Please cite the Published Version

A New Chaotic Map With Dynamic Analysis and Encryption Application in Internet of Health Things

NESTOR TSAFACK[1,2], **SYAM SANKAR**[3], **BASSEM ABD-EL-ATTY**[4], **JACQUES KENGNE**[2],
JITHIN K. C.[3], **AKRAM BELAZI**[5], **IRFAN MEHMOOD**[6],
ALI KASHIF BASHIR[7], (Senior Member, IEEE), **OH-YOUNG SONG**[8],
AND AHMED A. ABD EL-LATIF[4,9,10]

[1]Research Unit of Laboratory of Automation and Applied Computer (LAIA), Electrical Engineering Department of IUT-FV, University of Dschang, Bandjoun, Cameroon
[2]Research Unit of Laboratory of Condensed Matter, Electronics and Signal Processing (URMACETS) Department of Physics, Faculty of Sciences, University of Dschang, Dschang, Cameroon
[3]Department of Computer Science and Engineering, NSS College of Engineering, Palakkad 678008, India
[4]Center of Excellence in Cybersecurity, Quantum Information Processing, and Artificial Intelligence, Menoufia University, Shibin Al Kawm 32511, Egypt
[5]Laboratory RISC-ENIT (LR-16-ES07), Tunis El Manar University, Tunis 1002, Tunisia
[6]Faculty of Engineering and Informatics, School of Media, Design and Technology, University of Bradford, Bradford BD7 1DP, U.K.
[7]Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M15 6BH, U.K.
[8]Software Department, Sejong University, Seoul 05006, South Korea
[9]Department of Mathematics and Computer Science, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt
[10]School of Information Technology and Computer Science, Nile University, Giza 12677, Egypt

Corresponding authors: Ahmed A. Abd El-Latif (a.rahiem@gmail.com) and Oh-Young Song (oysong@sejong.edu)

ABSTRACT In this paper, we report an effective cryptosystem aimed at securing the transmission of medical images in an Internet of Healthcare Things (IoHT) environment. This contribution investigates the dynamics of a 2-D trigonometric map designed using some well-known maps: Logistic-sine-cosine maps. Stability analysis reveals that the map has an infinite number of solutions. Lyapunov exponent, bifurcation diagram, and phase portrait are used to demonstrate the complex dynamic of the map. The sequences of the map are utilized to construct a robust cryptosystem. First, three sets of key streams are generated from the newly designed trigonometric map and are used jointly with the image components (R, G, B) for hamming distance calculation. The output distance-vector, corresponding to each component, is then Bit-XORed with each of the key streams. The output is saved for further processing. The decomposed components are again Bit-XORed with key streams to produce an output, which is then fed into the conditional shift algorithm. The Mandelbrot Set is used as the input to the conditional shift algorithm so that the algorithm efficiently applies confusion operation (complete shuffling of pixels). The resultant shuffled vectors are then Bit-XORed (Diffusion) with the saved outputs from the early stage, and eventually, the image vectors are combined to produce the encrypted image. Performance analyses of the proposed cryptosystem indicate high security and can be effectively incorporated in an IoHT framework for secure medical image transmission.

INDEX TERMS Internet of health things, encryption, chaotic systems, dynamics analysis, lightweight security.

I. INTRODUCTION

As the data represented by medical images are of a vital source of information concerning the privacy of patients,

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

effective security mechanisms are to be developed. In the era of Internet of Healthcare Things (IoHT), the healthcare organizations should pay more attention for deploying secure cryptosystem to avoid security breaches. The patient's data have to be stored and transmitted in a secure way. We intend to build a chaos-based cryptosystem by exploiting the dynamic

properties of chaotic maps. A dynamic system can be seen as a mathematical concept with a fixed law [1] describing the time dependence of a point in the space. A chaotic dynamical system is a category of a dynamical system with very particular properties, including unpredictability, periodicity, sensitivity to the initial value(s), and control parameter(s). Such features are operated in various fields of science and engineering, including cryptography. Lorenz first discovered chaos in meteorology [2]. From this seminal work, chaos theory and chaotic systems are the topics of many discussions in the scientific community [3], [4].

Designing chaotic systems, scientists discovered that there are two categories of dynamical systems depending on the dimension: 1-D and n-D ($n \geq 2$) dynamic systems. Some mighty benefits of 1-D chaotic include low computational complexity, low processing time, easy to conceive, simple structure [5], [6]. Cryptosystems have been widely designed using low dimensional chaotic maps like 1-D. Yet, such maps are vulnerable to various onslaught given that the range of chaos dynamics for 1-D maps is limited, initial values and key parameters produce a small keyspace, and finally, it is easy to predict their output [7].

The second category, i.e., a high dimensional system, performs better than a one-dimensional map. Though high dimensional maps are difficult to implement and have high computation costs, their sequences can be used in various domains, including the design of unbreakable encryption algorithms [7]. These maps have been widely studied in the last decade. Some examples are Hénon map [8], 2-D sine map [9], CNN system [10], Chen and Lee system [11], jerk system [12], Chua's system [13], and hyperjerk systems [14]. It should be mention that the stability of equilibrium points is an efficient tool to foretell the dynamic of a system. Chaotic maps may display a finite number of unstable equilibrium points. Some recent studies investigated chaos in dynamic systems with zero equilibrium points [15], with a unique steady equilibrium point [16], with a large amount of equilibrium [17]. Here, we introduce a 2-D map with an infinite number of fixed points, which is particularly new. Besides, the sequences of the said map are used to design a robust encryption scheme for colour images.

We can now realize that more and more research has been done to develop modern encryption algorithms. For instance, chaos-based ciphers are used to protect the transferred information from attacks [18]. In [19], Habutsu *et al.* designed a chaos-based cryptosystem using an inverse tent map. The plaintext is utilized, like the initial state of the inverse tent map. The system is iterated N times to achieve an encrypted image. Based on random bits and the vulnerability of the tent map, classical types of attacks are used to break the above mention algorithm [20]. Baptista *et al.* constructed a new encryption scheme using the logistic map [21]. Very recently, [22], [23] used chaotic systems and hash function to design an encryption scheme with the key streams depending on the input image. Some weaknesses of the algorithms mentioned above can be stated as follows:

1) A lot of the state-of-art results exclusively depend on the key streams.
2) Shannon entropy of the cryptosystem is not pointedly improved even in recent papers.
3) Noise attack is not discussed by many authors.
4) Many of the works use chaotic systems with limited chaotic range.
5) The encryption time is not usually addressed, given that many of the cryptosystems seem computationally complex.
6) Lack of an exclusive algorithm to be used in an IoHT framework.

To overcome these weaknesses and contribute to enriching the literature, we present here the methodology to achieve a new efficient colour image cryptosystem. We intend to build a cryptosystem which can effectively ensure security in IoHT environment. The algorithm is designed using four main components: Trigonometric map (Logistic-Sine-Cosine), Mandelbrot Set, Bit-XOR operation, and new Conditional shift operation. Some well-known metrics are used to validate the security and speed of our algorithm.

In our work, at first, the input image received from medical devices is divided into its components R, G, and B. Three sets of key streams are generated from the newly designed trigonometric map and are used jointly with the image components (R, G, B) for hamming distance calculation. The output distance-vector, corresponding to each component, is then Bit-XORed with each of the key streams. The output is saved for further processing. The decomposed components are again Bit-XORed with key streams to produce an output, which is then fed into the conditional shift algorithm. The Mandelbrot Set is used as the input to the conditional shift algorithm so that the algorithm efficiently applies confusion operation (complete shuffling of pixels). The resultant shuffled vectors are then Bit-XORed (Diffusion) with the saved outputs from the early stage, and eventually, the image vectors are combined to produce the encrypted image. The outcomes of simulation demonstrate the efficiency of the presented scheme in cryptographic applications. Our main achievements in this paper can be sum up in the sequel:

1) We introduce a new and efficient 2-D map exhibiting chaotic dynamics.
2) The dynamic of the proposed map is analyzed with the help of stability of fixed point, Lyapunov exponents, bifurcation diagrams, phase portrait.
3) We design a robust cryptosystem using the sequences of our proposed map.
4) Our proposed cryptosystem is validated using a battery of well-known tests.
5) Security analysis proves the applicability of our cryptosystem in the secure healthcare environment.

II. APPLICATION IN HEALTHCARE
In the scenario of Internet of Healthcare Things (IoHT), the devices are connected to the internet to be able to
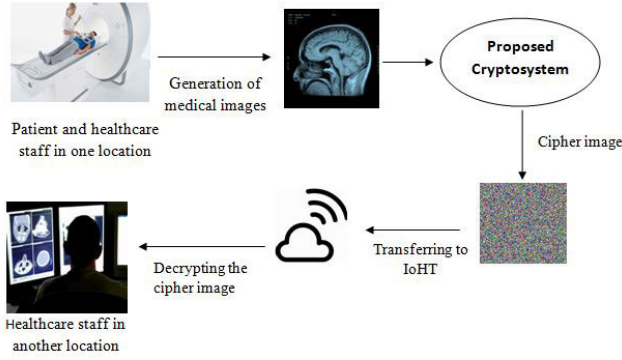
FIGURE 1. Architecture for secure healthcare.

