeline has been implemented using the novel maps and its evaluation has been conducted on two phases. In the first phase, diverse medical MRI and CT scans (e.g., brain, lung, kidney) were used. Secondly, for the purpose of evaluating the robustness of our pipeline against other (SOTA) literature techniques we use the benchmark color and greyscale images. The images used for testing include Lena, Cameraman, Baboon, and peppers. The simulation platform have been actualized using an Intel(R) machine with Core(TM) i5-24004, 4 GB of RAM and 160 GB HDD. All simulation experiments were performed using the R2017a MATLAB software. Finally, all simulation tests have been performed multiple times. The reported elapsed time represents the average of all trials for a given test.

In order to apply the proposed maps, controlling parameters values should be determined as their various combinations yield disorderly results. Our simulation experiments were conducted using $r = 17.0$ and r=2.35 for Eq. (1), and Eq. (2), respectively. The r values for both maps were chosen in the regions where chaos behaviour is noticed in the bifurcation and Lyapunov exponent diagrams in Figure 2. As the figure suggested, other values can be used and can provided a similar or close behaviour. Multiple experiments have been performed to select the best a and b values of Eq. (2). Namely, simulation experiments with various combinations of a and $b \in [0.1 : 0.1 : 1]$ were conducted and maps' trajectory are examined. The best a and b combinations where the map has good chaotic performance are then selected (i.e., $a = 0.5$, $b = 0.3$). The initial maps' values can be any arbitrate values and we select x_0 and y_0 to be equal to 0.1. The number of iterations was set to $n = 1000$ to obtain a chaotic sequence with good random performance.

A. STATISTICAL AND QUALITATIVE ANALYSES

A step-by-step demonstration of the encryption/decryption processes using a chest CT scan is shown in Fig. 4. The figure demonstrates various processing steps for the application of the proposed scheme in both encryption stage to obtain the encrypted data (Fig. 4 (e)). Decryption steps are carried out for splitting the diffused encrypted image; inverting diffusion process for each half using the same keys; inverting the permutation using the similar keys used in encryption process; combing the two halves of the decrypted image to attain the original image (Fig. 4) (f). This can only be achieved by using the right secret keys. More encryption and decryption simulation results to test the encryption algorithm are shown in Fig. 5(a, e, i, m) using various test medical scans (brain MRI image, abdomen CT, knee MRI, spine X-ray). As readily seen, the cipher images shown in Figs 4(e) and Fig. 5 appear as noise, thus revealing the effectiveness of the proposed scheme in hiding the information. Therefore, attackers or unauthorized users can not obtain/retrieve cipher images contents without the correct keys.

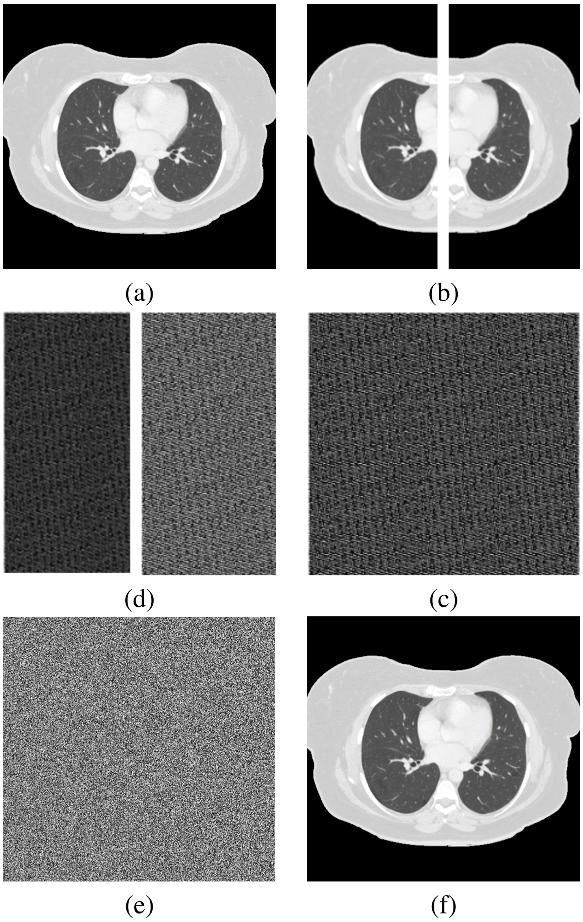

FIGURE 4. The simulation steps for encryption (a→e) and decryption (a←e) process: (a) original CT lung image; (b) split images; (c) permutation for each half of split images; (d) combination and permutation for the two halves; and final diffusion encrypted (e) and decrypted (f) image.

In image encryption, qualitative evaluation of a given scheme can be conducted using the well-known method of histogram analysis. The distributions of greyscale values of a given image (or its cipher counterpart) compromises its histogram. Particularly, the closer the greyscale distri-

