IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 21, 2020, accepted April 2, 2020, date of publication April 13, 2020, date of current version April 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2987615

A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map

TAHIR SAJJAD ALI AND RASHID ALI, (Member, IEEE)
Department of Mathematics, Faculty of Computing, Capital University of Science and Technology, Islamabad 45750, Pakistan
Corresponding author: Tahir Sajjad Ali (tahir.sajjad@cust.edu.pk)

ABSTRACT In tele-medicine, images based on patient diagnostic tests and reports are usually required to broadcast securely so that recipient can receive them without any error. For the secure communication of sensitive medical data, there is a need of authenticated and unforgeable cryptosystem. In this paper, we propose a novel signcryption technique for medical images that fulfills the necessary security requirements of sensitive medical data during its communication. The design of novel medical image signcryption scheme is empowered by the combination strategy of hybrid cryptography. It employs a technique of public key cryptography furnished with elliptic curve cryptography for the generation of secret encryption key. The proposed scheme uses elliptic curve for signcryption purpose and chaotic maps for performing encryption of the medical images. It gives a combined mechanism of key exchange, digital signature and chaotic image encryption. Image encryption phase contains permutation and diffusion for pixel scrambling. The proposed image signcryption scheme provides confidentiality, authentication, integrity, unforgability, forward secrecy and non-repudiation. The use of chaos-based symmetric image encryption scheme shows good results for key space analysis, key sensitivity, correlation analysis, number of pixel change rate, unified average changing intensity, entropy analysis and histogram analysis. On the basis of the results obtained from all these analyses, we believe that the proposed medical image signcryption scheme is efficient and robust, providing good security for sensitive medical images.

INDEX TERMS Authentication, chaotic communication, elliptic curves, image encryption, image signcryption, Henon map, logistic map, tent map.

I. INTRODUCTION

Due to the advancement in tele-medicine field the security of medical images is becoming more important. With the use of modern computer based technology, health-care system is now revolutionizing. Recent advancements in public health-care system provide an easy way to access patient's health record, treatment history, and medicine used records through cloud storage for effective health delivery. The malicious activities on cyber infrastructure are increasing day by day, therefore the security requirements of health-care sector are also rising. Medical images are dominant part of health infrastructure. In e-health system DICOM (Digital images communication in medicine) is considered as standard (ISO 12052 [37], [38]) for medical imaging. It provides the details about the bio-medical structure of organ, being examined. Many advanced tools are invented for the diagnostic purpose of pre-medical analysis and examination using DICOM system. These tools are based on imaging technology using signal processing to get the vision of internal body systems. Nowadays surgical operations are guided by sensors and artificial intelligence. These real time information systems collaborate in real time surgical operations. As medical data is mostly occurred in image format, therefore a rigorous security approach is required to secure it. In e-health care system, there are serious threats to data containing secret information of a patient's health reports. During the management and transmission of health-care data to third parties like private/public or hybrid clouds, there may occur many problems about the safety and security of this data. Thus we need an efficient and robust approach to provide secure transmission of sensitive medical data along-with its authentication over public networks.

Encryption and authentication are two essential primitives of cryptography. These are vastly used for maintaining privacy of communication. Authenticated encryption simultaneously offers encryption along with data authenticity and confidentiality of secret data. For this purpose authenticated

The associate editor coordinating the review of this manuscript and approving it for publication was Walid Al-Hussaibi.

encryption combines symmetric encryption scheme and message authentication code (MAC). Other methods used for protection and authentication are; sign-then-encrypt, encrypt-then-sign, sign and encrypt and authenticated encryption with associated data (AEAD). But these cryptographic protocols take extra computational efforts. In 1997, Zheng [68] combined these primitives in a single operation and named it ''signcryption''. It takes less computational cost and effort. Signcryption provides confidentiality, integrity, authentication of information and non-repudiation. Therefore it is used in many applications like electronic transaction protocols, key management, routing protocols etc. It also plays an important role in cloud computing and internet of things.

Deng and Bao [15] proposed a signcryption scheme that decreases computational cost to 16% and commuicational cost to 85% in comparison with signature then encryption scheme. But their proposed scheme is less efficient than that of Zheng [68]. Mahmood and Dony [31] have proposed an enhanced segmentation based medical image encryption scheme. In this scheme medical images are divided into two segments, region of interest (ROI) and region of background (ROB). It uses AES and Gold code (GC) algorithm to reduce computational time and also to provide hybrid design of encryption. Wong [57] proposed the idea of a digital trust center in 1996. It provides confidentiality and authenticity of digital images in hospitals.

Many conventional approaches like AES, RSA etc, are not suitable to protect sensitive records in DICOM system due to large storage requirements and long computational time. In 2012 Mohamed *et al.* [35] proposed chaos based image encryption scheme and compared the simulation results with AES against NPCR, UACI, correlation among the pixels in cipher image, histogram analysis and encryption time. On the basis of the above security tests it was concluded that for digital multimedia data, the traditionally used cryptographic schemes are less suitable. Recently in 2017 Chen and Hu [10] used multiple chaotic mappings for adaptive medical image encryption. A digital image is a two dimensional sequence that has a large size in comparison to the text file. Therefore the traditional encryption algorithms like AES, DES and RSA suffer from the shortfalls like long encryption time and huge computational power [11], [40].

In 2013 Eldayem and Mohamed [17] proposed encryption strategy for the encryption of DICOM images. They used watermarking technique and MD5 hash function for integrity of images. Their proposed scheme provides patient authentication, image integrity and patient information confidentiality. Bhopi *et al.* [7] in 2016 proposed a method for the security of medical images. In this proposed work, medical image encryption (MIE) is taken in two stages. In the first stage rotation is performed row-wise, column-wise and diagonally using binary keys. In the second phase four chaotic logistic maps are used to generate pseudo random sequences. Pixel value permutation is performed with these generated sequences. Cao *et al.* [9] proposed a method of medical image encryption using edge maps. Their proposed method consists of bit plane decomposition, chaotic sequence generation and scrambling technique.

Singh and Singh [47] used elliptic curve cryptography for encryption, decryption and digital signature of cipher image to give the authenticity and integrity. Shukla *et al.* [46] proposed an image encryption scheme that uses elliptic curves ECC with smaller key size. It reduces storing and transmission requirements. Their proposed scheme used Elgamel elliptic curve encryption. This scheme also provides confidentiality, authentication and integrity. Many other methods based on chaos theory [4], [63], [64] using one time key [27], bit level permutation [28], DNA sequence operation [51], dynamic random growth technique [52] and perceptron model [50] are also proposed for the encryption of multi-media images. There are some non chaos based methods for image encryption that use compressive sensing [41], non adjacent coupled mapped lattices [66], [67], parallel computing system [53], synchronously updating Boolean networks based on matrix semi-tensor product theory [54] and JPEG compression algorithm [1]. All these methods do not provide information about the key distribution or the authentication, non repudiation, integrity, unforgeability, forward secracy etc. Currently Zia and Ali improved an elliptic curve based signcryption scheme for firewalls [70] and established the enhancement of a blind signcryption scheme based on elliptic curves [71] in 2019.

Recently it is observed that hackers and unauthorized parties steal medical records on a large scale and sell them to the dealers on dark web [39], [44]. This sensitive data then misused in identity theft and fraudulent activities. The medical history of United States (US) for past 10 years shows that almost 3000 breaches are occurred, each of them containing more than 500 sensitive medical records caused by hacking [14], [48]. For example a damage of $115 million as settlement is reported [25] due to a breach of 78 million American's customers medical data of Anthem (medical insurance company). A U.S. government task force released a report [19] in 2017 about the cybersecurity performance in health care sector. It shows a critical situation and a number of vulnerabilities in computer, networks and medical devices [36] used in health care sector. In [34] it is reported that there are two major vulnerabilities in the DICOM imaging standard in March, April 2019. Thus it is exposed that DICOM standard have major cybersecurity holes.