FIGURE 2. Representation of the function $f(x)$ showing the solutions x_0 of system (4).

communicate medical data of patients effectively and also to access to the remote medical facilities with a focus of improving the health of patients promptly. Medical images are of paramount part of a patient's medical data. It needs security while transmitting. Researchers always focus on developing effective and exclusive cryptosystem for transmitting medical images [24]–[28]. Medical images convey very vital information concerning the health condition of patients. Usually, hospitals and other health organizations pay special attention to store and transmit medical images. As IoHT technologies are emerging nowadays, efficient security mechanisms should also be incorporated along with. As we focus on the secure transmission of medical images, this study is an absolute choice to make it secure. Chaos-based cryptography can be applied to transmit medical images effectively. It can simply resist most of the attacks. In this work, we design an exclusive trigonometric map, followed by an effective cryptosystem which enciphers the images of any kind, especially any kind of medical images.

The secure healthcare system is designed as per the following architecture(Fig. 1). The medical images generated at one location are encrypted by our cryptosystem and are transferred using IoHT protocols through the internet. The same image can be deciphered securely at another location for further analysis. In the following sections, we focus on the details of the proposed cryptosystem.

III. 2-D TRIGONOMETRIC MAP
A. STRUCTURE
Recently, the scientific community intensively discussed Logistic and Sine maps [29], [30]. Historically, the Logistic map describes animal population dynamics. A 1-D nonlinear dynamic defines this dynamic as:

$$x_{n+1} = r x_n (1 - x_n), \quad r \in [0, 4] \tag{1}$$

The sinusoidal function was used to derive a 1-D nonlinear dynamic map termed Sine map and defined as:

$$x_{n+1} = r \sin(\pi x_n), \quad r \in [0, 1] \tag{2}$$

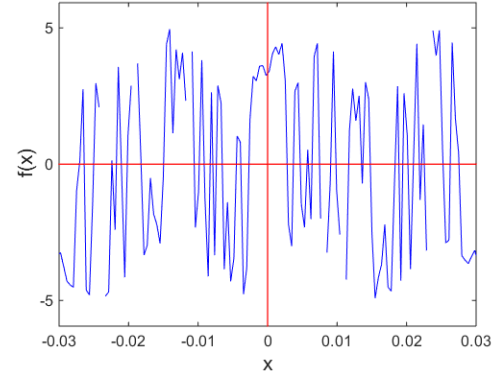Some well-known signal estimation algorithms can be easily used to predict the sequences of almost all existing 1-D

maps [7]. We address in this paper a new 2-D trigonometric map with complex, chaotic behaviour compared to current 2-D maps. The proposed map is settling as:

$$\begin{cases} x_{n+1} = \sin(\omega x_n) - r \sin(\omega y_n) \\ y_{n+1} = \cos(\omega x_n) \end{cases} \tag{3}$$

The map is chaotic for $\omega = 100\pi$, $r \in [0 ; 1000]$ and $x_0 = 1.5$, $y_0 = 0.5$.

B. STABILITY OF EQUILIBRIUM
The behaviour of a system is predicted by the use of stability of its equilibrium points. x_0 is the equilibrium point of a given map defined as $x_{k+1} = f(x_k; M)$ if $x_0 = f(x_0; M)$. Applying this definition to the proposed trigonometric map we can write the following:

$$\begin{cases} x_0 = \sin(\omega x_0) - r \sin(\omega y_0) \\ y_0 = \cos(\omega x_0) \end{cases} \tag{4}$$

To solve system (4) we can set and plot (Fig. 2) the function $f(x) = sin(\omega x) - rsin(\omega cos(\omega x)) - x$ to find the intersection with the line $y = 0$. From Fig. 2 it is patent that the trigonometric map under investigation (4) has infinite number of fixed points $(x_0; y_0)$. These points can be either stable or unstable. To analyze the steadiness of each equilibrium point, we estimate the Eigen values utilizing the following Jacobian matrix (5).

$$J = \begin{pmatrix} \omega \cos(\omega x_n) & -r\omega \cos(\omega y_n) \\ -\omega \sin(\omega x_n) & 0 \end{pmatrix} \tag{5}$$

It is well known that for 2-D maps have two Eigen values λ_1 and λ_2 :
1) $|\lambda_1| \prec 1$ and $|\lambda_2| \prec 1$ indicates steady equilibrium point.
2) $|\lambda_1| \succ 1$ or $|\lambda_2| \succ 1$ indicates unsteady equilibrium point.

In Table 1, we show some fixed points with the related Eigenvalues. From the table, it is evident that the fixed points are stable, given that at least one Eigenvalue has its absolute

TABLE 1. Stability analysis of the fixed point.

(r, ω)	Fixed points x_0 and y_0	Absolute Eigenvalues $|\lambda_1|$ and $|\lambda_2|$	Stability
(10, 314)	$x_0 = -0.0270; y_0 = -0.5843$	$|\lambda_1| = 496.3;\quad |\lambda_2| = 496.3$	unstable
	$x_0 = -0.0180; y_0 = 0.8073$	$|\lambda_1| = 570.6;\quad |\lambda_2| = 570.6$	unstable
	$x_0 = 0.0180; y_0 = 0.8073$	$|\lambda_1| = 711.2;\quad |\lambda_2| = 457.7$	unstable
	$x_0 = 0.0270; y_0 = -0.5843$	$|\lambda_1| = 596.4;\quad |\lambda_2| = 413.0$	unstable

(a)

(b)
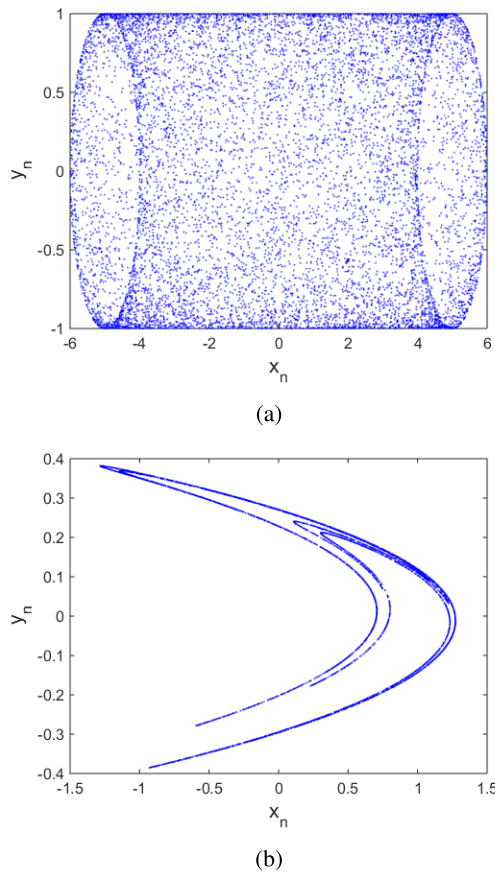
FIGURE 3. Phase portrait of the proposed trigonometric map (a) and the Hénon map (b).

value more significant than the unity. Consequently, neighbouring states can be embossed by the equilibrium point, and the map will be swing.

C. PHASE PORTRAIT

Phase portrait represents a valuable tool to demonstrate the chaotic dynamics in a given dynamical system. We have plotted the phase portrait of the proposed trigonometric map (see Fig. 3). Compared to some well-known 2-D maps like the Hénon map, the states of the proposed trigonometric map are more distributed in the phase plane. Consequently, the trigonometric map understudy can generate more random output sequences.

D. BIFURCATION DIAGRAM

The bifurcations diagram is a nonlinear dynamic system analysis tool showing the asymptotic evolution of the state

of the oscillator. Graphically, the bifurcation diagram is the representation of the sampled steady-state values of one of the variables on the vertical axis versus the variation of the control parameter on the horizontal axis. The dynamic may change from periodic to quasi-periodic, chaotic, or hyper-chaotic behaviour. Figure 3 shows the bifurcations of our proposed trigonometric map and a 2-D map (Hénon map) for comparison.

It should be noted that the dynamic of the Hénon map moves from periodic to chaotic behaviour with intertwining periodicity in chaotic dynamics(see Fig. 4-b). Given that parameter, disturbance can run a system from chaotic dynamic to periodic dynamic, this type of dynamic is not desired in practical applications where the system only works in chaotic windows [7]. To solve this issue, a trigonometric map with an aperiodic bifurcation diagram (see Fig. 4-a) is proposed.

E. HIGHEST LYAPUNOV EXPONENT

The degree of convergence and divergence of close orbits of the attractors for various directions in the state space is called Lyapunov exponent (LE). The n-D dynamic system possesses n LEs. The highest Lyapunov exponent (HLE) is a popular metric used to analyze the behaviour of a dynamical system [31]. Lyapunov exponents of a discrete chaotic map are calculated using the following formula:

$$LE_j = \lim_{t \to \infty} \frac{1}{t} \ln |\lambda_j|, \tag{6}$$

where $j = 1, 2, \ldots, N$ and $\lambda_1, \lambda_2, \ldots, \lambda_N$ are the N Eigenvalues of the Jacobian matrix. Three cases can be considered concerning the value and the sign of the Lyapunov exponents:

1) If $HLE \succ 0$, we conclude that the map is chaotic. Also, if the HLE is large enough, this shows that close orbits diverge quickly;
2) If the system possesses more than one positive Lyapunov exponents, hyperchaotic behaviour is identified;
3) If $HLE \leq 0$, the dynamic of the system is periodic.