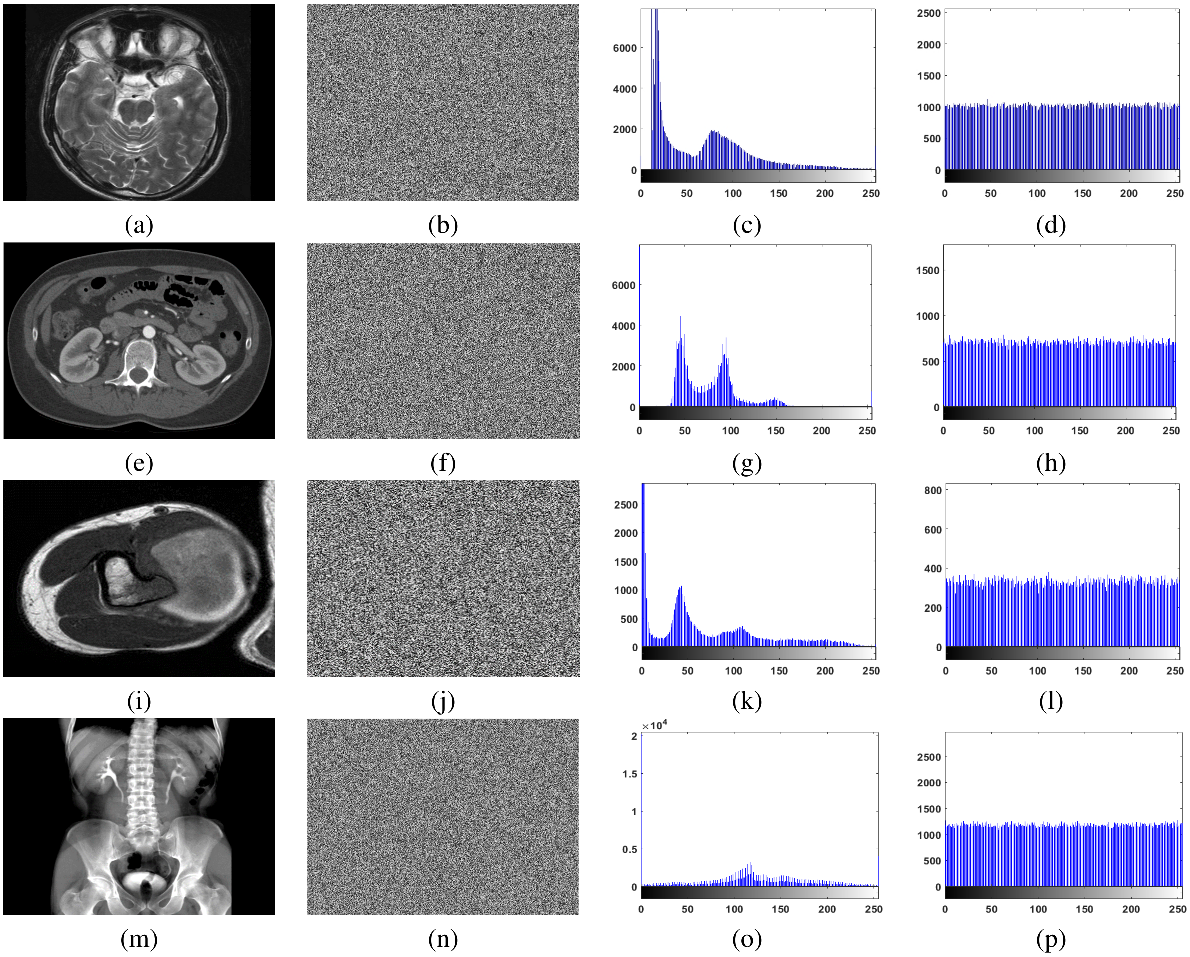

FIGURE 5. Qualitative results of the proposed model using various medical images– *rows top to bottom*– brain MRI image; abdomen CT scan of the kidney; MRI of the knee; and X-ray of the spine – *columns from left to right*–original images, cipher counterparts, original images histograms, and cipher images histograms.

TABLE 1. Evaluation metrics of the proposed approach tested on several medical images.

	Test Medical Images			
	Brain	Kideny	Knee	Spine
Metric	MRI	Abdomen CT	MRI	X-Ray
R	-0.004	0.003	0.004	-0.001
Entropy	7.999	7.998	7.998	7.999
MSE	12.809	12.483	16.672	14.355
PSNR	7.055	7.167	5.910	6.560
UACI (%)	33.66	33.63	33.64	33.78
NPCR (%)	99.68	99.69	99.71	99.70

R: correlation coefficient; MSE: mean square error ($\times 10^3$); PSNR: peak signal-to-noise ratio; UACI: unified average changing intensity; NPCR: number of pixels change rate

butions of cipher images is, the better the encryption algorithm, i.e., the higher their encryption level. That means, the distribution of cipher images logically needed to be uniform [43]. Figure 5 shows the histogram analysis for the selected sample medical images and their encrypted counterparts. As shown in Fig. 5 (c, g, k, o), original images histograms are clustered around certain grey values, while those of the cipher images are distributed uniformly over the greyscale span (Fig. 5 (d, h, l, p)). This documents the ability of the encrypted data to counter statistical attacks.

Additional measurable quantitative metrics, such as those obtained via statistical analysis are widely utilized for encryption techniques evaluation. Namely, several types of statistics including correlation and information entropy-based metrics are widely adopted [44]. The correlation coefficient (R) between the original and cipher images is a statistical metric describing the randomness of encrypted images (ideal value is "1") and is defined by [44] as:

$$R = \frac{\sum_H \sum_W (I_o - \overline{I_o})(I_d - \overline{I_d})}{\sqrt{(\sum_H \sum_W (I_o - \overline{I_o})^2)(\sum_H \sum_W (I_d - \overline{I_d})^2)}} \quad (3)$$

where H and W are the input image dimensions (i.e., the number of columns and rows, respectively); and $\overline{I_o}$ ($\overline{I_d}$) is the mean intensity values of original (decrypted) image. The R values of our experiments using the test medical images are given in the first row of Table 1. Another perfect metric to evaluate the encryption randomness, beside pixel distributions and R, is information entropy (E), which can be

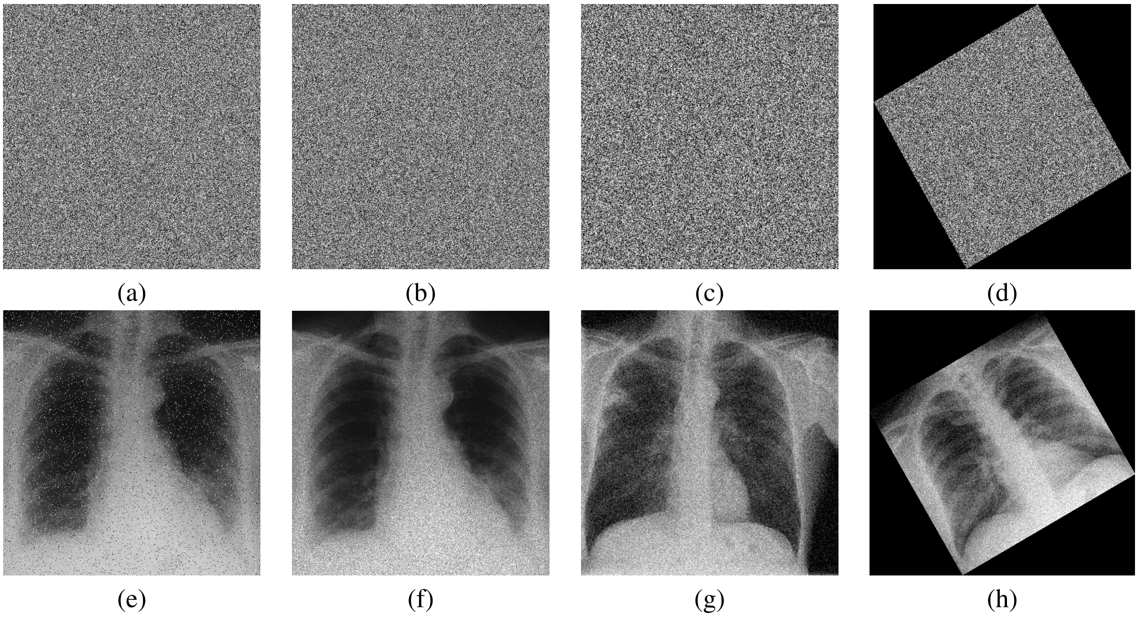

FIGURE 6. Simulation results for noise attack effects using a chest X-ray image. The first row shows encrypted images with (a) 5% salt & pepper noise; (b) 4% speckle noise; (c) 10% Gaussian noise; (d) 2% Gaussian commotion and 30^{o} rotation and the second row shows the respective decrypted images.