Contributions: Our research contributions aim to provide solution of many problems faced by e-healthcare system [16]. To achieve the objective, we design a novel medical image signcryption scheme empowered by the combination strategy of hybrid cryptography. It employs a technique of public key cryptography furnished with elliptic curve cryptography for the generation of secret encryption key. Then chaos-based symmetric, medical image encryption is performed by using that generated secret key. The combination of elliptic curve cryptography together with chaotic maps provides the effective protection measures for secure transmission of sensitive medical images on public networks with their

authentication. In this work the proposed signcryption scheme provides confidentiality, unforgeability, integrity, non-repudiation and forward secrecy of authenticated health-care transmission system. The proposed signcryption approach not only essentially yields security requirements but also detects efforts/attacks by adversaries.

Paper organization: The rest of the article is organized as follows: in Section 2 preliminary material on elliptic curve, logistic and tent chaotic maps are described. In Section 3, we first describe the tent-logistic-tent chaotic map and then propose a new image signcryption scheme. Results and discussion with the help of examples and figures, the security analysis of the scheme and comparison with other schemes are discussed in Section 4. Finally the work is concluded in Section 5.

II. PRELIMINARIES

A. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) is an example of public key cryptography. It was developed by Koblitz [26] and Miller [33] independently in 1985. Then Washington [55] provided proof of various theories related to elliptic curves. It has gained a wide acceptance around 2004. ECC gives an efficient and secure public key cryptography implementation with relatively smaller key size than RSA.

Elliptic curves are a type of algebraic curves. ECC brainpool [8] and NIST (National Institute of Standard and Technology) [60] has provided many recommended ECC parameters of various bit sizes. In this paper we are using elliptic curves for the generation of symmetric key. An elliptic curve $E(\mathbb{F}_p)$ over a finite field $\mathbb{F}_p$ is defined as the set of all points (x, y) satisfying the following equation,

$$y^2 = x^3 + ax + b \mod p, \tag{1}$$

where the parameters $a, b \in \mathbb{F}_p$ follow the relation

$$4a^3 + 27b^2 \neq 0.$$

There is a point O at infinity taken as identity element under addition. A point $R = (x,\ y)$ is said to be a point on elliptic curve $E(a, b)$ if it satisfies equation (1). Another point $R' = (x,\ -y)$. is the negative of R that is

$$R = -R'.$$

Let $R_1 = (x_1,\ y_1)$ and $R_2 = (x_2,\ y_2)$ be two distinct elliptic curve points, that satisfy the equation (1), then their addition is defined as: a line joining these point and its intersection with a line in same elliptic curve. The resulting point of addition $R'_3 = (x_3,\ y_3)$ (the negative of R_3) can be obtained by performing the following calculations as shown in (2):

$$\begin{cases} x_3 = \lambda - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3 - y_1), \end{cases} \tag{2}$$

where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$. An elliptic curve point can be added to itself by using the point doubling technique. Let R^* be a point on the elliptic curve, then the point doubling can be defined as, a tangent line of the point R^* and its intersection with another line on that elliptic curve. The result of point doubling is a point $R'_1 = (x'_3,\ y'_3)$. The point R'_1 can be obtained by following the relation (3) as shown below:

$$\begin{cases} x'_3 = \lambda - 2x_1 \\ y'_3 = \lambda(x_1 - x'_3 - y_1), \end{cases} \tag{3}$$

where $\lambda = \dfrac{3x_1^2 - a}{2y_1}$. Also there exists a base point G of elliptic curve E over finite field $\mathbb{F}$ with a prime order n that is

$$nG = O.$$

Elliptic curve $E(a, b)$ points along with a point O at infinity form a cyclic addition group. The equation of elliptic curve has the similarity with one used for calculating circumference of ellipse. Therefore these are called elliptic curves.

Elliptic curves provide hard problems like elliptic curve discrete log problem (ECDLP), elliptic curve Diffie-Hellman problem (ECDHP) etc to use for cryptographic purposes. For given two points S and S^* of an elliptic curve E, where $S = bS^*,\ (b < n)$. The (ECDLP) is that, it is computationally infeasible to find the integer b. The (ECDHP) is defined as: for given two elliptic curve points U and U^*, where $U = c_1G$, $U^* = c_2G$ and $(c_1, c_2 < n)$, it is computationally infeasible to get the another point $V = c_1c_2G$. For further details on ECC see [12].

B. CHAOTIC MAPS

Chaotic maps [29] are used to produce non linear, complex, random sequences. Output of such maps is highly sensitive to initial conditions and control parameters. These parameters can be treated as secret keys when we use chaotic maps in cryptography. Due to this phenomenon of chaotic maps, it looks natural to use such type of structures in modern cryptography.

1) TENT MAP

Tent map [13] is the simplest chaotic iterative map. It is one dimensional map and also known as triangle map defined as,

$$x_{n+1} = \begin{cases} rx_n & \text{if } 0 \leq x_n \leq 0.5 \\ r(1 - x_n) & \text{if } 0.5 < x_n < 1 \end{cases} \tag{4}$$

Here $x_0 \in (0, 1)$ is the state variable and $r \in (0, 2)$ is the control parameter. Although the chaotic map (4) is simple having linear equations but for certain parameter values, it shows highly complex and even chaotic behavior.

2) LOGISTIC MAP

Logistic map [32] is a type of chaotic system. It is one dimensional, discrete time and non-linear map with quadratic non-linearity. The state equation of logistic map with initial state w_n is given by

$$w_{n+1} = f(w_n) = \mu w_n(1 - w_n), \quad n = 0, 1, 2, \ldots \tag{5}$$

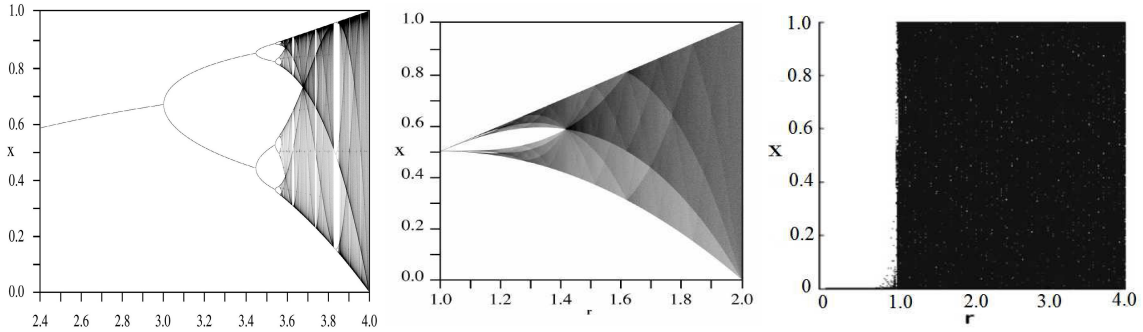

FIGURE 1. Bifurcation diagrams of (a) chaotic logistic map, (b) chaotic tent map and (c) tent-logistic-tent map.

where $w_n \in (0, 1)$ is the state of the system at any time n and $\mu \in (0, 4)$ is the control parameter also known as bifurcation parameter. Term w_{n+1} expresses the next state and n shows the discrete time. For the values of μ between 3.567 and 4 the logistic map (5) behaves chaotically with infinite period. Lyapunov exponent is the measure of sensitive dependence on initial condition. For $\mu = 3.57$ to 4 the value of lyapunov exponent is mostly positive, which shows that in this interval logistic map exhibits chaotic behavior.

3) HENON MAP

Henon map [23] is two dimensional discrete time non-linear chaotic map. It was proposed by Henon in 1976. The two dimensional invertible Henon map is defined as,

$$\begin{aligned} x_{n+1} &= 1 - ax^2(n) + y(n), \\ y_{n+1} &= b\,x(n), \end{aligned} \tag{6}$$

where a and b are the control parameters of chaotic map (6). For $a \in (0.54, 2)$, and $b \in (0, 1)$, it shows chaotic behavior.

III. PROPOSED IMAGE SIGNCRYPTION SCHEME

In this section. first we introduce tent logistic tent map, then we use it in our proposed signcryption scheme for chaos-based image encryption.