Using the Wolf algorithm [31], we computed the HLE (Fig. 4-a) of the trigonometric map and the HLE of Hénon map (see Fig. 5-b). It is evident that collated to Hénon map, the HLE of the proposed trigonometric map is always positive and get more substantial. Consequently, close trajectories diverge faster.

F. ApEn: APPROXIMATE ENTROPY

ApEn (Approximate entropy) represents a measure employed to measure the rate of reliability and the uncertainty in the
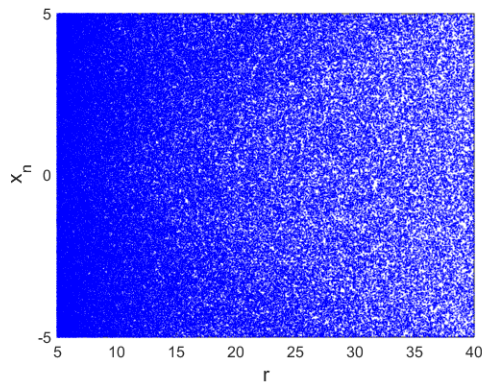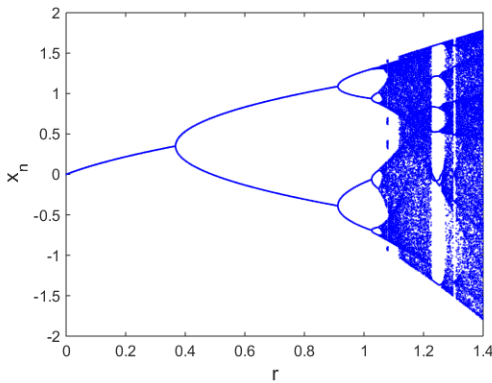
FIGURE 4. Bifurcation plot of the trigonometric map (a) and the Hénon map (b).

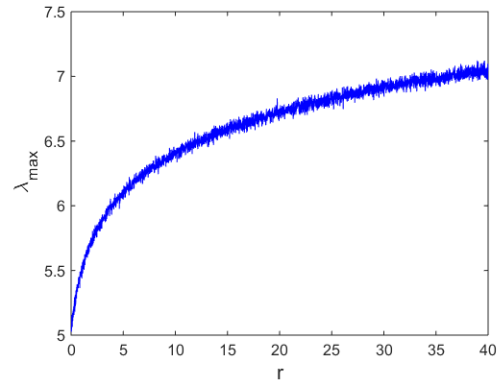FIGURE 5. HLE of the proposed trigonometric map (a) and the Hénon map (b).

variations of series information [32]. It was also used to investigate the chaotic behaviour of chaos-based systems [33]. Indeed, it quantifies the complexity and irregularity of the time series derived from chaotic systems. An interpretation of such entropy is as follows: Series with much redundancy in its variation is more foreseeable than series with reduced redundancy. ApEn computes the probability that identical patterns of objection does not cause extra similar observations [34]. A small ApEn reflects many redundancy patterns in the considered time series, while high ApEn refers to better unpredictability in such time series. The calculation details of ApEn are as follows:

Let $x(1), x(2), \ldots, x(N)$ be a N data sample, $y(1), y(2), \ldots, y(N-m+1) \in R^m$ and a m-D sequence given as:
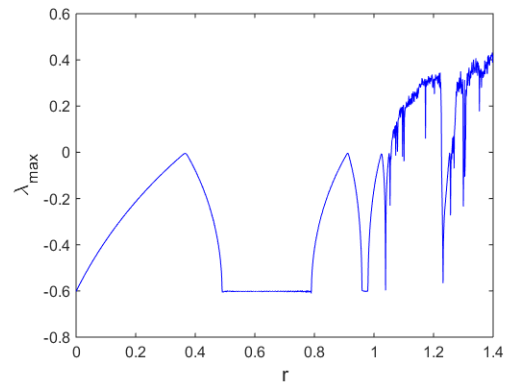
$$y(i) = [x(i), x(i+1), \ldots, x(i+m-1)] \quad (7)$$

where $i \in 1 \le i \le N - m + 1$ and m denotes the length of compared run of data. The length amid $y(i)$ and $y(j)$ is expressed as

$$d[y(i), y(j)] = \max_{h=1,\cdots,m} (|x(i+h-1) - x(j+h-1)|) \quad (8)$$

The statistics of $d[y(i), y(j)]$ within a filtering level $r(r > 0)$ is calculated as

$$C_i^m(r) = (N - m + 1)^{-1} Sum\{d[y(i), y(j)] \le r\} \quad (9)$$

The mean of the logarithm of C_i^m can be calculated as

$$\phi^m(r) = (N - m + 1)^{-1} \sum_{i=1}^{N-m+1} \ln C_i^m(r) \quad (10)$$

Accordingly, the ApEn is given as:

$$ApEn(m, r) = \lim_{N \to \infty} \left[\phi^m(r) - \phi^{m+1}(r) \right] \quad (11)$$

Given that the data sample N is small, the ApEn is simplified as

$$ApEn(m, r, N) = \phi^m(r) - \phi^{m+1}(r) \quad (12)$$

Figure 6 shows the ApEns of the trigonometric map versus those of the Hénon map. It is found that the ApEns of the trigonometric map are always higher than those of the Hénon map. The average ApEns of x_n/y_n time series is equal to 1.0887/1.1758 for the proposed map and to 0.4581/0.4576 for the Hénon map. Consequently, the trigonometric map is more complex than the Hénon map, i.e., it can produce time series with better unpredictability behaviour.
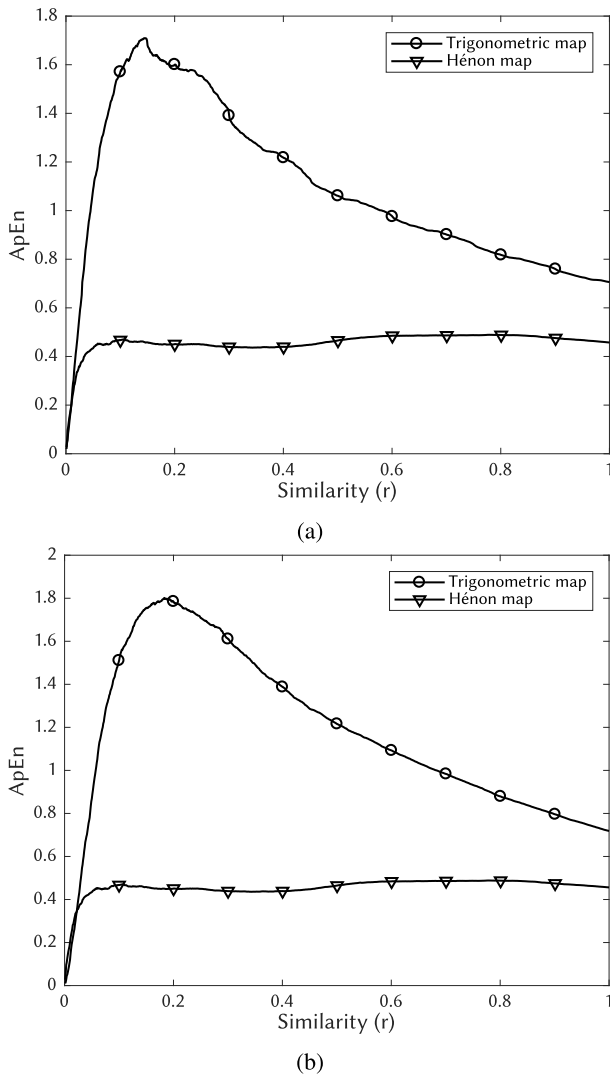
(a)

(b)

Let us start by presenting the new conditional shift algorithm based on a new Mandelbrot Set:

A. MODIFIED MANDELBROT SET

A complex plane with a collection of points is defined as Mandelbrot Set. A given point P in the complex plane is related to a complex number $p \in C / p = re^{j\theta}$ where r is the magnitude of p and θ is its argument. A point P in the complex plane belongs to the Mandelbrot Set if:

$$\lim_{n \to \infty} \left\| z_{n+1} = z_n^2 + p \right\| \to \infty \quad where \ z_0 = 0. \quad (13)$$

If a set of points belonging to the Mandelbrot set in the complex plane are coloured in grey, we obtain the shape of Fig. 7-a. To elucidate the set of pixels coloured in black from Fig. 7-a we used algorithm 1 to achieve a new Mandelbrot (Figure 7-b) set where $W(i, j)$ represents the intensity of the pixel situated at the position (i, j) in Fig. 7-a.

Algorithm 1 Modified Mandelbrot Set

Input: read the image of figure 6-a
Output: obtain the image of figure 6.b
if W(i,j) == 0 then
    $W(i, j) = [(i * j) + c] \mod 256$
end

B. NEW CONDITIONAL SHIFT ALGORITHM

The conditional shift algorithm used in combination with the modified Mandelbrot set image is outlined as in Algorithm 2.

C. PROPOSED ENCRYPTION ALGORITHM

As mentioned above, a new conditional shift algorithm based on a modified Mandelbrot Set is used to generate confusion on the constituents of the plain colour image. Using the XOR operation, we diffuse the confusing image to achieve the cipher image. The general framework of the proposed cryptosystem is depicted in Fig. 8 and nine steps can be used for description.