computed by [23] as:

$$E(m) = -\sum_{i=0}^{2N_b-1} p(m_i)\log_2(p(m_i)) \tag{4}$$

here $p(m)$ is the probability of symbol m_i, and N_b represents the number of bits for each symbol. The E values of the encrypted test medical images using our scheme are listed in the second row of Table 1. Note that our scheme gives a Shannon entropy of 7.99 or higher, which means it rarely leaks any useful information.

In addition to statistical metrics, encryption algorithm evaluation against differential attacks is important. Cipher sensitivity to tiny changes in plain-image should be high. Namely, to reduce the efficiency of such attacks and make them useless, small disturbances in the input image should results in a significant change in the cipher one [45]. In practice, several metrics can used to qualitatively asses the robustness against differential attacks. The peak signal to noise ratio (PSNR) is one of those metrics that is used to measure the degradation between the original and decrypted images [46]. Another useful metric is the unified average changing intensity (UACI), which numerically quantify the average intensity difference between a given plain images and its cipher [47]. In addition to PSNR and UACI, mean square error (MSE) is also a commonly used evaluation metric. Practically, UACI should be about 0.33 [47] and complying with robust security needs necessitate lower PSNR and higher MSE values. The MSE, PSNR, and UACI results using the proposed technique are summarized in Table 1.

Moreover, sensitivity analysis attacks occurring during cipher image transmission is a common encryption practise. There are four classical types of attacks: ciphertext, known plaintext, chosen plaintext and chosen ciphertext. Among those types, chosen plain text attack is considered the most powerful attack and if a given cryptosystem can withstand such attack, it can resist other types of attack. As an intuitive practice, the encryption robustness is usually evaluated by applying noise attacks (e.g., salt & pepper, Gaussian, and speckle noise), and rotation attacks. The simulation results against different types of noise attacks (salt and pepper noise, speckle noise, Gaussian noise, and Gaussian commotion and rotation noise) for the proposed method using an X-ray image of chest is illustrated in Fig. 6.

To further assess the accuracy and robustness of the our encryption framework, we have tested it on benchmark images and compared its performance against other SOTA encryption schemes. We used both greyscale and color "Lena", "Baboon", "Cameraman", and "Peppers" images. Simulation results of the proposed approach are statistically analyzed using different measures (e.g., Entropy, MSE, and PSNR) in comparison with other schemes. The quantitative comparative results using the benchmark greyscale images are summarized in Tables 2 and 3. As the results show, our scheme security performance is on a comparable bar with other SOTA methodologies. Also, higher Shannon entropy documents that our scheme rarely leak useful information.

Generally, secure encryption schemes must possess a strong ability of differential attacks resistance. The proposed encryption uses different averages when encrypting different input images. This successively can considerably increase its resistance against unknown, chosen, or differential attacks. We tested our scheme robustness using both greyscale and color images and have compared its robustness

TABLE 2. Entropies of various ciphered images comparing our technique with other state-of-the-art techniques.

	Test Images			
Scheme	Lena	Cameraman	Baboon	Peppers
Liu et al. [31]	7.235	–	–	7.204
Khan et al. [35]	7.997	–	7.997	7.999
Wang et al. [36]	7.999	–	7.993	7.999
Younas et al. [37]	7.997	–	7.997	7.997
Our Method	7.999	7.999	7.999	7.999

TABLE 3. Comparative quantitative results for our scheme and literature techniques using various benchmark greyscale images.

	Proposed		[35]		[37]	
Image	MSE	PSNR	MSE	PSNR	MSE	PSNR
Lena	11.523	7.994	10.870	7.768	4.859	11.30
Cameraman	9.128	8.114	–	–	–	–
Baboon	11.512	7.563	10.930	7.745	6.399	10.10
Peppers	11.823	7.541	10.898	7.758	7.274	9.55

MSE: mean square error ($\times 10^3$); PSNR: peak signal-to-noise ratio.

against differential attacks with literature work. The numerical evaluation values using well-known differential metric, i.e., UACI and NPCR are summarized in Tables 4 – 7. The reported results show that the NPCR metric is above 99% and the UACI values are all above 33%. Those results simply imply that quantitative metrics of the proposed approach are closer to the ideal values, thus documenting that our encryption pipeline is highly sensitive to resisting differential attacks. Additionally, Table 5 summarizes the critical NPCR and UACI values. On one hand, the $N^*_{0.05}$, $N^*_{0.01}$, and $N^*_{0.001}$ are critical values for rejecting the null hypothesis at significance levels of $\alpha = 0.05, 0.01$, and 0.001, respectively. This indicates that if the NPCR value for the two encrypted images is less than N^*_α, the two encrypted images are not sufficiently random with a significance α level. The proposed cipher's NPCR values at all degrees of confidence meet the theoretical (critical) condition of the NPCR randomness test are passed. On the other hand, the UACI critical value U^*_α is made up of two parts: U^{*-}_α, which is the left value, and U^{*+}_α, which is the right value. The null hypothesis is rejected if any value for the proposed cipher's UACI is beyond $(U^{*-}_\alpha, U^{*+}_\alpha)$ range. The UACI values for all sizes of the proposed encryption satisfy the UACI randomness test's crucial values.

TABLE 4. Quantitative average NPCR and UACI of ciphered benchmark grayscale images for our technique compared with other literature approaches.

	Evaluation Metric	
Method	NPCR (%)	UACI (%)
Alghafis et al. [18]	99.86	33.34
Wang et al. [48]	99.60	33.47
Xian et al. [49]	99.61	33.46
Proposed Method	99.86	33.72

NPCR: number of pixels change rate; UACI: unified average changing intensity.