A. TENT LOGISTIC TENT MAP

From the combination of tent and logistic chaotic maps, recently in [2] a new chaotic system namely the tent logistic tent map is introduced. In this system '+' and '×' are floating point addition and multiplication respectively. The exponentiation r^{σ} is a multiplier that is employed for better distribution of state variables. The proposed system has more complex and chaotic characteristics than individual chaotic maps. This chaotic system is defined as,

$$x_{n+1} = \begin{cases} \left(\frac{r^2}{2}x_n\left(1 - \frac{r}{2}x_n\right) + \frac{r}{2}x_n\right) r^{14} \bmod 1 & \text{if } 0 < x_n < 0.5 \\ \left(\frac{r^2}{2}(1-x_n)\left(1 - \frac{r}{2}(1-x_n)\right) + \frac{r}{2}(1-x_n)\right) r^{14} \bmod 1 & \text{if } 0.5 \le x_n < 1 \end{cases} \tag{7}$$

Here $r \in (0, 4)$ is the control parameter and $x_0 \in (0, 1)$ is the state variable. Here r^{14} is selected experimentally to generate a balance between optimal chaotic behavior and speed of system.

Tent and logistic chaotic maps have limited chaotic ranges as shown in FIGURE 1. Therefore, when we use their control parameters as secret keys they provide limited key space. Also it is known that they have periodic windows hence these are inclined towards parameter estimation attacks. To overcome the weaknesses of tent and logistic maps, they are combined to generate a new stronger chaotic system [2]. In this system logistic chaotic map plays main role while tent map plays the role of seed map. Hence generated chaotic system is called tent logistic tent system (TLTS). The proposed chaotic system shows chaotic behavior without window of periodicity in $r \in (1.05, 4)$ as presented in FIGURE 2. The lypunouv exponent of this new system is also greater than tent and logistic maps. Hence it shows better results when used for cryptographic purposes.

In the proposed medical image signcryption scheme, the patient/user uses the public key of health-care authority to generate common secret encryption key 'K'. Then he takes encryption with the proposed chaos-based medical image encryption scheme using the secret key 'K'. He signs the cipher image and sends cipher image C, digital signature s and authentication parameter G' to the authority. FIGURE 3 shows the proposed signcryption model, while FIGURE 4 and FIGURE 5 are the block diagrams of the proposed signcryption and unsigncryption schemes.

Health-care authority uses C, s and his private key s_b to generate the common secret key 'K'. Then the authority takes symmetric decryption using that key to find the image, verifies it by using G' and accept, if it is authenticated.

B. GLOBAL PARAMETERS

In this phase following parameters are selected and published:
q: A large prime number, where $q > 2^{256}$.
$E(a, b)$: The used elliptic curve over finite field $\mathbb{F}_q$,

$$y^2 = x^3 + ax + b \bmod q.$$

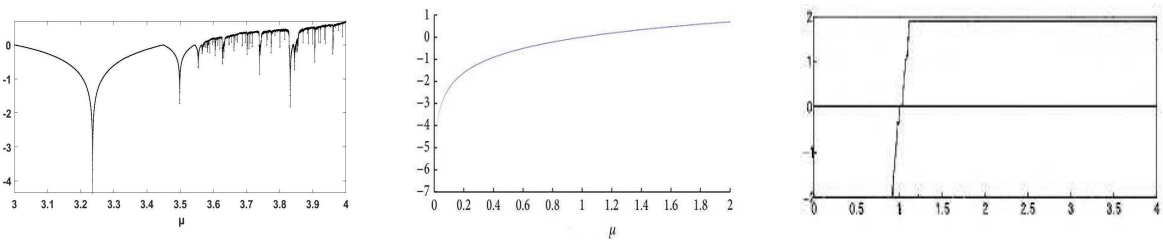

FIGURE 2. Lyapunov exponents of (a) chaotic logistic map, (b) chaotic tent map and (c) tent-logistic-tent map.

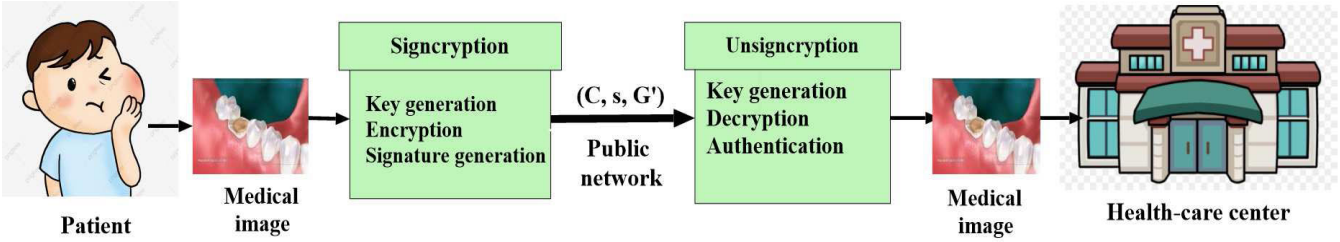

FIGURE 3. Proposed signcryption model.

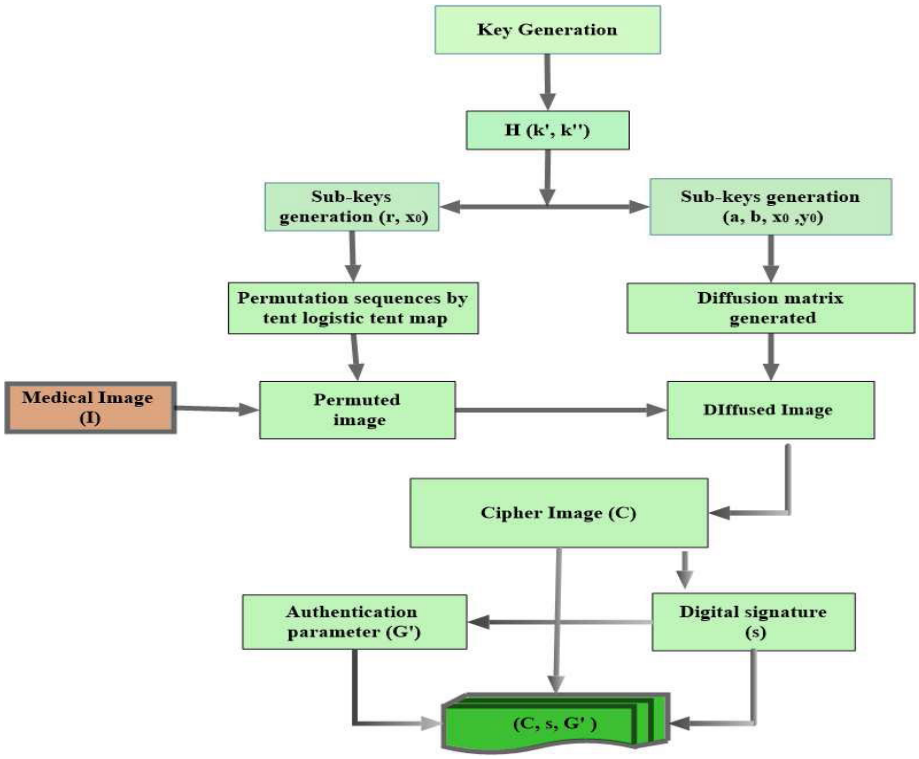

FIGURE 4. Block diagram of the proposed medical image signcryption scheme.

Here a and b are two integers that are smaller than q and satisfy $4a^3 + 27b^2 \neq 0 \bmod q$.

G: The base point of elliptic curve $E(a, b)$ with order n.

O: The point of $E(a, b)$ at infinity.

n: The order of G, i. e., $nG = O$.

H: A one-way hash function.