IV. TRIGONOMETRIC ENCRYPTION

Image encryption techniques can be mainly categorized into spatial domain based techniques and transform-based techniques. Image enciphering methods based on the spatial domain are those techniques applied directly to the pixels of the input image [35]–[38]. In the case of transform-based cryptosystems, the plain text is converted from spatial area to the frequency area by the usage of some well-known mathematical transformations. The reconstructed image is encrypted and re-transform from the frequency domain to the spatial domain [39]. Due to the unique properties of chaotic sequences, the chaos-based enciphering method is one of the best encryption techniques in spatial domain encryption [40]. In this context, we designed an unbreakable cryptosystem using the sequence of the proposed trigonometric chaotic map. A new conditional shift algorithm based on a modified Mandelbrot Set is used to create confusion on the constituents of input colour images. Using the bit-xor operation, we diffuse the confusing image to achieve the cipher image.
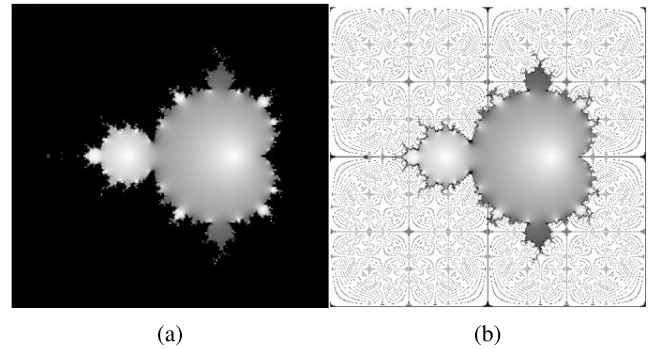

Algorithm 2 New Conditional Shift Algorithm

Input: M is the modified Mandelbrot set image of figure 6-b, X_{DR}, X_{DG} *and* X_{DB} are the output of bit XOR amid R, G and B channels of the plain image and chaotic sequences.

Output: S_R, S_G *and* SB are the final shifted matrices corresponding respectively to X_{DR}, X_{DG} and X_{DB}

while $i = 0$ *to n do*

    //n represents the total of columns in M

    Find the maximum value of ith row elements of X_{DR}, X_{DG} and X_{DB};

    denote them as $\max_{ri}$, $\max_{gi}$, $\max_{bi}$ *respectively.*

    Apply shifting operation as follows :

    case 1 *do if* $(\max_i \leq \max_{bi})$ *then*

        apply left cyclic shift $\max_i$ *times on i^{th} row of X_{DR}*

          else apply right cyclic shift $\max_i$ *times on i^{th} row of X_{DR}*

          end if

    end

    case 2 *do if* $(\max_i \leq \max_{ri})$ *then*

        apply left cyclic shift $\max_i$ *times on i^{th} row of X_{DG}*

          else apply right cyclic shift $\max_i$ *times on i^{th} row of X_{DG}*

          end if

    end

    case 3 *do if* $(\max_i \leq \max_{gi})$ *then*

        apply left cyclic shift $\max_i$ *times on i^{th} row of X_{DB}*

          else apply right cyclic shift $\max_i$ *times on i^{th} row of X_{DB}*
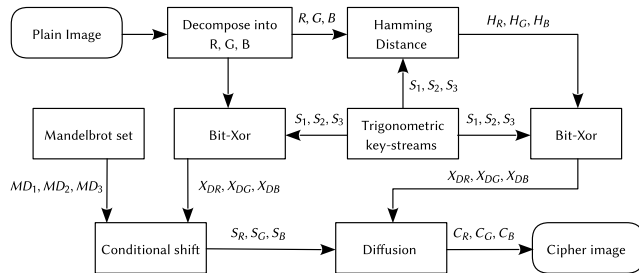
          end if

    end

FIGURE 8. General framework of the proposed cryptosystem.

Step 1: Input a plain image, P. we used medical colour images labelled as "Img01", 'Img02' and "Img03" each of dimension 256×256.

Step 2: Decompose P to R, G, and B constituent and convert them to binary form.

Step 3: Using the trigonometric map, we generate three chaotic sequences (S_1, S_2 and S_3) for each component of the input image. Initial seed are $x_0 = 1.5$; $y_0 = 0.5$; $r = 10$; $\omega = 314$. Normalize each sequence using $S_i = mod((X_i \times (10^{10}), 256)$ $i = 1, 2, 3$ and convert them to their respective binary form.

Step 4: Apply XOR operation amid the binary R, G, B channels and the binary form of chaotic sequence (S_1, S_2, and S_3) and produce three outputs: X_{DR}, X_{DG} and X_{DB} as:

$$X_{DR}(i) = bitxor(R(i), S_1(i)); \tag{14}$$

$$X_{DG}(i) = bitxor(G(i), S_2(i)); \tag{15}$$

$$X_{DB}(i) = bitxor(B(i), S_3(i)); \tag{16}$$

Step 5: Calculate the Hamming distance between R, G, B, and chaotic Sequences to produce H_R, H_G and H_B as:

$$H_R(i) = Ham\_dist(R(i), S_1(i)) \tag{17}$$

$$H_G(i) = Ham\_dist(R(i), S_2(i)) \tag{18}$$

$$H_B(i) = Ham\_dist(R(i), S_3(i)) \tag{19}$$

For any two numbers a and b, the hamming distance between them is defined as the different bits count at the same position in both a and b.

Step 6: Realize XOR operation on Hamming distance and chaotic sequences to produce X_R, X_G and X_B as:

$$X_R(i) = bitxor(H_R(i), S_1(i)); \tag{20}$$

$$X_G(i) = bitxor(H_G(i), S_2(i)); \tag{21}$$

$$X_B(i) = bitxor(H_B(i), S_3(i)); \tag{22}$$

Step 7: Perform conditional shift algorithm (see algorithm 2) on X_{DR}, X_{DG} and X_{DB} using M_{D1}, M_{D2} and M_{D3} generated from Mandelbrot Set (see algorithm 1) to perform confusion and produces S_R, S_G and S_B.

Step 8: Final diffusion operation using bit-xor on S_R, S_G, S_B and X_R, X_G, X_B to produce the cipher image components
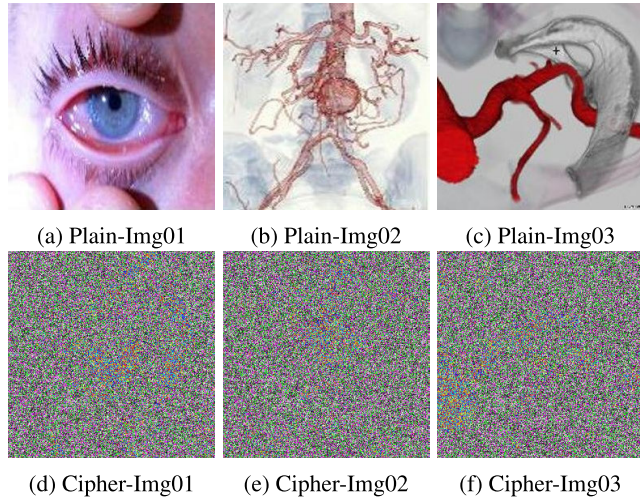
| (a) Plain-Img01 | (b) Plain-Img02 | (c) Plain-Img03 |
| (d) Cipher-Img01 | (e) Cipher-Img02 | (f) Cipher-Img03 |

FIGURE 9. Results of visual tests.

TABLE 2. NPCR and UACI outcomes.

Image	NPCR %	UACI %
Img01	99.6195	33.5867
Img02	99.6134	33.4794
Img03	99.6109	33.4748

TABLE 3. Chi-square test of the histograms.

Image	Component	χ^2-test	
		Score	Result
Img01	R	287.992	Pass
	G	256.687	Pass
	B	291.929	Pass
Img02	R	253.867	Pass
	G	226.398	Pass
	B	232.710	Pass
Img03	R	257.859	Pass
	G	244.242	Pass
	B	225.117	Pass

as follows:

$$C_R(i) = mod(((bitxor(S_R(i), X_R(i)))), 256); \quad (23)$$
$$C_G(i) = mod(((bitxor(S_G(i), X_G(i)))), 256); \quad (24)$$
$$C_B(i) = mod(((bitxor(S_B(i), X_B(i)))), 256); \quad (25)$$

Step 9: The image components are fused to form the final cipher image C.

V. SECURITY ANALYSIS OF THE PROPOSED CRYPTOSYSTEM

To examine and assess the security of the above encryption, the trigonometric chaotic map with infinite equilibrium is solved with initial seed as: $x_0 = 1.5$ and $y_0 = 0.5$ and system parameter as $\omega = 314$ and $r = 10$. The data set is composed of three different colour images each of size 256×256 ("*Img03*", "*Img02*" and "*Img01*"). The simulations were done on a laptop endowed with Intel processor ® core TM i5-2450QM 6 GB of RAM and MATLAB R2016b application software. Figure 9 shows the outcome of visual tests. The coded images are visually unrecognizable. However, some security analysis tools like statistical, differential analysis need to be carried to validate the encryption process.