B. KEY SPACE ANALYSIS

In cryptography, the set of all various keys that can be used in a given encryption scheme compromises it key space. The proposed pipeline consists of two execution steps; or the permutation and diffusion. In the permutation process, we use the two proposed maps presented with the independent factors (i.e., x_0, y_0, a, b and r) for each half of the divided image and therefore the composite vector. On the other hand, the proposed maps in the diffusion process contain separate variables x_0, y_0 and r within the key specified with the regular content algorithm, we've a uniform integer $c \in [1,255]$. Thus, the key space is $\{x_0, y_0, a, b, r\}$, each of which is a double precision number with a more than 1014 various attributes. Therefore, a huge key area ($\geq 1014 \times 1014 \times 1014 \times 1014 \times 255$) is achievable and is enough to resist any brute-force attacks.

TABLE 5. NPCR and UACI randomness test critical values (percentage) for test medical images.

	Test Image			
	Brain MRI	Kidney CT	Knee MRI	Spine X-Ray
$N^*_{0.05}$	99.6515	99.6726	99.6992	99.6957
$N^*_{0.01}$	99.6432	99.6684	99.6964	99.6944
$N^*_{0.001}$	99.6339	99.6638	99.6933	99.6928
$U^{*-}_{0.05}$	33.5049	33.4749	33.4849	33.6249
$U^{*+}_{0.05}$	33.6861	33.6561	33.6661	33.8061
$U^{*-}_{0.01}$	33.7145	33.4465	33.4565	33.5965
$U^{*+}_{0.01}$	33.7476	33.6845	33.6945	33.8345
$U^{*-}_{0.001}$	33.4434	33.4134	33.4234	33.5634
$U^{*+}_{0.001}$	33.4765	33.7176	33.7276	33.8676

C. KEY SENSITIVITY ANALYSIS

Key sensitivity is another important analysis procedure that evaluates the characteristics of chaotic coding. Ideally, cipher images should be very sensitive to slight changes in their secret keys. Namely, flipping a single bit or one parameter in the employed key leads to different results during decoding, i.e., cipher data will never be correctly decrypted. Not only that but the keys order is extremely important, otherwise the cipher data decryption will fail as the decryption does not occur in the correct order. Sensitivity analysis of our scheme regarding a slight change in employed secret key have been tested. An example for plain ultrasound (US) image of the liver is shown in Fig. 7, where Fig. 7 (a) shows the plain image and Fig. 7 (b, c) show the encrypted images obtained by our approach when different encrypted keys are employed. Each secret key changed only 10^{-4}, i.e., x_0 was changed to $0.1 + 10^{-4}$, and $r = 2.35 + 10^{-4}$. Although the results in Fig. 7 (b, c) are visually similar, their actual difference is highlighted in Fig. 7 (d). These results show the security key has good sensitivity.

In the decryption process, slight key change yield widely different results. A demonstrative example is in Figure 8. In this figure, decrypted MRI-knee image using exact same keys used during encryption stage is shown in Fig. 8 (a). The same cipher image is decrypted by making two different tiny modifications in the original keys and the results are referred to in Fig. 8 (b, c). The decrypted image in Fig. 8 (b) utilized $x_0 = 0.1 + 10^{-4}$, and that in Fig. 8 (c) is obtained by

TABLE 6. Quantitative UACI comparison between our scheme and other literature schemes using encrypted benchmark color images.

	Test Image								
	Lena			Baboon			Peppers		
	Channels			Channels			Channels		
Method	R	G	B	R	G	B	R	G	B
Alghafis et al. [18]	32.98	34.06	32.91	36.58	33.77	35.01	35.36	35.64	36.06
Cheng et al. [32]	33.4885	33.4930	33.5089	33.4568	33.4761	33.6113	–	–	–
Wang et al. [33]	33.420	33.45	33.41	33.46	33.42	33.46	33.37	33.42	33.40
Huang et al. [34]	33.4655	33.4652	33.4591	33.4575	33.4625	33.4607	–	–	–
Khan et al. [35]	33.27	33.36	33.50	33.47	33.48	33.45	33.39	33.36	33.40
Wang et al. [36]	33.4290	33.4306	33.3665	32.6845	31.9555	33.4146	33.5577	32.713	33.5702
Proposed Method	33.7502	33.6613	33.7810	33.6424	33.5321	33.6753	33.7991	33.6512	33.7523

UACI: unified average changing intensity; R: red; B: blue; G: green

TABLE 7. Quantitative NPCR comparison between our scheme and other literature schemes using encrypted benchmark color images.

	Test Image								
	Lena			Baboon			Peppers		
	Channels			Channels			Channels		
Method	R	G	B	R	G	B	R	G	B
Alghafis et al. [18]	99.84	99.81	99.79	99.87	99.77	99.74	99.78	99.87	99.76
Cheng et al. [32]	99.6404	99.6334	99.6470	99.6325	99.6367	99.6438	–	–	–
Wang et al. [33]	99.570	99.610	99.600	99.750	99.470	99.640	99.510	99.700	99.720
Huang et al. [34]	99.6103	99.6098	99.6089	99.6094	99.6100	99.6081	–	–	–
Khan et al. [35]	99.58	99.56	99.64	99.62	99.60	99.60	99.60	99.60	99.61
Wang et al. [36]	99.6037	99.5983	99.6159	99.6246	99.5914	99.5972	99.6315	99.6071	99.6380
Proposed Method	99.8321	99.7452	99.8551	99.8902	99.7914	99.8792	99.8725	99.7841	99.8814

NPCR: number of pixels change rate; R: red; B: blue; G: green

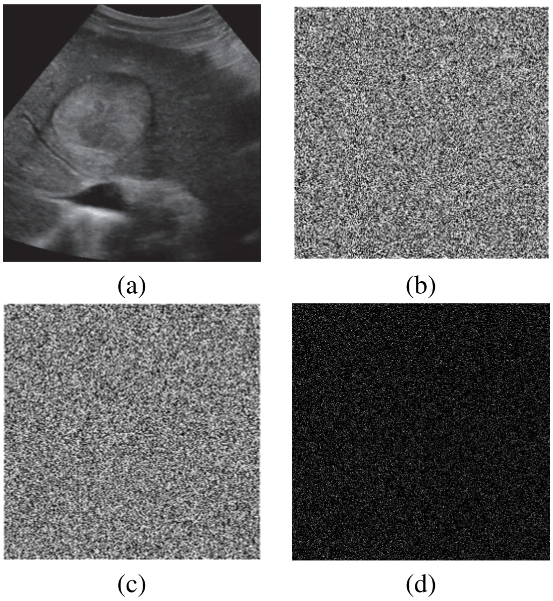

FIGURE 7. Key sensitivity of encryption phase (a) ultrasound plain image; (b) encrypted image with first key; (c) encrypted image with another key; and (d) difference between (b) and (c).

using the key $r = 2.35 + 10^{-4}$. Obviously, the decrypted images are all unrecognized when wrong/illegal key are used. The above examples document that slightly small changes in encryption keys of our scheme (or their orders at any position) produce noise-like output and thus protect original images from recovery by an authorized users. This highlights the effectiveness our algorithm and its high sensitive.