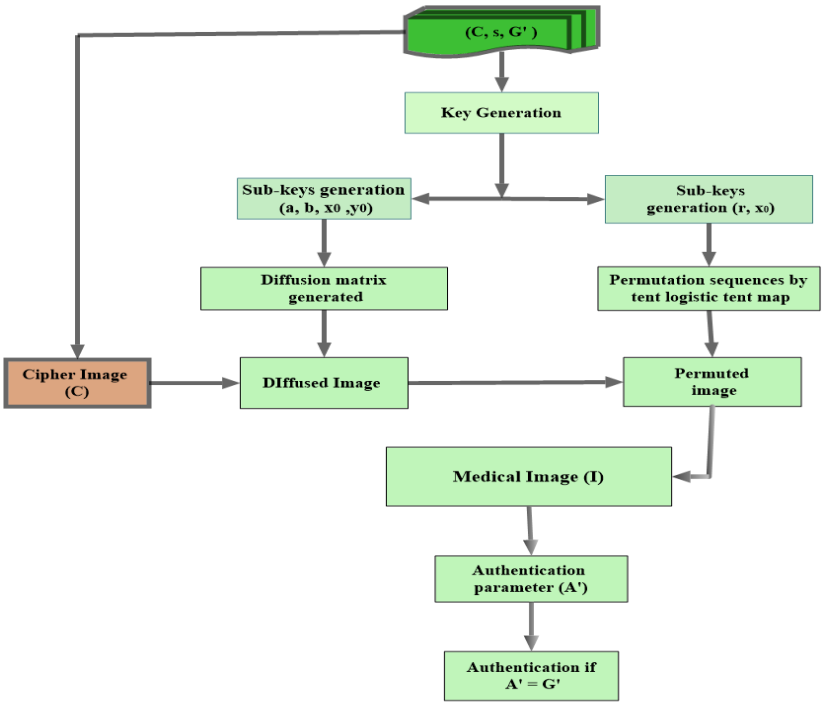

FIGURE 5. Block diagram of the proposed medical image unsigncryption scheme.

C. KEY GENERATION

Patient selects a random integer $s_a < n$ as his/her private key and computes public key $P_a = s_aG$. Similarly health-care authority chooses a random integer $s_b < n$ as his/her private key and computes public key $P_b = s_bG$. These public keys will be used at both the sender and the receiver ends to generate a common secret key K.

D. SIGNCRYPTION PHASE

For sending a medical image to health-care authority, the patient uses symmetric chaos-based image encryption scheme to generate cipher image. To signcrypt the medical image, following steps will be performed:

1) Select a random integer $k \in \mathbb{F}_q$, multiply it with health-care authority's public key P_b to generate the secret key as,

$$K = kP_b = (k', k'').$$

2) Apply the hash function H (using SHA-256) on the components of secret key $K = (k', k'')$, as:

$$H(k') = b'_{255},\ b'_{254},\ \ldots, b'_1,\ b'_0,$$
$$H(k'') = b''_{255},\ b''_{254},\ \ldots, b''_1,\ b''_0,$$

where $b'_i,\ b''_i \in [0, 1]$ for $i \in 0, 1, \ldots, 255$ are used to get the parameters of the chaotic maps (6) and (7) as stated below:

a) Compute the parameters $r \in (0, 4)$ and $x_0 \in (0, 1)$ of the chaotic map (7) from the two halves of 256-bits of $H(k')$ as follows:

$$r = (b'_{255} \times 2^1 + b'_{254} \times 2^0).$$
$$(b'_{253} \times 2^{125} + \ldots + b'_{128} \times 2^0),$$

similarly compute $x_0 \in (0, 1)$ as:

$$x_0 = 0.(b'_{127} \times 2^{128} + b'_{126} \times 2^{127} + \ldots + b'_0 \times 2^0).$$

b) Generate the initial values, control parameters of Henon chaotic map (6) and the subkeys $M_0,\ N_0$ (for encryption of the first pixel and the last pixel of pre-encrypted image D respectively). Use the output of $H(k'')$ to get the values of $a \in (0.54, 2),\ b,\ x'_0,\ y_0 \in (0, 1)$ and $M_0,\ N_0 \in [0, 255]$ as follows:

$$a' = (b''_{239} \times 2^1 + b''_{238} \times 2^0).$$
$$(b''_{237} \times 2^{45} + \cdots + b''_{192} \times 2^0),$$
$$a = \begin{cases} 2 - a' & \text{if} \quad 0 \le a' < 0.54 \\ a' & \text{if} \quad 0.54 \le a' < 2 \end{cases}$$
$$b = 0.\ (b''_{191} \times 2^{47} + b''_{126} \times 2^{46} + \ldots + b''_{144} \times 2^0),$$
$$x'_0 = 0.(b''_{143} \times 2^{47} + b''_{142} \times 2^{46} + \cdots + b''_{96} \times 2^0),$$
$$y_0 = 0.\ (b''_{95} \times 2^{47} + b''_{94} \times 2^{46} + \cdots + b''_{48} \times 2^0),$$
$$M_0 = b''_{47} \times 2^7 + b''_{46} \times 2^6 + \ldots + b''_{40} \times 2^0.$$
$$N_0 = b''_{39} \times 2^7 + b''_{38} \times 2^6 + \ldots + b''_{31} \times 2^0.$$

Encryption process

3) Convert the image I in digital form as the matrix D' of order $M \times N$, where M and N are the dimensions of the image.

4) Rewrite the matrix D' as one dimensional array,

$$Z = \{z_1, z_2, \ldots, z_{MN}\}.$$

Permutation:

5) Iterate the chaotic map (7) using the parameters from Step 2 (a) to obtain the sequence:

$$A = \{a_i\}_{i=1}^{MN},$$

and sort sequence A in ascending order to form,

$$B = \{b_i\}_{i=1}^{MN}.$$

6) Using the relationship of the sequences A and B,

$$b_i = a_{t_i}, \quad \text{for } i = 1, \ldots, MN,$$

compute permutation vector,

$$T = \{t_1, t_2, \ldots, t_{MN}\}.$$

7) Use T to permute the position of elements of the array Z. After applying permutation on Z it becomes,

$$D = \{g_1, g_2, g_3, \ldots, g_{MN}\},$$

convert D into two dimensional array of order $M \times N$.

8) Use parameters generated from $H(k'')$ in Step 2(b) for Henon chaotic map (6) to generate two random sequences,

$$X = \{x_k\}_{k=1}^{MN} \quad \text{and } Y = \{y_k\}_{k=1}^{MN}$$

9) Convert the real number sequences x_k and y_k where $k = 1, 2, \ldots, MN$ into integer sequences using these relations:

$$x_k = \text{int}(254 \times (x_k - \min(x_k))/d) + 1,$$

where $d = \max(x_k) - \min(x_k)$.

$$y_k = \text{int}(254 \times (y_k - \min(y_k))/d) + 1,$$

where $d = \max(y_k) - \min(y_k)$.

10) Express $\{x_k\}$ and $\{y_k\}$ as two dimensional arrays of order MN, and mix them with two dimensional permuted image D (obtained from Step 7) as follows to get encrypted image C:

```
for r=1:M do
    for c=1:N do
        if r=1,c=1 then
            C'(r,c) ← D(r,c) ⊕ X(r,c) ⊕ M_o
        else
            if r ≥ 2 and c = 1 then
                C'(r,c) ← X(r,c) ⊕ C'(r−1,N) ⊕ D(r,c);
            else
                C'(r,c) ← X(r,c) ⊕ C'(r,c−1) ⊕ D(r,c);
            end
        end
    end
end
```

```
for c=N, N−−,c=1 do
    for r=M, M−−, r=1 do
        if r=M,c=N then
            C(r,c) ← C'(r,c) ⊕ Y(r,c) ⊕ N_o
        else
            if r = M and c < N then
                C(r,c) ← C'(r,c) ⊕ C(r,c+1) ⊕ Y(r,c);
            else
                C(r,c) ← C'(r,c) ⊕ C(r+1,c) ⊕ Y(r,c);
            end
        end
    end
end
```

Signature generation:

11) Compute h by applying hash function H on I, C and K. That is:

$$h = H(I, C, K).$$

12) Also find digital signature s as:

$$s = \frac{k}{h + s_a} \bmod q.$$

13) Calculate authentication parameter G' as:

$$G' = hG.$$

14) Send (C, s, G') to the health-care authority.

E. UNSIGNCRYPTION PHASE

The health-care authority receives cipher image C, digital signature s and verification parameter G'. Then it uses the following steps to get plain image I with its authentication.

1) Solve;

$$s_b\ s\ G' + s_b\ s\ P_a = K.$$

to generate the secret key K.

2) Use hash function H to get sub-keys as described in Step (2) of above signcryption phase.