A. NPCR AND UACI ANALYSIS

NPCR and UACI are the main metrics utilized to certify if a cryptosystem can withstand differential intrusions [41]. NPCR determine the quota of different intensity pixel among two encoded images of $I(i, j)$ and $I'(i, j)$ while UACI measures the mean intensity of divergence between the encrypted version of $I(i, j)$ and $I'(i, j)$. Mathematical computations are:

$$NPCR = \frac{\sum_{i=0}^{m-1} \sum_{j=0}^{n-1} D(i, j)}{m \times n} \times 100, \quad (26)$$

where $D(i, j) = \begin{cases} 1, & if\ E(i, j) \neq E'(i, j) \\ 0, & if\ E(i, j) = E'(i, j) \end{cases}$

$$UACI = \frac{1}{m \times n} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} \frac{\left| IE(i, j) - I'(i, j) \right|}{255} \times 100 \quad (27)$$

NPCR and UACI range from 0 to 100. A good cryptosystem should lead to an NPCR close to 100%. Generally, the UACI of useful encryption algorithms is close to 33.6% [42]. Table 2 provides NPCR and UACI of data set, modifying the unique from different positions. From these results, the proposed encryption algorithm is unbreakable.

B. HISTOGRAM AND CHI-SQUARE ANALYSES

Histogram and Chi-square analyses are two metrics commonly used to test the robustness of a cryptosystem against third party intrusion. With this regard, uniformity in the distribution of pixels is the property of encrypted data, while original data pixels are non-uniformly distributed. Figure 10 illustrates the histograms of the output images, which are flat and histograms of input images completely different from the previous ones. This flatness is more verified by applying the Chi-square analysis [23]. Table 3 lists the Chi-square results along with their *p*-values whit a weight level of 0.05 considered for the histograms of the cipher images. The Chi-square test is accepted (i.e., the histogram is uniform) if the obtained score is smaller than $\chi^2_{th}(255, 0.05) = 293.2478$, i.e., the corresponding *p*-value is higher than 0.5. According to results given in Table 3, the histograms of the encoded images follow the features of uniformity in the distribution of pixels. This proves that the cryptosystem under investigation can effectively withstand any histogram-based attack.

C. CORRELATION OF ADJACENT PIXELS

A cryptosystem can resist statistical intrusion when the correlation is minimized. The following computations were carried
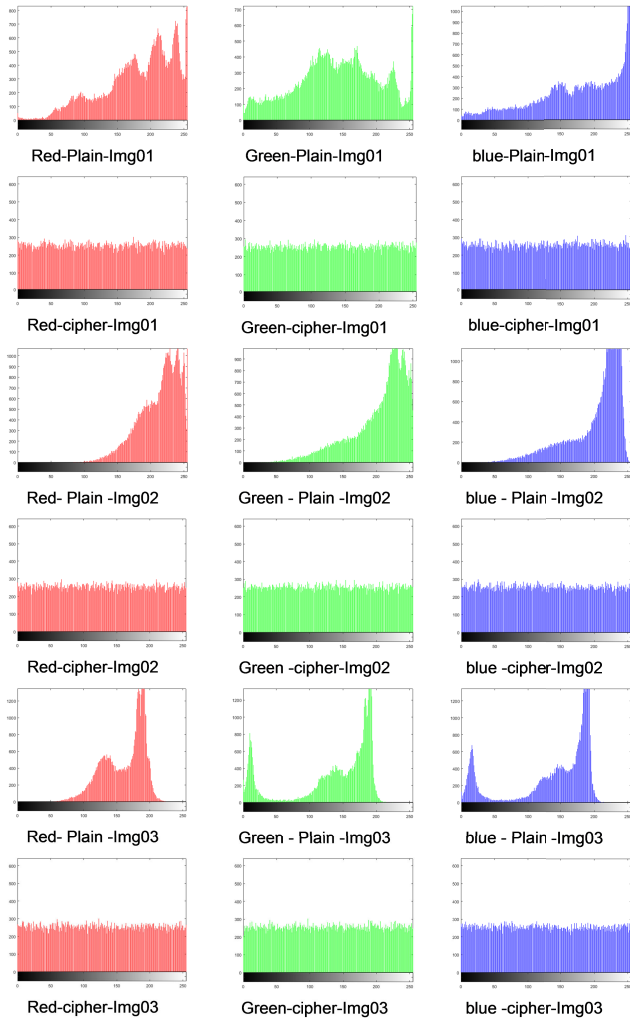
FIGURE 10. Histograms representation of the plain and encrypted data set (R, G, and B channels).

out to achieve the correlation values:

$$Cor_{xy} = \frac{E\left((x - E\left(x\right))\left(y - E\left(y\right)\right)\right)}{\sqrt{D\left(x\right)}\sqrt{D\left(y\right)}}$$

$$with \quad E\left(x\right) = \frac{1}{N}\sum_{i=1}^{N}x_i$$

$$and \quad D\left(x\right) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E\left(x\right)\right)^2 \quad (28)$$

where x and y symbolized the values of the pixels at the same index of the images I and I'; $P(x)$ and $T(x)$ the variances with N the number of used pixels. Table 4 groups together the correlation coefficients obtained from the original and encoded images. Besides, the distribution of neighbouring pixels is represented in Table 5. It is evident from Table 5 that we achieve minimal correlation values in three directions, including vertical, horizontal, or diagonal. Consequently, the encryption scheme is unbreakable by the attackers regarding the Correlation coefficient.

TABLE 4. Correlation coefficient of test images.

Image	Direction	R	G	B
Img01	H	-0.0018	0.0020	-0.0012
	V	0.0018	0.0025	0.0020
	D	0.0002	-0.0015	-0.0008
Img02	H	-0.0010	-0.0001	0.0010
	V	0.0007	0.0008	-0.0009
	D	0.0001	-0.0019	-0.0022
Img03	H	-0.0007	0.0013	0.0005
	V	-0.0013	0.0028	-0.0001
	D	-0.0014	0.0018	-0.0008

D. BIT DISTRIBUTION UNIFORMITY INSIDE EACH BIT-PLANE

Bit-planes are produced by converting an image to its binary form. They consist of the group of bits relative to each bit location in the binary representation of the pixels. In grayscale images, the pixels are encoded into 8 bits, which yields eight bit-planes. As reported in [43], the higher bit-planes in a plain image present high correlation values, which can be in favour of a potential attacker; he/she tries to extract some useful information by analyzing the connection in higher bit-area. To overcome such an issue, the percentage of 1's and 0's within each bit-plane must be at a balanced rate of 50%. It is clear from Table 6 that, for all testes images, the percentage of 1's within all bit-planes are very close to 50%, which reflects an excellent uniformity within these bit-planes. So, no information can be provided by examining the distribution rate of 1's and 0's in these bit-planes.

E. SHANNON ENTROPY

Shannon entropy measures the amount of information hidden in an image. It is an evaluation of the randomness for a given image. Considering the probability $p(z_i)$ of each pixel z_i, we can compute the global entropy as:

$$E\left(z_i\right) = -\sum_{i=0}^{255} p\left(z_i\right) \log_2 p\left(z_i\right), \quad (29)$$

The pixels of an image are randomly distributed if the entropy value is close to 8 [13], [41]. Nevertheless, this randomness is efficiently evaluated using local entropy rather than global [41]. Table 7 provides the global and local entropies calculated for the used data set. It obvious from these results to conclude that the proposed trigonometric encryption achieves highly randomness in the cipher images.

F. KEY RANGE ANALYSIS

To withstand brute force intrusions, the key range of a cryptosystem should be above 2^{100}. The keyspace is defined as the set of all combinations of secret keys:

1) The values of parameter-r ranges from 0 to 1000 *(three different values from the range for each channel)*
2) The matrices of the hamming distance corresponding to each component: H_R, H_G, H_B. (256 x 256 is the size of both the Hamming distance matrix and the image.
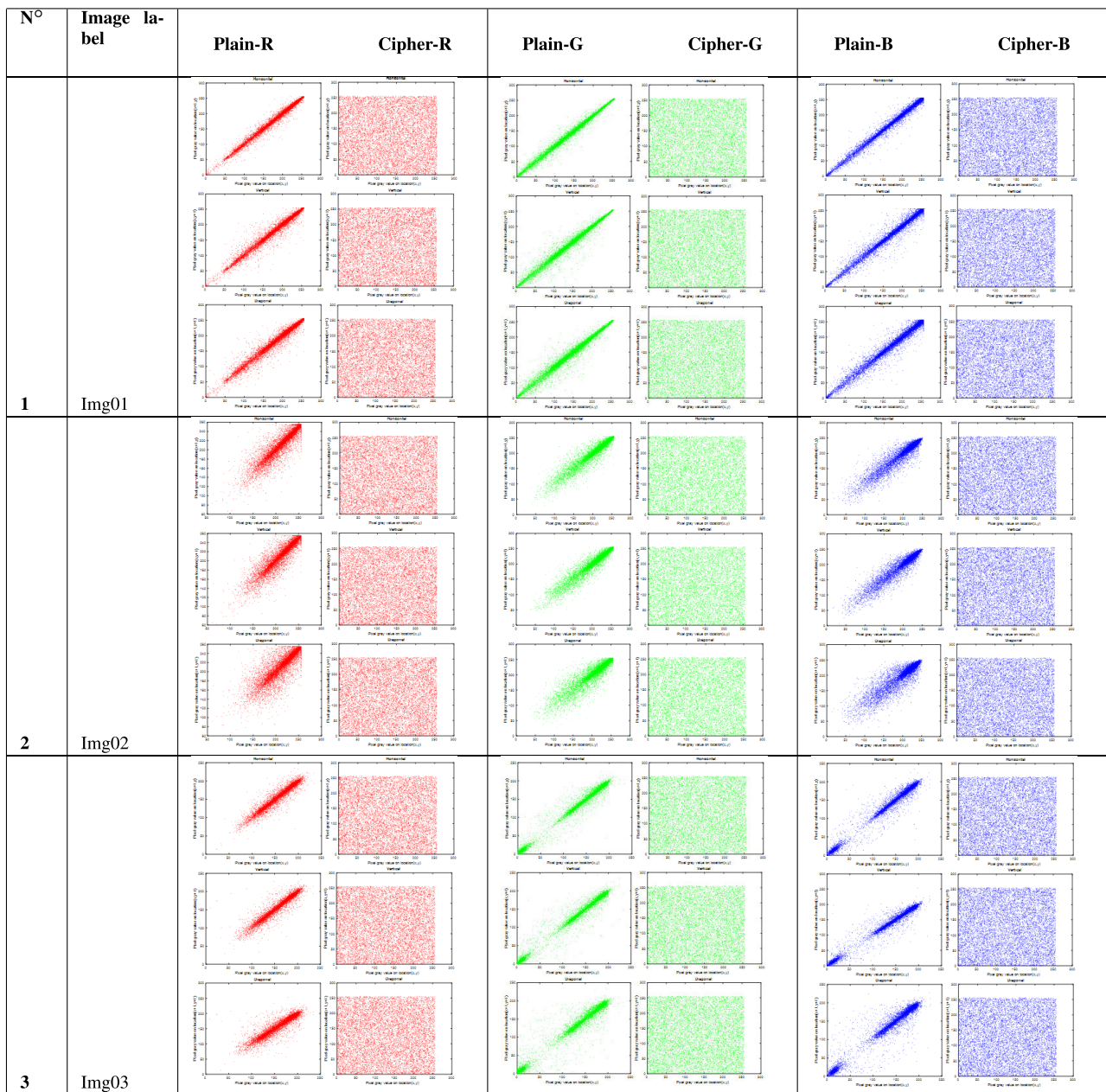
137739

TABLE 5. Correlation distribution of cipher images.

N°	Image label	Plain-R	Cipher-R	Plain-G	Cipher-G	Plain-B	Cipher-B
1	Img01						
2	Img02						
3	Img03						

TABLE 6. Percentage of '1's in cipher images for the proposed scheme.

Image	Component	8th bit	7th bit	6th bit	5th bit	4th bit	3rd bit	2nd bit	1st bit
Img01	R	49.9420	49.9374	50.3112	49.0997	50.1770	49.8138	50.1083	50.2502
	G	50.0549	50.2075	49.9176	49.9816	49.9069	49.9038	50.5447	50.0671
	B	50.1892	49.9435	49.7222	50.1708	50.2059	50.0427	50.4196	50.1846
Img02	R	49.7040	49.9496	50.0580	50.0031	50.1053	49.8871	49.9619	49.8535
	G	49.9146	49.8901	50.1312	49.9695	50.0015	50.1099	49.9237	49.8291
	B	49.6109	50.0595	49.7910	50.2991	49.7498	49.9451	49.9954	49.9374
Img03	R	49.6216	50.2441	49.7910	49.9741	49.8734	50.0748	49.9176	49.8550
	G	50.2274	50.1205	49.9283	49.4446	50.1984	50.1068	49.9725	49.9390
	B	49.5407	50.2289	49.9588	49.8947	49.8047	49.9664	49.9084	49.8932

There are $(1001 \times 10^{15})^3$ different values for r. There are 65,536 elements in each matrix. There are 256 (0–255) different values possible for each element location. For the entire three hamming distance matrices, the total number of different values possible is around $256^{(65,536\times3)}$. So the total keyspace is around $(2 \times 10^{15})^3 \times (256)^{(65,536\times3)}$. This value

**TABLE 7.** Global and local entropies for the encrypted data set.

Image	Component	Global entropy	Local entropy
Img01	R	7.9968	7.9040
	G	7.9972	7.8990
	B	7.9968	7.9021
Img02	R	7.9972	7.9033
	G	7.9975	7.9031
	B	7.9974	7.9014
Img03	R	7.9972	7.9037
	G	7.9973	7.9039
	B	7.9975	7.9036

FIGURE 11. Cipher images of the (a) all-black and (c) all-white images; their histograms (b) and (d), respectively.

FIGURE 12. Correlation of adjacent pixels couples (in the horizontal, vertical, and diagonal directions) for the all-black and all-white images in row-major order.

is greater than 2^{100}, which shows that our system is resistant to brute-force attacks. Apart from these keys, we also use some keys with a modified Mandelbrot set and the fixed initial values of the Trigonometric map.

G. CLASSICAL TYPES OF ATTACK

Everyone can see and interpret the encryption architecture, and its working as it is open to all, except the keys that are transferred between the sending and receiving side. Among the classical type of attacks (chosen-plaintext, chosen ciphertext, ciphertext only, and known-plaintext attack) chosen-plaintext attack is the most dangerous [44]. In this attack, the hacker uses the vulnerability of the system to obtain access to the cryptosystem and recover the ciphertext temporarily. When a cryptosystem resists to chosen-attacks, it can withstand the remaining three intrusions. Our algorithm is susceptible to parameter r of the trigonometric map proposed and also to the initial seed of the same map. It is very significantly stating that there is an essential step in the encryption algorithm, which deals with the calculation of the Hamming distance among the constituent components of the input image and the chaotic key sequences. The hamming distance vectors are also acting as keys.

The Hamming distance sequence plays a significant function in the subsequent processing and the overall security of our encryption system. Consequently, the cryptosystem under investigation depends on both the keys and the plain image. Thanks to their ability to disabling the permutation/substitution processes, the all-black, and all-white data set are the most popular chosen images for breaking an image cryptosystem. By doing so, the attacker tries to recover some valuable data from the secret key. Figure 11 depicts the cipher full-black and full-white images, alongside their histograms. The cipher images are noisy-like images so that no visual information can be extracted from them. Figure 12 illustrates the correlation among bordering pixels pairs of the cipher full-black and cipher full-white images. Table 8 lists some quantitative statistical analyses for full-black images and full-white images. It is found for both cipher images that the histograms match to a uniform distribution, the adjacent pixel pairs satisfy zero-correlation, and the global and local entropies are nearly equal to their ideal values of 8 and 7.9024693 [23], respectively. Accordingly, the proposed scheme is qualified to encipher full-black and
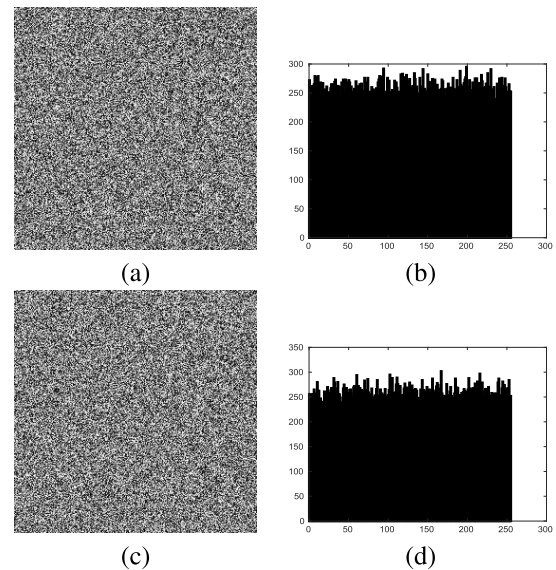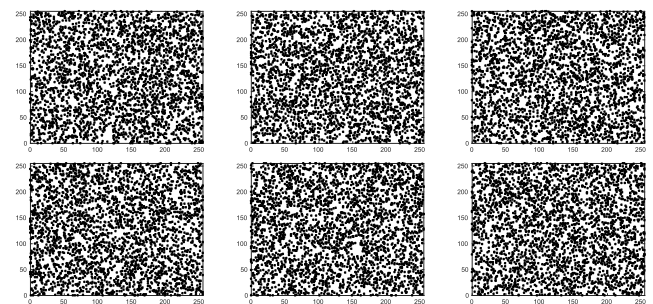
full-white images ideally and resisting known-plaintext and chosen-plaintext attacks.

H. NOISE INTRUSION ANALYSIS

During the acquisition of images, Gaussian noise is added to the images. This noise is mainly due to the level of illumination and electronic circuits connected to the sensor. A robust encryption/decryption technique should be able to operate on such type of images. Another type of noise mostly encountered on images is the salt-and-pepper noise. It is mainly introduced in the image by the error elements from the analogue-to-digital converter or through bit changes that occurred during transmission. Salt & pepper noise affects the image in such a way that bright regions will be affected by dark pixels, and dark regions will be affected with bright pixels [45]. A well-designed encryption algorithm must resist to this noise. To prove the robustness of the encryption/decryption algorithm, a low level of Gaussian noise and salt & pepper noise is induced into the encrypted image. Our algorithm is then used to decrypt the noise-infected cipher images. Table 9 shows that the decrypted images are

TABLE 8. Statistical analyses of the cipher full-black and full-white images.