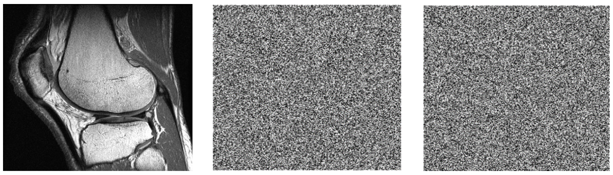

FIGURE 8. Decrypted process for an MR-knee image with key sensitivity using correct encryption keys (left); and wrong keys (middle and right).

Our technique is sensitive both of the initial parameters and their respective initial values. If one of them changes, the ciphered values would be totally different. Furthermore, the encrypted value of the combined diffusion phase not only relates to the employed key and plain value, but also relates to both former plain and ciphered values. Thus, different encrypted image has different former plain and ciphered values. So, the proposed approach can counter the chosen plaintext/ciphertext attacks.

D. TIME COMPLEXITY ANALYSIS

Execution-time is also a significant factor with regard to the degree of security. The speed level depends on many factors, including the number of iterations, the type of calculations performed, and the efficiency of the machine used. It is therefore difficult to compare the speed performance based on published results, since they use different systems and employ different technical programming approaches. However, the speed output of the reference papers is shown in Table 8. This is intended as a general description of the speed efficiency of the proposed method relative to the reference method. The length of our scheme is evaluated and compared to those algorithms using both color and grayscale images of different sizes. According to the results in Table 8, (i) the time of encryption increases with an increase in the size of the test image; and (ii) the proposed encryption algorithm is faster than the methods in [34], [38], [50], [51] and is more suitable for actual applications.

TABLE 8. Comparative average execution time (in seconds) for benchmark greyscale and color images (Lena, Baboon, and Peppers) with different sizes.

	Image size			
	256×256		512×512	
Scheme	Grey	Color	Grey	Color
Huang et al. [34]	0.3039	1.1552	0.9047	3.5145
Xiong et al. [38]	–	–	–	21.0135
Chai et al. [50]	–	–	0.44	2.77
Cai et al. [51]	0.4389	1.8112	1.1347	4.6058
Proposed Method	0.2788	0.5341	0.1721	1.9912

E. CORRELATION OF ADJACENT PIXELS

Usually visual inspection to compare decrypted images is not easy. Quantitative metrics can however be used to compare/evaluate decrypted images. Among those metrics is the correlation coefficient, or R, as discussed above. Usually evaluation is conducted by estimating R between encrypted images and various decrypted images. More effective approach for evaluation is to estimate R between adjacent pixels. Namely, R between a set of randomly chosen pair of pixels in all direction (i.e., two horizontally–, two vertically–, and two diagonally–adjacent pixels) in the plain and the corresponding encoded images [42].

In our experiments, the following procedure is performed to test the correlation between adjacent pixels in original and ciphers. First, in each direction (i.e., horizontal, vertical and diagonal) a set of 5, 000 pairs of adjacent pixels are randomly selected from a given image. Then, R values for each set of paired pixels is estimated using Eq. (3). The calculated results are shown in Table 9 for the test color images. For the coded image in all three directions and color channels (i.e., red (R), green (G) and blue (B)), it is clear that the correlation coefficients are smaller than their counterparts for the plain image. Also, the correlation coefficients for cipher images are negligible (i.e., ≈0, hardly any correlations) and those of the plain images show strong connection to adjacent pixels (i.e., ≈1 or ideal). Furthermore, the correlation distributions in the three direction for the MRI brain image in Fig. 3 are shown in Fig. 9. Based on those results, we can conclude that our scheme (i) has good confusion and diffusion properties; and (ii) can combat attacks based on the statistical characteristics of the images.

TABLE 9. Correlation coefficient of adjacent pixels in all directions of original and encrypted color images using the proposed maps.

Test Image		Channel	Horizontal	Diagonal	Vertical
Lena	Original	R	0.96422	0.96025	0.96182
		G	0.98215	0.96541	0.97486
		B	0.96215	0.92458	0.96215
	Encrypted	R	0.00061	0.00300	-0.04001
		G	-0.00091	-0.00810	0.00051
		B	0.00051	-0.00749	0.00612
Baboon	Original	R	0.91002	0.92541	0.90912
		G	0.96221	0.92155	0.96215
		B	0.97125	0.93125	0.96201
	Encrypted	R	0.00413	-0.00895	0.00301
		G	0.00125	0.00213	-0.00601
		B	0.00512	0.01245	-0.01325
Peppers	Original	R	0.96821	0.91255	0.96021
		G	0.97212	0.9526	0.97125
		B	0.95321	0.94154	0.94413
	Encrypted	R	0.00312	0.02812	0.02146
		G	-0.00215	-0.00595	0.00412
		B	0.00529	0.02766	-0.02534

R: red; B: blue; G: green

TABLE 10. The national institute of standards and technology (NIST) (SP800) test analysis results.

Test name	P value	Result
Frequency	0.53254872	√
Block frequency	0.595421347	√
Runs (M = 10,000)	0.584200186	√
Long runs of ones	0.554826912	√
Rank	0.562145874	√
Spectral DFT	0.665214	√
No overlapping templates	0.740125	√
Universal (L = 7, Q = 1280, K = 141,577)	0.462154125	√
Lempel–Ziv complexity	0.7812004	√
Linear complexity	0.595412037	√
Serial P-value1	0.712458719	√
Serial P-value2	0.642100587	√
Approximate entropy	0.762351470	√
Cumulative sums forward	0.565214785	√
Cumulative sums reverse	0.620124584	√

"√" indicates success

TABLE 11. Result of DIEHARD tests suite.