Decryption method:

3) Generate $\{x_k\}$ and $\{y_k\}$ two dimensional arrays of order $M \times N$ by following the Step (8) and Step (9) of above used signcryption phase.

4) To eliminate diffusion effects, apply Step (10) of the above mentioned scheme, by replacing G with C to obtain permuted array G.

5) Perform Step (5, 6) of the signcryption phase to get permutation vector T, also calculate inverse permutation vector i.e., T^{-1}.

6) Apply T^{-1} on D to get original medical image I.

7) Take the hash value of plain image I, cipher image C and secret key K to find h as:

$$h = \text{H}(I, C, K).$$

8) Calculate another authentication parameter A' as:

$$A' = hG.$$

TABLE 1. Summary of proposed image signcryption scheme.

Signcryption	Unsigncryption
1. Select a random integer $k \in \mathbb{F}_q$ and compute $K = kP_b = (k', k'')$.	1. Receive (C, s, G') from the sender.
2. Encrypt the medical image I to obtain the cipher image C as: $C = \mathrm{E}_{H(K)}(I)$.	2. Use s, G' to compute the shared key K, $K = s_b s G' + s_b s P_a$.
3. Use the hash function H to generate the signature s as: $s = \frac{k}{h + s_a} \bmod q$, where $h = H(I, C, K)$.	3. Decrypt the cipher image C to get the medical image I as: $I = \mathrm{D}_{H(K)}(C)$.
4. From the above values of h compute also $G' = hG$.	4. Use the hash function H to compute, $h = H(I, C, K)$ and calculate $A' = hG$.
5. Send (C, s, G') to authority.	5. Accept the medical image if $A' = G'$.

Authentication:

9) The received image is accepted, if the calculated value of A' and received G' are same *i.e.*,

$$A' = G'.$$

The above signcryption and unsigncryption scheme is summarized in TABLE 1.

F. CORRECTNESS

The health-care authority receives $(C,\ s,\ G')$ from patient. It calculates key by using its private key s_b, patient's public key P_a, received digital signature s and authentication parameter G'.

$$\begin{aligned} & s_b s\, G' + s_b\, s\, P_a \\ &= s_b \frac{k}{h + s_a}\, h\, G + s_b \frac{k}{h + s_a} s_a\, G \\ &= \frac{s_b\, k\, h\, G}{h + s_a} + \frac{s_b\, k\, G\, s_a}{h + s_a} \\ &= \frac{(s_b\, k\, G)(h + s_a)}{h + s_a} \\ &= (s_b\, k\, G) \\ &= k\, P_b = K \end{aligned}$$

IV. RESULTS AND DISCUSSIONS

For the performance evaluation of the proposed medical image signcryption scheme, test images are selected from open-access medical image repositories/Ayland.org [49] image database. The proposed scheme is then implemented on MATLAB R2016b, 64-bit and applied on medical data. The proposed method can be used for different types/sizes of medical images. Medical images along with their encryption results are shown in FIGURE 6.

In this section, firstly we discuss the security features of chaos-based encryption, then signcryption attributes and possible attacks will be discussed.

A. SECURITY FEATURES OF CHAOS-BASED ENCRYPTION

In the proposed scheme a novel chaos-based encryption mechanism is adopted for secure transmission of medical image. FIGURE 6 shows the encryption results of various medical images. Performance evaluation tests like key space, key sensitivity, ability of resisting against differential attacks, histogram analysis, correlation analysis and information entropy are also employed in this section.

1) KEY SPACE ANALYSIS

Key space is considered as an important feature in any cryptosystem. It should be large enough to produce the ability to resist against brute force attacks. In the proposed encryption model, we have used two chaotic maps. For tent-logistic-tent map (7) control parameter r and initial state x_0 are used. Another chaotic map used in proposed encryption scheme is Henon map (6). It uses a and b as control parameters and two state variables x_0' and y_0. M_0 is the key used for encryption of first pixel. According to IEEE floating format precision [56] each key component should be greater than 10^{-15}. If the precision of these parameters is taken as 10^{-15}, the key space size will be $(10^{15})^6 = 10^{90} \approx 2^{299}$. Alvarez and Li [5] identified that the adequate key space for image encryption scheme should be larger than 2^{100} to oppose brute force attacks. The key space of our proposed scheme is large enough to resist against brute force attack. In order to decrypt the medical image correctly, the adversary has to guess all these six components.

2) KEY SENSITIVITY ANALYSIS

An image encryption scheme should be highly sensitive and conscious for its secret keys and a change of single-bit in any of its secret keys should crop an entirely different encrypted result [3]. Hence generated cipher image can not be decrypted by a changed key to give required results. Note that in our proposed scheme, we have used tent logistic tent map (7) with key components $a = 1.4$, $b = 0.3$, $x_0' = 0.7666$ and $y_0 = 0.3$ and Henon map (6) with $r = 3.78$ and $x_0 = 0.5748$. These maps are highly sensitive for initial conditions and control parameters as seen by their lyapunov exponent in FIGURE 2. For testing the key sensitivity, we take four medical images used in FIGURE 6 of size 256×256 as a test case, and modify only one key component i. e. x_0' from 0.7666 to 0.7666000000000001. FIGURE 7 shows the experimental results of key sensitivity for encryption process using slightly changed key. From here it can be seen that the encryption results are totally different. Similar results can be seen by making a small change in any other component of used secret key. Hence the obtained results show that the proposed scheme is highly sensitive to secret keys.

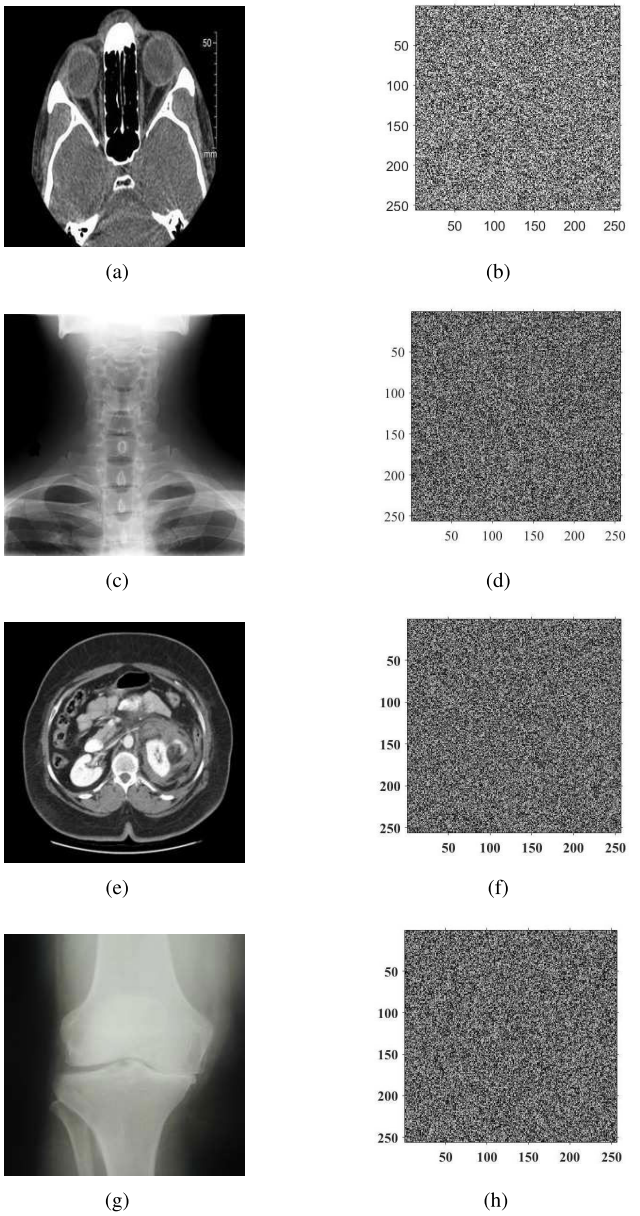

FIGURE 6. (a, b) CT Paranasal and its cipher image, (c, d) Pair of Cervical X-Ray image with the corresponding cipher image, (e, f) CT Abdomem image with the corresponding cipher image, (g, h) Knee X-Ray image with its corresponding cipher image.