Image	χ^2 test of histogram		Correlation			information entropy	
	score	p-value	Horizontal	Vertical	Diagonal	Global entropy	Local entropy
full-black	245.2969	0.6575	0.0023	0.0015	-0.0030	7.9973	7.9008
full-white	233.2422	0.8321	-0.0005	0.0005	-0.0052	7.9974	7.8998

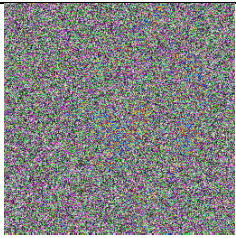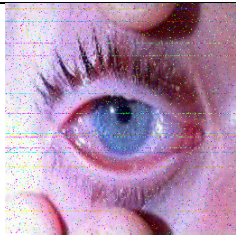**TABLE 9.** Gaussian noise and Salt & pepper noise attack analysis.
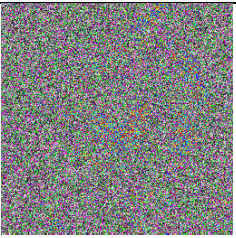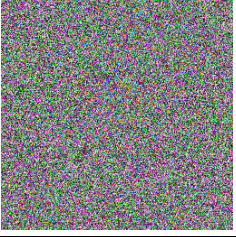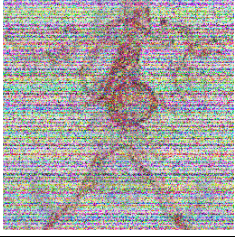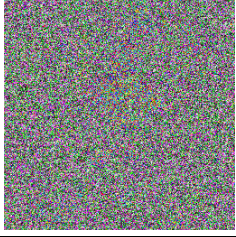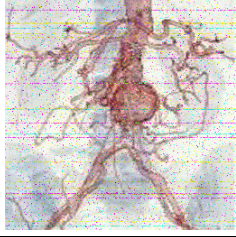
N°	image name	Gaussian noise encrypted	Gaussian noise decrypted	Salt & pepper noise encrypted	Salt & pepper noise decrypted
1	Img01				
2	Img02				
3	Img03				

TABLE 10. Comparison of running speed of the proposed algorithm (in seconds) and other related algorithms for various sizes of images.

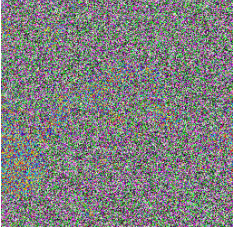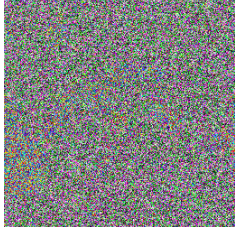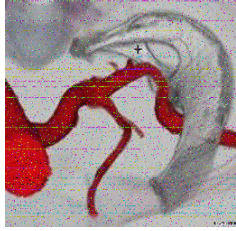| Scheme	Type	Image size			
		128×128	256×256	512×512	1024×1024
Proposed	Colour image	0.126985	0.258994	0.655412	1.323154
Ref. [41]	Grey-scale image	0.0138	0.0487	0.2177	0.7813
Ref. [46]	Grey-scale image	0.0244	0.0949	0.4010	1.9857
Ref. [9]	Grey-scale image	0.013	0.0538	0.2338	1.1494
Ref. [47]	Grey-scale image	-	0.382	1.489	-
Ref. [48]	Grey-scale image	-	0.5554	-	-

understandable. We can observe that the encryption method is more efficient with Salt & pepper.

I. OCCLUSION ATTACK

During transmission of the cipher image from sender to receiver, some data or pixel information may be occluded or lost. A transmission channel can cause a mislay of a part of the transmitted message [24], [26]. Our cryptosystem must be efficient in terms of resisting occlusion attacks too. Through analysis, we test the capacity of producing original images from the occluded cipher images. This test consists of creating on the encrypted image of size $m \times n$, a dark matrix

of size $w \times h$ with $w \times h \ < \ m \times n$. Our algorithm is then used to decrypt the cipher images with occlusion areas. The results are shown in Fig. 13. Accordingly, occlusion does not affect the decryption process.

J. ENCRYPTION TIME

One of the essential measures to assess the performance of an algorithm is its running speed. An encryption algorithm should take minimum execution time so that it can be effectively used in enciphering images. The tech world accepts only those with fast response [41]. In that sense, we should also check the speed of our proposed encryption algorithm

TABLE 11. Comparison of average values of correlation coefficients, NPCR, UACI, χ^2-test, and information entropy of the proposed mechanism alongside other related schemes.

Algorrithm	Correlation			NPCR%	UACI%	χ^2-test	Entropy	
	H	V	D				Global	Local
Proposed	0.00267	-0.00008	-0.00007	99.633	33.53	254.9902	7.9972	7.9021
Ref. [41]	-0.0042	-0.0049	-0.0045	99.6101	33.525	249.8444	7.9995	7.9030
Ref. [49]	-0.0016	-0.0026	0.0116	99.598	33.43	249.4286	7.9972	7.9025
Ref. [50]	0.0022	0.0017	0.0019	99.611	33.47	240.3535	7.9993	7.9024
Ref. [51]	0.0020	0.0007	0.0004	99.5215	33.2585	277.9708	7.9824	-
Ref. [46]	-0.0033	-0.0008	- 0.0002	99.6061	33.4548	-	-	-

(a) occluded-cipher-Img01 (b) occluded-cipher-Img02 (c) occluded-cipher-Img03

(d) Decrypted-Img01 (e) Decrypted-Img02 (f) Decrypted-Img03
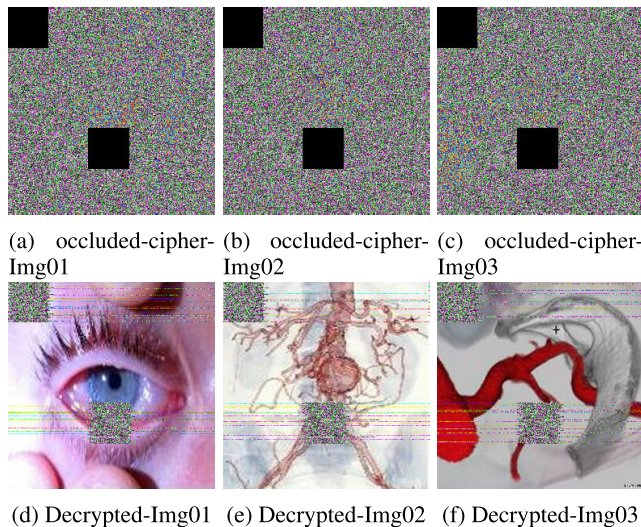
FIGURE 13. Occlusion attack results.

against each test image. Table 10 shows the running speed of the proposed algorithm (in seconds) and other related algorithms as reported in [9], [41], [46]–[48] for various size of images, which demonstrates the efficiency of the presented mechanism. Note that the stated results in Table 10 are for tested grey-scale images except our proposed mechanism are for colour images.

K. COMPARATIVE ANALYSIS

This part verifies how well the evaluation of different parameters in terms of security is boosted over existing works. Table 11 compare the evaluation measures of correlation coefficients, NPCR, UACI, χ^2-test, and information entropy with other related schemes. The cryptosystem behaves in such a way that it exhibits high sensitivity to the input image, and it can block the classical types of intrusions, showing that our system possesses more security features than existing schemes.

VI. CONCLUSION

In this work, we designed a 2-D trigonometric map. First, some well-known dynamic analysis tools like Lyapunov exponent, bifurcation diagram, and phase space trajectories are used to illustrate the chaotic dynamic of the map. Beyond, it was shown that the map has infinite equilibria. Second,

a robust encryption/decryption scheme for colour images is designed. The encryption/decryption scheme is based on four ingredients: the proposed trigonometric map, Mandelbrot Set, Bit-XOR operation, and new Conditional shift operation. The dominant contribution in our study is to introduce a chaotic-cryptographic system which can block all forms of intrusions, and also improve the Shannon entropy measure of the cipher images. A variety of metrics are used for experimental validation of the proposed algorithm, including histogram study, Shannon entropy study, NPCR, and UACI study, keyspace study, Noise attack study, occlusion study, and speed study. Finally, a comparative analysis shows the superiority of our algorithm over some robust existing algorithms. The analysis part clearly proves that the system can be effectively used to encrypt medical images in IoHT framework. In future investigations, we intend to combine discrete orthogonal moment and s-box to design and implement on raspberry board a new robust encryption algorithm.

REFERENCES

[1] J. Piórek, "On generic chaos of shifts in function spaces," *Ann. Polonici Math.*, vol. 52, no. 2, pp. 139–146, 1990.

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

[3] N. Tsafack and J. Kengne, "Complex dynamics of the Chua's circuit system with adjustable symmetry and nonlinearity: Multistability and simple circuit realization," *World J. Appl. Phys.*, vol. 4, no. 2, p. 24, 2019.

[4] L. K. Kengne, J. R. M. Pone, H. T. K. Tagne, and J. Kengne, "Dynamics, control and symmetry breaking aspects of a single opamp-based autonomous LC oscillator," *AEU-Int. J. Electron. Commun.*, vol. 118, May 2020, Art. no. 153146.

[5] A. Belazi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Selective image encryption scheme based on DWT, AES S-box and chaotic permutation," in *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, Aug. 2015, pp. 606–610.

[6] J. Peng, A. A. A. El-Latif, A. Belazi, and Z. Kotulski, "Efficient chaotic nonlinear component for secure cryptosystems," in *Proc. 9th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2017, pp. 989–993.