Test name	Average value	Result
Birthday spacing	0.741248	√
Overlapping permutation	0.701214	√
Binary rank 31 × 31	1.041254	√
Binary rank 32 × 32	0.645217	√
Binary rank 6 × 8	0.881254	√
Bitstream	0.624154	√
OPSO	0.67124	√
OQSO	0.74580	√
DNA	0.77014	√
Count the ones 01	0.671245	√
Count the ones 02	0.485421	√
Parking lot	0.852012	√
Minimum distance	0.681245	√
3DS spheres	0.540129	√
Squeeze	0.752145	√
Overlapping sum	0.674542	√
Runs	0.641201	√
Craps	0.585454	√

"√" indicates success

F. RANDOMNESS TESTS FOR THE CIPHERED IMAGE

To ensure the security of the encryption system, the image should contain properties for further measurable investigation to separate designs, for example, a large spread (i.e., arrangement's connection gets feeble), a wide span (a long key period), and a nature and productivity (i.e., disarray and dissemination) [52]. Some tests are generally used to randomly test the component image. These tests

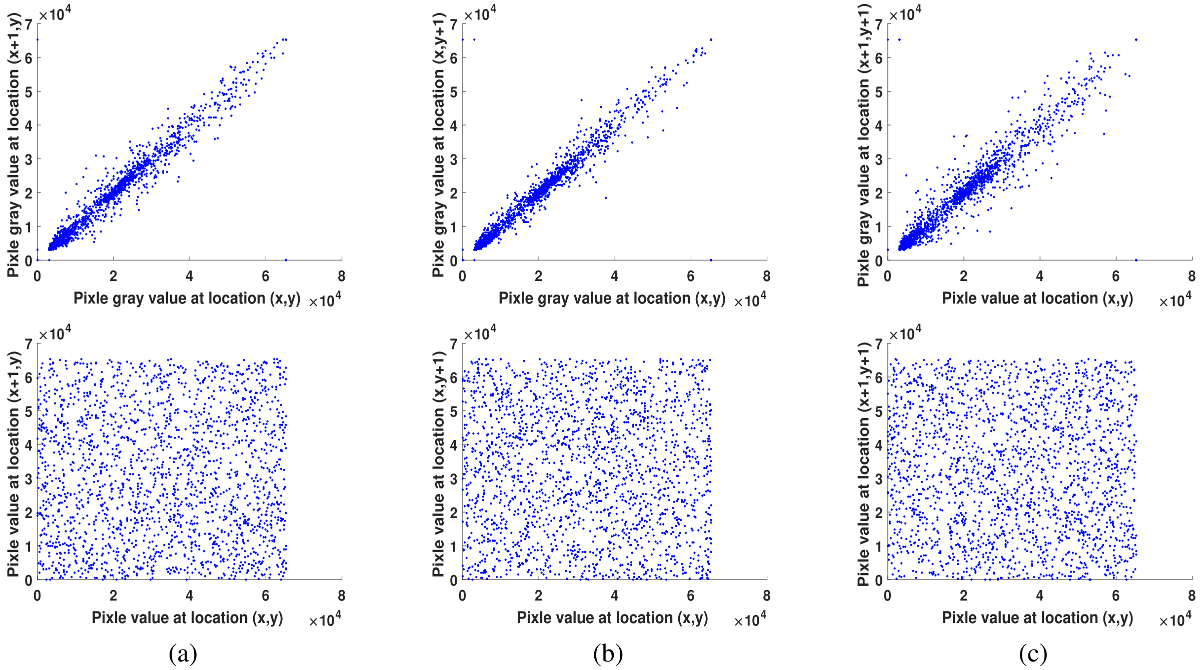

FIGURE 9. Correlation distributions for adjacent-pixels for the "brain MRI" greyscale image (first row) and its cipher image (second row) in the horizontal (a), vertical (b), and diagonal (c) directions.

include measurable DIEHARD and NIST (SP800) test kits. The DIEHARD test is important because, by all accounts, it represents the most striking and disturbing set of tests to pass [53]. The P estimation of each test must be inside the achievement scope of 0.01 < P esteem < 0.99. NIST is a measurable bundle comprising of a lot of tests. These tests were created to randomly test the coded image that is based on semi-random generators. Tables 10 and 11 show the consequences of the NIST and DIEHARD. The results show that the encrypted images have passed all revisions, which means that they show highly random behavior.

VI. CONCLUSION

This paper has introduced a novel and robust medical image encryption scheme that can integrated in cloud-based internet-of-heath systems (IoHS). The proposed pipeline introduced two novel chaotic maps, which demonstrated strong and effective chaotic behaviours, unpredictability, and extreme sensitive to initial seeds. Dynamic analysis and validation using bifurcation diagram and Lyapunov exponent showed that the proposed maps are hyperchaotic overall with high complexity and high sensitivity. Moreover, the proposed pipeline scheme (1) consists of a two-run confusion-diffusion architecture, and (2) incorporates other input parameters besides the plain image and the secret key unlike those encryption algorithms based on one-time keys. The latter has the advantage that it permits controlling the encrypted data values without affecting the secret keys. Thus, our system breaks the limitation of those based on one-time keys and possess multiple advantage, including improved encryption quality, performance, and robustness; and also secure and speed encryption of many images using the same key. This has been documented using various experiments and various test medical images. Additional companion with state-of-the-art encryption scheme using benchmark images (both color and greyscale) highlighted the high effectiveness and robustness of the proposed scheme to prevent many existing cryptography attacks and cryptanalysis techniques. Quantitative results showed that the average value NPCR and UACI are 99.814% and 33.694%, respectively. It is worth mentioning that the proposed pipeline is general and can be applied for any multimedia encryption application, including non-medical ones.

REFERENCES

[1] M. Elhoseny, K. Shankar, S. Lakshmanaprabu, A. Maseleno, and N. Arunkumar, "Hybrid optimization with cryptography encryption for medical image security in Internet of Things," *Neural Comput. Appl.*, vol. 32, pp. 10979–10993, 2018.

[2] S. Madhu and M. A. Hussain, "Securing medical images by image encryption using key image," *Int. J. Comput. Appl.*, vol. 104, no. 3, pp. 30–34, Oct. 2014.