3) STATISTICAL RANDOMNESS ANALYSIS

Encrypted image generated by any cryptographic encryption scheme, should be invulnerable to statistical attacks. The presence of randomness is essential not only for pseudo random number generators (PRNGs) [20] but also for the encrypted data [61]. Therefore the randomness is evaluated in the resulting encrypted data by using National Institute of Standard and Technology (NIST) statistical random test suite [65]. With the suggested parameters for input sequence, the p-value is expected to be greater than 0.01 to qualify for the randomness in the bit stream of encrypted data.

The results of NIST randomness tests [65] for CT Paranasal image are shown in TABLE 2.

4) CORRELATION ANALYSIS

The property of having high confusion and diffusion can be checked by a test of correlation among neighboring pixels in the plain image and their corresponding cipher image. For the calculation of correlation coefficients in horizontal, vertical and diagonal directions, the following relation [42] has been used,

$$C_r = \frac{(n\sum_{t=1}^{n} x_t y_t - \sum_{t=1}^{n} x_t \sum_{t=1}^{n} y_t)}{\sqrt{(n\sum_{t=1}^{n}(x_t)^2 - (\sum_{t=1}^{n} x_t)^2)((n\sum_{t=1}^{n}(y_t)^2 - (\sum_{t=1}^{n} y_t)^2)}}. \quad (8)$$

Here x_t and y_t are values of neighboring pixels in the image and n is the total number of pixels taken for calculation of correlation in equation (8). We have also analyzed correlation in the adjacent pixels of the plain images and cipher image in FIGURE (9, 10) respectively. From the results of TABLE 3 and FIGURE (9, 10), it is seen that cipher image has very low correlation among neighboring pixels. Hence cipher images are revealing no information about the structure of plain image.

5) HISTOGRAM ANALYSIS

Image histogram displays the dispersion of pixels in an image [43]. The uniform dispersion can be observed by analyzing the shape of histogram, generated by plotting the pixels of image. The histograms of the original images are shown in FIGURE 11 and their corresponding encrypted image components are shown in FIGURE 12. From histogram analysis it is clear that, there does not exist any clue to mount a statistical attack on the encrypted image.

However the histogram visual effects are not sufficient to validate the randomness of pixel value in cipher image [59], [66]. Therefore the histogram is also evaluated quantitatively by using chi-square (χ^2) test. Chi-square (9) can be defined as:

$$\chi^2_{\text{exp}} = \sum_{i=1}^{S} \frac{(o_i - e_i)^2}{e_i}, \quad (9)$$

$$e_i = \frac{\text{M} \times \text{N}}{S} \quad (10)$$

where S indicates grayscale ($S = 256$ in this case), o_i is the frequency of occurrence of each level observed on the histogram of cipher image, e_i is the expected uniform distribution frequency of occurrence and M × N shows total length of image sequence in (10).

The experimental chi-square value should be less than the theoretical value (293 with significance level 0.05) for an ideal image encryption system. TABLE 4 indicates the output of chi-square test and pass rate. The chi-square test is passed by all the test images. It is therefore clear that the redundancy of plain image is fully concealed, which demonstrates the inability of stability of statistical attacks.

6) ENTROPY ANALYSIS

This feature of analysis measures the randomness in a cipher image. It also tells us the average amount of information

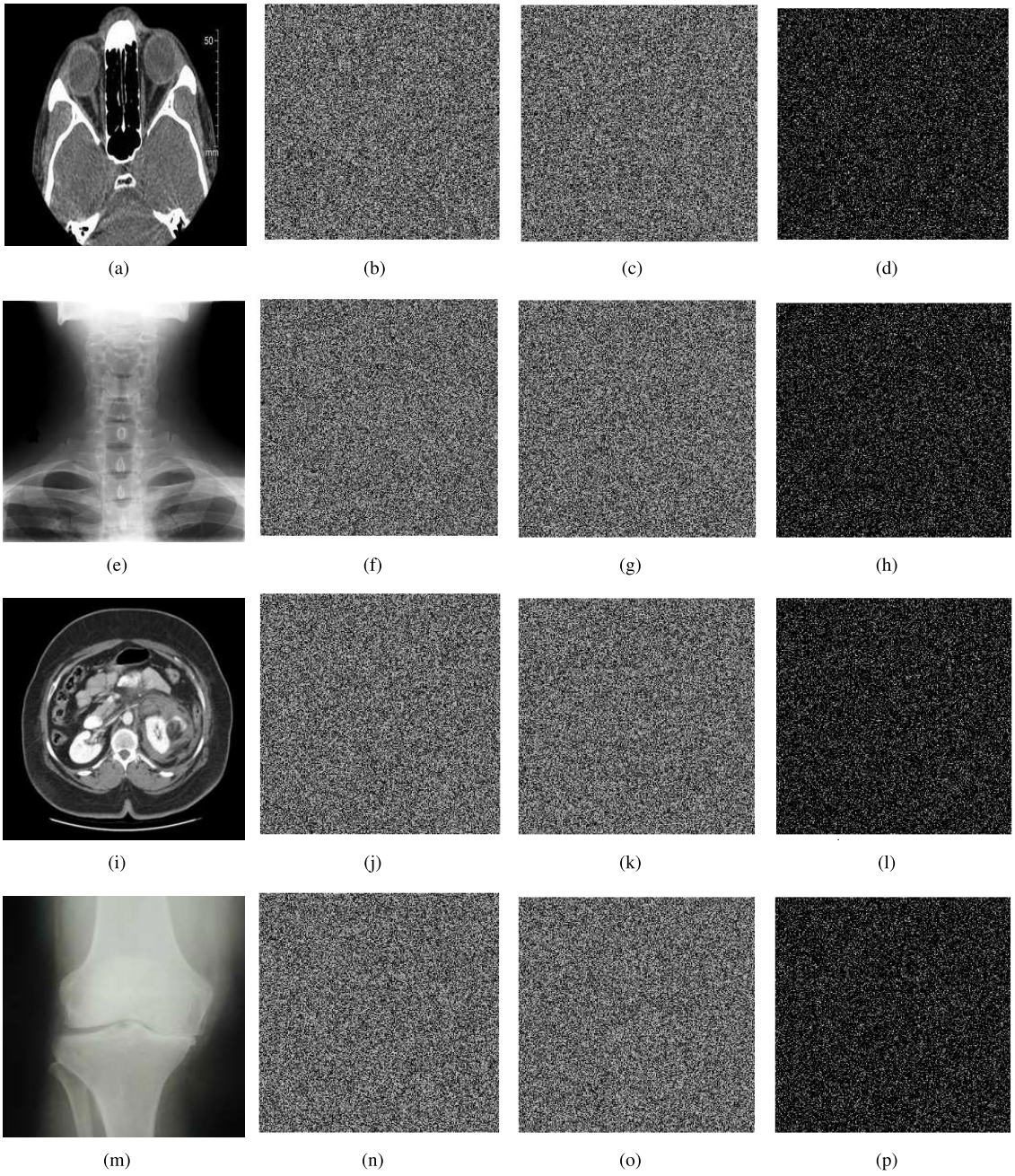

FIGURE 7. Experimental encryption results with a small change in secret key component, (a, e, i, m) original images, (b, f, j, n) cipher images I_c, (c, g, k, o) encrypted images by slightly changed key I'_c, (d, h, l, p) absolute intensity difference images $|I_c - I'_c|$.

carried by cipher image. Let g be a cipher image then entropy value of g can be calculated by the formula [45]:

$$E(g) = \sum_{i=o}^{2^N-1} P(g_i) log_2 \frac{1}{P(g_i)} \tag{11}$$

Here in equation (11) $P(g_i)$ shows the probability of appearing of symbol g_i in cipher image g. For exact random source having 256 different symbols, the ideal value of entropy $E(g)$ is 8. If the calculated value of entropy is significantly less than the ideal value of entropy in cipher image then it means that there is a possibility of predictability of plain image. In this scheme entropy values for cipher image g, is checked. The calculated values of entropy for the plain images and their corresponding cipher images are shown in TABLE 5. In our example of proposed scheme, the entropy value of cipher images with 2^N as 255, using Matlab R2016b, turn out to be $\approx$ 8. Hence it is assumed that proposed scheme is robust having minimum information dissipation.