[7] Z. Hua and Y. Zhou, "Exponential chaotic model for generating robust chaos," *IEEE Trans. Syst., Man, Cybern. Syst.*, early access, Aug. 28, 2019, doi: 10.1109/TSMC.2019.2932616.

[8] X. Wu, H. Hu, and B. Zhang, "Parameter estimation only from the symbolic sequences generated by chaos system," *Chaos, Solitons Fractals*, vol. 22, no. 2, pp. 359–366, Oct. 2004.

[9] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.

[10] A. Kadir, A. Hamdulla, and W.-Q. Guo, "Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN," *Optik*, vol. 125, no. 5, pp. 1671–1675, Mar. 2014.

[11] H.-K. Chen and C.-I. Lee, "Anti-control of chaos in rigid body motion," *Chaos, Solitons Fractals*, vol. 21, no. 4, pp. 957–965, Aug. 2004.

[12] J. Kengne, V. R. F. Signing, J. C. Chedjou, and G. D. Leutcho, "Nonlinear behavior of a novel chaotic jerk system: Antimonotonicity, crises, and multiple coexisting attractors," *Int. J. Dyn. Control*, vol. 6, no. 2, pp. 468–485, Mar. 2017.

[13] N. Tsafack and J. Kengne, "Multiple coexisting attractors in a generalized Chua's circuit with a smoothly adjustable symmetry and nonlinearity," *J. Phys. Math.*, vol. 10, no. 298, pp. 0902–2090, 2019.

[14] G. D. Leutcho and J. Kengne, "A unique chaotic snap system with a smoothly adjustable symmetry and nonlinearity: Chaos, offset-boosting, antimonotonicity, and coexisting multiple attractors," *Chaos, Solitons Fractals*, vol. 113, pp. 275–293, Aug. 2018.

[15] S. Jafari, J. C. Sprott, and S. M. R. H. Golpayegani, "Elementary quadratic chaotic flows with no equilibria," *Phys. Lett. A*, vol. 377, no. 9, pp. 699–702, Mar. 2013.

[16] M. Molaie, S. Jafari, J. C. Sprott, and S. M. R. H. Golpayegani, "Simple chaotic flows with one stable equilibrium," *Int. J. Bifurcation Chaos*, vol. 23, no. 11, Nov. 2013, Art. no. 1350188.

[17] T. Gotthans and J. Petržela, "New class of chaotic systems with circular equilibrium," *Nonlinear Dyn.*, vol. 81, no. 3, pp. 1143–1149, Apr. 2015.

[18] M. Xu and Z. Tian, "A novel image cipher based on 3D bit matrix and latin cubes," *Inf. Sci.*, vol. 478, pp. 1–14, Apr. 2019.

[19] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A secret key cryptosystem by iterating a chaotic map," in *Advances in Cryptology*. Berlin, Germany: Springer, 1991, pp. 127–140.

[20] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, Jan. 1991.

[21] M. S. Baptista, "Cryptography with chaos," *Phys. Lett. A*, vol. 240, pp. 50–54, Mar. 1998.

[22] A. Li, A. Belazi, S. Kharbech, M. Talha, and W. Xiang, "Fourth order MCA and chaos-based image encryption scheme," *IEEE Access*, vol. 7, pp. 66395–66409, 2019.

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

[24] A. A. A. El-Latif, B. Abd-El-Atty, E. M. Abou-Nassar, and S. E. Venegas-Andraca, "Controlled alternate quantum walks based privacy preserving healthcare images in Internet of Things," *Opt. Laser Technol.*, vol. 124, Apr. 2020, Art. no. 105942.

[25] A. A. A. El-Latif, B. Abd-El-Atty, S. Elseuofi, H. S. Khalifa, A. S. Alghamdi, K. Polat, and M. Amin, "Secret images transfer in cloud system based on investigating quantum walks in steganography approaches," *Phys. A, Stat. Mech. Appl.*, vol. 541, Mar. 2020, Art. no. 123687.

[26] B. Abd-El-Atty, A. M. Iliyasu, H. Alaskar, and A. A. A. El-Latif, "A robust quasi-quantum walks-based steganography protocol for secure transmission of images on cloud-based E-healthcare platforms," *Sensors*, vol. 20, no. 11, p. 3108, May 2020.

[27] M. Kamal and M. Tariq, "Light-weight security and data provenance for multi-hop Internet of Things," *IEEE Access*, vol. 6, pp. 34439–34448, 2018.

[28] M. Kamal and M. Tariq, "Light-weight security and blockchain based provenance for advanced metering infrastructure," *IEEE Access*, vol. 7, pp. 87345–87356, 2019.

[29] G.-C. Wu and D. Baleanu, "Chaos synchronization of the discrete fractional logistic map," *Signal Process.*, vol. 102, pp. 96–99, Sep. 2014.

[30] Z. Hua, B. Zhou, and Y. Zhou, "Sine chaotification model for enhancing chaos and its hardware implementation," *IEEE Trans. Ind. Electron.*, vol. 66, no. 2, pp. 1273–1284, Feb. 2019.

[31] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Phys. D, Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, Jul. 1985.

[32] S. M. Pincus, "Approximate entropy as a measure of system complexity," *Proc. Nat. Acad. Sci. USA*, vol. 88, pp. 2297–2301, Mar. 1991.

[33] A. Ouannas, X. Wang, A.-A. Khennaoui, S. Bendoukha, V.-T. Pham, and F. Alsaadi, "Fractional form of a chaotic map without fixed points: Chaos, entropy and control," *Entropy*, vol. 20, no. 10, p. 720, Sep. 2018.

[34] K. K. L. Ho, G. B. Moody, C.-K. Peng, J. E. Mietus, M. G. Larson, D. Levy, and A. L. Goldberger, "Predicting survival in heart failure case and control subjects by use of fully automated methods for deriving nonlinear and conventional indices of heart rate dynamics," *Circulation*, vol. 96, no. 3, pp. 842–848, Aug. 1997.

[35] B. Abd-El-Atty, A. A. A. El-Latif, and S. E. Venegas-Andraca, "An encryption protocol for NEQR images based on one-particle quantum walks on a circle," *Quantum Inf. Process.*, vol. 18, no. 9, Jul. 2019, Art. no. 272.

[36] A. A. A. El-Latif, B. Abd-El-Atty, S. E. Venegas-Andraca, H. Elwahsh, M. J. Piran, A. K. Bashir, O.-Y. Song, and W. Mazurczyk, "Providing end-to-end security using quantum walks in IoT networks," *IEEE Access*, vol. 8, pp. 92687–92696, 2020.

[37] A. A. A. El-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption," *Phys. A, Stat. Mech. Appl.*, vol. 547, Jun. 2020, Art. no. 123869.

[38] A. A. A. El-Latif, B. Abd-El-Atty, M. Amin, and A. M. Iliyasu, "Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications," *Sci. Rep.*, vol. 10, no. 1, pp. 1–16, Dec. 2020.

[39] Q. Wang, Q. Guo, L. Lei, and J. Zhou, "Linear exchanging operation and random phase encoding in gyrator transform domain for double image encryption," *Optik*, vol. 124, no. 24, pp. 6707–6712, Dec. 2013.

[40] K. C. Jithin and S. Sankar, "Colour image encryption algorithm combining arnold map, DNA sequence operation, and a mandelbrot set," *J. Inf. Secur. Appl.*, vol. 50, Feb. 2020, Art. no. 102428.

[41] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. A. El-Latif, "Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption," *Inf. Sci.*, vol. 515, pp. 191–217, Apr. 2020.

[42] T. Nestor, N. De Dieu, K. Jacques, E. Yves, A. Iliyasu, and A. A. El-Latif, "A multidimensional hyperjerk oscillator: Dynamics analysis, analogue and embedded systems implementation, and its application as a cryptosystem," *Sensors*, vol. 20, no. 1, p. 83, Dec. 2019.

[43] W. Zhang, K.-W. Wong, H. Yu, and Z.-L. Zhu, "A symmetric color image encryption algorithm using the intrinsic features of bit distributions," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 3, pp. 584–600, Mar. 2013.

[44] C. Zhu, G. Wang, and K. Sun, "Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box," *Symmetry*, vol. 10, no. 9, p. 399, Sep. 2018.

[45] J. Li, "Asymmetric multiple-image encryption based on octonion fresnel transform and sine logistic modulation map," *J. Opt. Soc. Korea*, vol. 20, no. 3, pp. 341–357, Jun. 2016.

[46] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, pp. 403–419, Apr. 2019.

[47] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-box," *IEEE Access*, vol. 8, pp. 25664–25678, 2020.

[48] X. Wang, Ü. Çavuşoğlu, S. Kacar, A. Akgul, V.-T. Pham, S. Jafari, F. Alsaadi, and X. Nguyen, "S-box based image encryption application using a chaotic system without equilibrium," *Appl. Sci.*, vol. 9, no. 4, p. 781, Feb. 2019.

[49] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Trans. Nanobiosci.*, vol. 16, no. 8, pp. 850–858, Dec. 2017.

[50] X. Wang, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.

[51] X. Lv, X. Liao, and B. Yang, "A novel scheme for simultaneous image compression and encryption based on wavelet packet transform and multi-chaotic systems," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 28633–28663, Nov. 2018.