[3] J. Li and H. Liu, "Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map," *IET Inf. Secur.*, vol. 7, no. 4, pp. 265–270, Dec. 2013.

[4] Q. Zhang and Q. Ding, "Digital image encryption based on advanced encryption standard (AES)," in *Proc. 5th Int. Conf. Instrum. Meas., Comput., Commun. Control (IMCCC)*, Sep. 2015, pp. 1218–1221.

[5] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Springer-Verlag, 2002, p. 238, doi: 10.1007/978-3-662-04722-4.

[6] N. B. Slimane, K. Bouallegue, and M. Machhout, "Nested chaotic image encryption scheme using two-diffusion process and the secure hash algorithm SHA-1," in *Proc. 4th Int. Conf. Control Eng. Inf. Technol. (CEIT)*, Dec. 2016, pp. 1–5.

[7] X. Wu, K. Wang, X. Wang, H. Kan, and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Process.*, vol. 148, pp. 272–287, Jul. 2018.

[8] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.

[9] A. Akhavan, A. Samsudin, and A. Akhshani, "Cryptanalysis of an image encryption algorithm based on DNA encoding," *Opt. Laser Technol.*, vol. 95, pp. 94–99, Oct. 2017.

[10] Y. Dou, X. Liu, H. Fan, and M. Li, "Cryptanalysis of a DNA and chaos based image encryption algorithm," *Optik*, vol. 145, pp. 456–464, Sep. 2017.

[11] S. K. Pujari, G. Bhattacharjee, and S. Bhoi, "A hybridized model for image encryption through genetic algorithm and DNA sequence," *Proc. Comput. Sci.*, vol. 125, pp. 165–171, Dec. 2018.

[12] H. M. Waseem, S. S. Jamal, I. Hussain, and M. Khan, "A novel hybrid secure confidentiality mechanism for medical environment based on Kramer's spin principle," *Int. J. Theor. Phys.*, vol. 60, no. 1, pp. 314–330, 2021.

[13] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Process.*, vol. 11, no. 5, pp. 324–332, 2017.

[14] S. Tariq, M. Khan, A. Alghafis, and M. Amin, "A novel hybrid encryption scheme based on chaotic Lorenz system and logarithmic key generation," *Multimedia Tools Appl.*, vol. 79, no. 31, pp. 23507–23529, 2020.

[15] U. A. Waqas, M. Khan, and S. I. Batool, "A new watermarking scheme based on Daubechies wavelet and chaotic map for quick response code images," *Multimedia Tools Appl.*, vol. 79, nos. 9–10, pp. 6891–6914, Mar. 2020.

[16] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A chaotic-based encryption/decryption framework for secure multimedia communications," *Entropy*, vol. 22, no. 11, p. 1253, Nov. 2020.

[17] A. Alghafis, N. Munir, and M. Khan, "An encryption scheme based on chaotic Rabinovich–Fabrikant system and s8 confusion component," *Multimedia Tools Appl.*, vol. 80, no. 5, pp. 7967–7985, Feb. 2021.

[18] A. Alghafis, H. M. Waseem, M. Khan, S. S. Jamal, M. Amin, and S. I. Batool, "A novel digital contents privacy scheme based on quantum harmonic oscillator and Schrodinger paradox," *Wireless Netw.*, pp. 1–20, May 2020, doi: 10.1007/S11276-020-02363-7.

[19] S. Tariq, A. Elmoasry, S. I. Batool, and M. Khan, "Quantum harmonic oscillator and Schrodinger paradox based nonlinear confusion component," *Int. J. Theor. Phys.*, vol. 59, no. 11, pp. 3558–3573, Nov. 2020.

[20] B. Yousif, F. Khalifa, A. Makram, and A. Takieldeen, "A novel image encryption/decryption scheme based on integrating multiple chaotic maps," *AIP Adv.*, vol. 10, no. 7, Jul. 2020, Art. no. 075220.

[21] M. Boussif, N. Aloui, and A. Cherif, "Smartphone application for medical images secured exchange based on encryption using the matrix product and the exclusive addition," *IET Image Process.*, vol. 11, no. 11, pp. 1020–1026, Nov. 2017.

[22] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.

[23] I. Yasser, F. Khalifa, M. A. Mohamed, and A. S. Samrah, "A new image encryption scheme based on hybrid chaotic maps," *Complexity*, vol. 2020, pp. 1–23, Jul. 2020.

[24] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new Beta chaotic maps," *Opt. Lasers Eng.*, vol. 96, pp. 39–49, Sep. 2017.

[25] E. Yavuz, R. Yazici, M. C. Kasapbaşi, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Comput. Electr. Eng.*, vol. 54, pp. 471–483, Aug. 2016.

[26] X. Wang, S. Wang, N. Wei, and Y. Zhang, "A novel chaotic image encryption scheme based on hash function and cyclic shift," *IETE Tech. Rev.*, vol. 36, no. 1, pp. 39–48, 2018.

[27] R. Parvaz and M. Zarebnia, "A combination chaotic system and application in color image encryption," *Opt. Laser Technol.*, vol. 101, pp. 30–41, May 2018.

[28] J. Wu, X. Liao, and B. Yang, "Image encryption using 2D Hénon–Sine map and dna approach," *Signal Process.*, vol. 153, pp. 11–23, Dec. 2018.

[29] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 60, pp. 12–32, Jul. 2018.

[30] H. Luo and B. Ge, "Image encryption based on Henon chaotic system with nonlinear term," *Multimedia Tools Appl.*, vol. 78, no. 24, pp. 34323–34352, Dec. 2019.

[31] 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.

[32] G. Cheng, C. Wang, and H. Chen, "A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture," *Int. J. Bifurcation Chaos*, vol. 29, no. 9, Aug. 2019, Art. no. 1950115.

[33] X.-Y. Wang, P. Li, Y.-Q. Zhang, L.-Y. Liu, H. Zhang, and X. Wang, "A novel color image encryption scheme using DNA permutation based on the Lorenz system," *Multimedia Tools Appl.*, vol. 77, no. 5, pp. 6243–6265, 2018.

[34] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Opt. Lasers Eng.*, vol. 115, pp. 7–20, Apr. 2019.

[35] M. Khan and F. Masood, "A novel chaotic image encryption technique based on multiple discrete dynamical maps," *Multimedia Tools Appl.*, vol. 78, no. 18, pp. 26203–26222, Sep. 2019.