7) LOCAL SHANON ENTROPY

The randomness of a cipher image is usually measured with information entropy. Higher entropy values generally indicates a stronger encryption result. The values obtained from

TABLE 2. Statistical randomness tests results.

Test #	Test name	P. value	Result
1	Frequency (monobit)	0.6017	Success
2	Block Frequency ($m = 128$)	0.6879	Success
3	Cumulative Sums (Forward)	0.7166	Success
4	Cumulative Sums (Reverse)	0.8596	Success
5	The Run Test	0.4217	Success
6	Longest Run of Ones	0.4581	Success
7	Rank	0.0167	Success
8	DFT Spectral	0.6537	Success
9	Non Overlapping Template ($m = 9, B = 000000001$)	0.4520	Success
10	Overlapping Template ($m = 9$)	0.6315	Success
11	Universal Statistical Test	0.4371	Success
12	Approximate Entropy ($m = 10$)	0.5184	Success
13	Random Excursions	0.1463	Success
14	Random Excursions Variant	0.1526	Success
15	Serial ($m = 16$)	0.2621	Success
16	Linear Complexity ($M = 500$)	0.4136	Success

TABLE 3. Correlation coefficient of two neighboring pixels in Plain and Cipher image.

FIGURE 6	CT Paranasal		Cervical X-Ray		CT Abdomen		Knee X-Ray	
Direction	Orig.	Ciph.	Orig.	Ciph.	Orig.	Ciph.	Orig.	Ciph.
Horizontal	0.9776	0.0032	0.9960	-0.0019	0.9580	-0.0002	0.9994	-0.0016
Vertical	0.9432	0.0223	0.9979	0.0132	0.9710	0.0176	0.9989	0.0239
Diagonal	0.9310	0.0029	0.9942	-0.0042	0.9311	-0.0071	0.9986	0.0001

TABLE 4. Results of chi-square test for cipher image.

FIGURE 6	Image type	Image size	Chi-square test scores		Results
			Theoretical value	Proposed scheme	
CT Paranasal	Gray	256×256	293	257	Pass
Cervical X-Ray	Gray	256×256	293	268	Pass
CT Abdomen	Gray	256×256	293	214	Pass
Knee X-Ray	Gray	256×256	293	244	Pass

TABLE 5. Entropy values comparison.

Test Image #	FIGURE 6	Image size	Entropy values	
			Orig. image	Encrypted image
1	CT Paranasal	256×256	5.2795	7.9975
2	Cervical X-Ray	256×256	7.1655	7.9973
3	CT Abdomen	256×256	5.8963	7.9970
4	Knee X-Ray	256×256	7.3071	7.9969

the GSE (global Shannon entropy) test sometimes does not represent the true randomness [59] in an image in comparison to GSE, local Shannon entropy is capable of capturing the randomness in local image block that could not be accurately reflected in GSE score. GSE is also considered incompatible for images of different sizes, thus inappropriate for universal measure.

Local Shannon entropy tests the randomness of an image with the same parameters irrespective to the size of test image and offer relatively fair random comparison between multiple images. The local Shannon entropy can be measured by following these steps: (1) Take S_k, non overlapping image blocks containing T_B pixels each. (2) Find the entropy value $H(S_k)$ of each image block S_k. (3) Find the average of all the calculated entropy values $H(S_k)$. In this test we use parameters (k, T_B, α), where k is number of blocks taken, T_B shows number of pixel in each block and α is the significance level. By taking different block size we have checked local Shannon entropy values of test images and compared the results with standard random local Shannon entropy values with the mean

TABLE 6. Comparison with theoretical mean and standard deviation of LSE scores.

Sr. no.	FIGURE 6	Type	Block size T_B	LSE of cipher image	Random Grayscale image values	
					$\mu_{\overline{H_{(k,T_B)}}(R)}$	$\sigma_{\overline{H_{(k,T_B)}}(R)}$
1	CT Paranasal	Gray	16×16	7.1756	7.174966353	$0.052437999/\sqrt{k}$
		Gray	32×32	7.8121	7.808756571	$0.017246343/\sqrt{k}$
		Gray	64×64	7.9542	7.954588734	$0.004024888/\sqrt{k}$
2	Cervical X-Ray	Gray	16×16	7.1741	7.174966353	$0.052437999/\sqrt{k}$
		Gray	32×32	7.8081	7.808756571	$0.017246343/\sqrt{k}$
		Gray	64×64	7.9543	7.954588734	$0.004024888/\sqrt{k}$
3	CT Abdomen	Gray	16×16	7.1698	7.174966353	$0.052437999/\sqrt{k}$
		Gray	32×32	7.8090	7.808756571	$0.017246343/\sqrt{k}$
		Gray	64×64	7.9546	7.954588734	$0.004024888/\sqrt{k}$
4	Knee X-Ray	Gray	16×16	7.1828	7.174966353	$0.052437999/\sqrt{k}$
		Gray	32×32	7.8084	7.808756571	$0.017246343/\sqrt{k}$
		Gray	64×64	7.9559	7.954588734	$0.004024888/\sqrt{k}$

TABLE 7. Local Shannon entropy values of 8-bit gray medical images with $k = 30$ and $T_B = 1936$ and their comparison with significance level 0.05 and 0.01.

Sr. no.	FIGURE 6	LSE of cipher image	Theoretical LSE critical values			
			Significance level = 0.05		Significance level = 0.01	
			h^{l*}_{left}	h^{l*}_{right}	h^{l*}_{left}	h^{l*}_{left}
1	CT Paranasal	7.901874247	7.901901305	7.90303732	7.901722822	7.903215812
2	Cervical X-Ray	7.902626309	7.901901305	7.90303732	7.901722822	7.903215812
3	CT Abdomen	7.902892198	7.901901305	7.90303732	7.901722822	7.903215812
4	Knee X-Ray	7.901989084	7.901901305	7.90303732	7.901722822	7.903215812

and variance in TABLE 6. The cipher image passes the test if result falls in the interval otherwise it fails, Also by using the standard parameters i. e., $(k, T_B) = (30, 1936)$ the local Shannon entropy for various medical images is calculated and found in range as shown in TABLE 7. The cipher images obtained from proposed encryption scheme goes in the critical interval. It shows that the proposed image encryption scheme produces cipher images that results high randomness for non overlapping blocks.

8) DIFFERENTIAL ANALYSIS

An essential property of a good performance image encryption algorithm is that, images encrypted with that algorithm should be totally different from plain images. To check the difference in an encrypted image and making one pixel change in original image then encrypted image, we use number of pixel change rate (NPCR) and unified average changing intensity (UACI). The values of NPCR and UACI can be calculated by using (12) and (13);

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{w \times h} \tag{12}$$

$$\text{UACI} = \frac{1}{w \times h}\left[\sum_{i,j} \frac{|X(i,j) - X'(i,j)|}{255}\right] \tag{13}$$

Here w and h show the width and height of the encrypted image respectively. X and X' are cipher images generated by plain image and one pixel difference in plane image respectively. If $X = X'$ then $D = 0$ otherwise 1. To resist differential attacks, NPCR and UACI [29], [58] values should be large enough.

It can be seen from the experimental results shown in TABLE 8 and TABLE 9, that the proposed scheme gets high performance for NPCR and UACI. Therefore it will give well resistance against ''known plain text attacks'' and ''chosen plain text attacks''.

9) NOISE AND DATA LOSS ATTACKS

The perfect encryption scheme ought to diminish the noise effects caused by differences in pixels in the dectypted image. For checking the capability of our proposed scheme in opposing noise and data loss attacks, we take a medical image FIGURE 6(g) of size 256×256 as test case. In the encryption result of test image we replace 1%, 2% and 5% pixels with the dark part as shown in the FIGURE 8 (a, b, c).

The decryption results of noised cipher images are also shown in FIGURE 8(d, e, f). From the FIGURE 8 it is clear that when the cipher image endure salt and pepper noise or data loss attacks, the decrypted image obtained by using our encryption scheme maintain vast majority of original image information containing only a small portion of uniformly distributed noise.