[36] X. Wang, X. Qin, and C. Liu, "Color image encryption algorithm based on customized globally coupled map lattices," *Multimedia Tools Appl.*, vol. 78, no. 5, pp. 6191–6209, Mar. 2019.

[37] I. Younas and M. Khan, "A new efficient digital image encryption based on inverse left almost semi group and Lorenz chaotic system," *Entropy*, vol. 20, no. 12, p. 913, 2018.

[38] Z. Xiong, Y. Wu, C. Ye, X. Zhang, and F. Xu, "Color image chaos encryption algorithm combining CRC and nine palace map," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 31035–31055, Nov. 2019.

[39] N. Munir, M. Khan, Z. Wei, A. Akgul, M. Amin, and I. Hussain, "Circuit implementation of 3D chaotic self-exciting single-disk homopolar dynamo and its application in digital image confidentiality," *Wireless Netw.*, pp. 1–18, May 2020, doi: 10.1007/s11276-020-02361-9.

[40] S. Su, Y. Su, and M. Xu, "Comparisons of firefly algorithm with chaotic maps," *Comput. Model New Technol.*, vol. 18, no. 12, pp. 326–332, 2014.

[41] E. A. Albahrani and T. K. Alshekly, "New chaotic substation and permutation method for image encryption," *Int. J. Appl. Inf. Syst.*, vol. 12, pp. 34–39, Jul. 2017.

[42] G. Hanchinamani and L. Kulakarni, "Image encryption based on 2-D Zaslavskii chaotic map and pseudo Hadmard transform," *Int. J. Hybrid Inf. Technol.*, vol. 7, no. 4, pp. 185–200, 2014.

[43] J. Thiyagarajan, B. Murugan, and A. Gounder, "A chaotic image encryption scheme with complex diffusion matrix for plain image sensitivity," *Serbian J. Electr. Eng.*, vol. 16, no. 2, pp. 247–265, 2019.

[44] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, 2010.

[45] K. Gupta and S. Silakari, "Efficient hybrid image cryptosystem using ECC and chaotic map," *Int. J. Comput. Appl.*, vol. 29, no. 3, pp. 1–13, 2011.

[46] S. Lian, J. Sun, and Z. Wang, "A block cipher based on a suitable use of the chaotic standard map," *Chaos Solitons Fract.*, vol. 26, no. 1, pp. 117–129, Oct. 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0960077905000378

[47] A. Akhshani, S. Behnia, A. Akhavan, S. Lim, and Z. Hassan, "An image encryption approach using quantum chaotic map," in *Proc. Int. Conf. Adv. Comput. Inf. Technol. (ACIT)*, Kuala Lumpur, Malaysia, May 2013, pp. 171–176.

[48] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Inf. Sci.*, vol. 539, pp. 195–214, Oct. 2020.

[49] Y. Xian and X. Wang, "Fractal sorting matrix and its application on chaotic image encryption," *Inf. Sci.*, vol. 547, pp. 1154–1169, Feb. 2021.

[50] X. Chai, X. Zheng, Z. Gan, and Y. Chen, "Exploiting plaintext-related mechanism for secure color image encryption," *Neural Comput. Appl.*, vol. 32, no. 12, pp. 8065–8088, Jun. 2020.

[51] S. Cai, L. Huang, X. Chen, and X. Xiong, "A symmetric plaintext-related color image encryption system based on bit permutation," *Entropy*, vol. 20, no. 4, p. 282, 2018.

[52] O. M. Al-Hazaimeh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys," *Neural Comput. Appl.*, vol. 31, no. 7, pp. 2395–2405, 2019.

[53] T. Sobh, K. Elleithy, A. Mahmood, and M. A. Karim, *Novel Algorithms and Techniques in Telecommunications, Automation and Industrial Electronics*. Dordrecht, The Netherlands: Springer, 2008, doi: 10.1007/978-1-4020-8737-0.

IBRAHIM YASSER received the B.Sc. degree in electronics and communications from Benha University, Egypt, and the M.Sc. and Ph.D. degrees from the Electronics and Communications Engineering Department, Mansoura University, Egypt, in 2016 and 2020, respectively. His research work has been materialized in books and ISI index articles in international specialty journals. His research interests include neutrosophic sets, security, multimedia, fog and cloud computing, chaotic maps, machine learning, big data, artificial intelligent, and flexible education. Future research interests include design security techniques for the cloud requiring little user awareness and computer-aided diagnosis medical images analysis. He is a member of chief editors for *Neutrosophic Knowledge* journal.

ABEER T. KHALIL received the B.Sc. and Ph.D. degrees from the Electronics and Communications Engineering Department, Faculty of Engineering, Mansoura University, in 2001 and 2013, respectively. She is currently working as an Assistant Professor with the Faculty of Engineering, Mansoura University. She has published more than 20 articles and supervised ten postgraduate students in many universities. Her research interests include wireless networking and digital hardware realization.

MOHAMED A. MOHAMED received the Ph.D. degree in electronics and communications engineering from the Faculty of Engineering, Mansoura University, Egypt, in 2006. He is currently the Dean of the Faculty of Engineering, Mansoura University. He has more than 120 publications in various international journals and conferences. His current research interests include multimedia processing, wireless communication systems, and field programmable gate array (FPGA) applications. He had been awarded the Best Ph.D. Thesis at Mansoura University, in 2007.

AHMED S. SAMRA received the B.Sc. and M.Sc. degrees in communications engineering from Menoufia University, in 1977 and 1982, respectively, and the Ph.D. degree in optical communications and integrated optics from ENSEG, Grenoble, France, in 1988. He is currently a Professor in electronics and communications engineering with the Faculty of Engineering, Mansoura University, where he was the Department Head, from 2011 to 2013. His research interests include optical communications and optical measurement technique.

FAHMI KHALIFA (Senior Member, IEEE) received the B.Sc. and M.Sc. degrees in electronics and electrical communication engineering from Mansoura University, Egypt, in 2003 and 2007, respectively, and the Ph.D. degree in electrical engineering from the Electrical and Computer Engineering Department, University of Louisville, USA, in 2014. He is currently an Assistant Professor with the Electronics and Communications Engineering Department, Mansoura University. He has more than 12 years of hands-on experience in the fields of image processing, machine learning, medical image analysis, computer-aided diagnosis, and digital and analog signal processing. He has authored/coauthored more than 150 peer-reviewed publications appearing in high-impact journals, selective peer-reviewed top-rank international conferences, and leading edited books.