The peak signal to noise ratio (PSNR) provides a quantitative measure for the distinction between the original plain image I_P and its decryption result I_D. The cumulative squared error between the decrypted image and the original image can be measured by using mean square error (MSE). For an image of size MN the PSNR and MSE values can be calculated using

TABLE 8. NPCR values of 8-bit 256 × 256 gray medical images and their comparison with theoretical values of significance level 0.05, 0.01 and 0.001.

Sr. no.	FIGURE 6	NPCR values	Theoretical NPCR critical values		
			Significance level		
			0.05	0.01	0.001
1	CT Paranasal	99.6014%	99.5693%	99.5527%	99.5341%
2	Cervical X-Ray	99.5755%	99.5693%	99.5527%	99.5341%
3	CT Abdomen	99.5976%	99.5693%	99.5527%	99.5341%
4	Knee X-Ray	99.6189%	99.5693%	99.5527%	99.5341%

TABLE 9. UACI values of 8-bit 256 × 256 gray medical images and their comparison with theoretical values of significance level 0.05 and 0.01.

Sr. no.	FIGURE 6	UACI values	Theoretical UACI critical values			
			Significance level = 0.05		Significance level = 0.01	
			$u^{*-}_{0.05}$	$u^{*+}_{0.05}$	$u^{*-}_{0.01}$	$u^{*+}_{0.01}$
1	CT Paranasal	33.4385%	33.2824%	33.6447%	33.2255%	33.7016%
2	Cervical X-Ray	33.3571%	33.2824%	33.6447%	33.2255%	33.7016%
3	CT Abdomen	33.4123%	33.2824%	33.6447%	33.2255%	33.7016%
4	Knee X-Ray	33.5643%	33.2824%	33.6447%	33.2255%	33.7016%

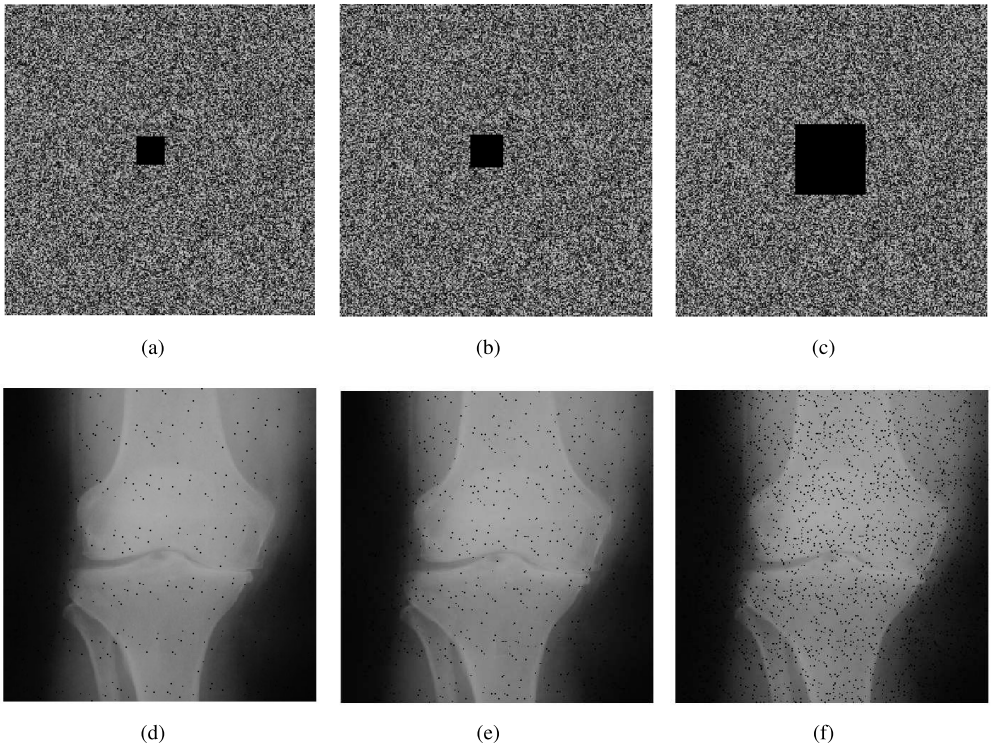

FIGURE 8. Experimental results for the performance evaluation of data loss attacks: (a,b,c) cipher images with 1%, 2% and 5% data loss, (d, e,f) decryption results of corresponding images using our scheme.

the following relations,

$$\text{PSNR} = 10.\log \frac{255^2}{\text{MSE}}\,(db), \tag{14}$$

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{i=0}^{N-1} (\text{I}_P(i,j) - \text{I}_D(i,j))^2. \tag{15}$$

The least value of MSE (15) shows the minimum error by using the proposed encryption scheme. While the PSNR (14) measure is usually employed to calculate the ability of rehabilitation. The greater value of PNSR indicates the higher fidelity of decrypted image towards its original plain image [62]. If I_D and I_P are similar then the calculated value of PSNR approaches to infinity. The value above 30 db shows that I_D and I_P are not sensible for PSNR. For the values above 35 db, it is difficult to differentiate between the original image and decrypted image. For checking the cipher image's robustness against noise attacks, we add 1%, 2% and 5% noise in

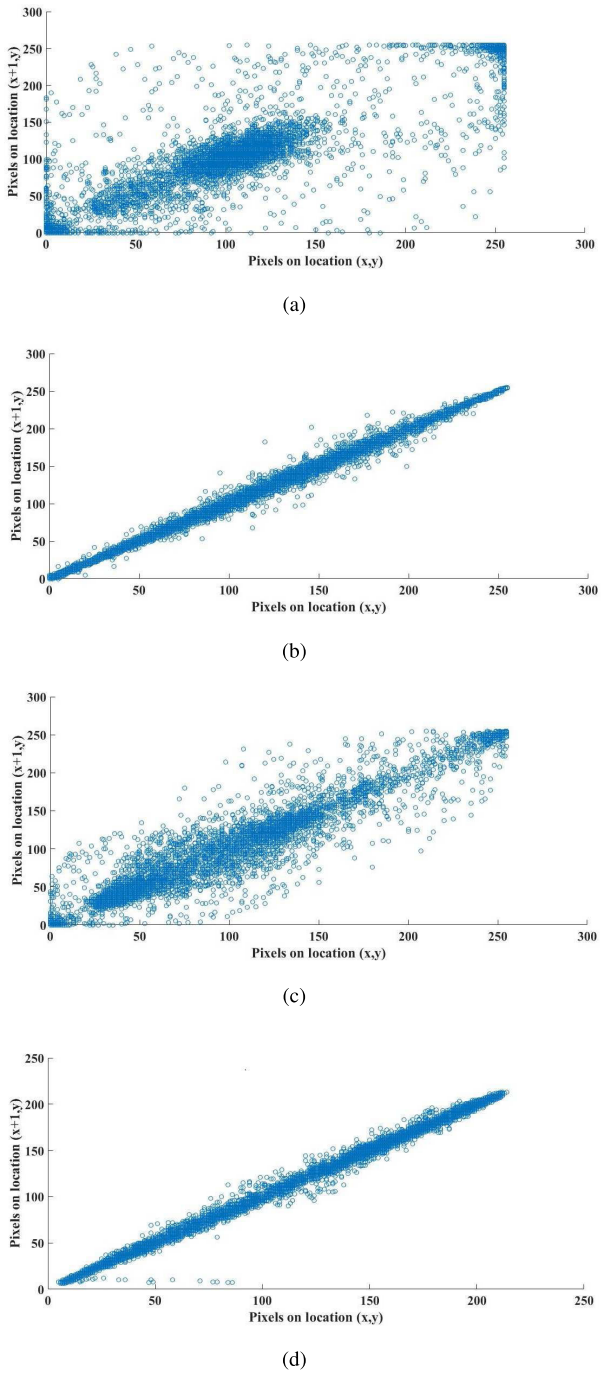

FIGURE 9. Correlation among neighboring pixels in (a) CT Paranasal, (b) Cervical X-Ray, (c) CT Abdomen, (d) Knee X-Ray.

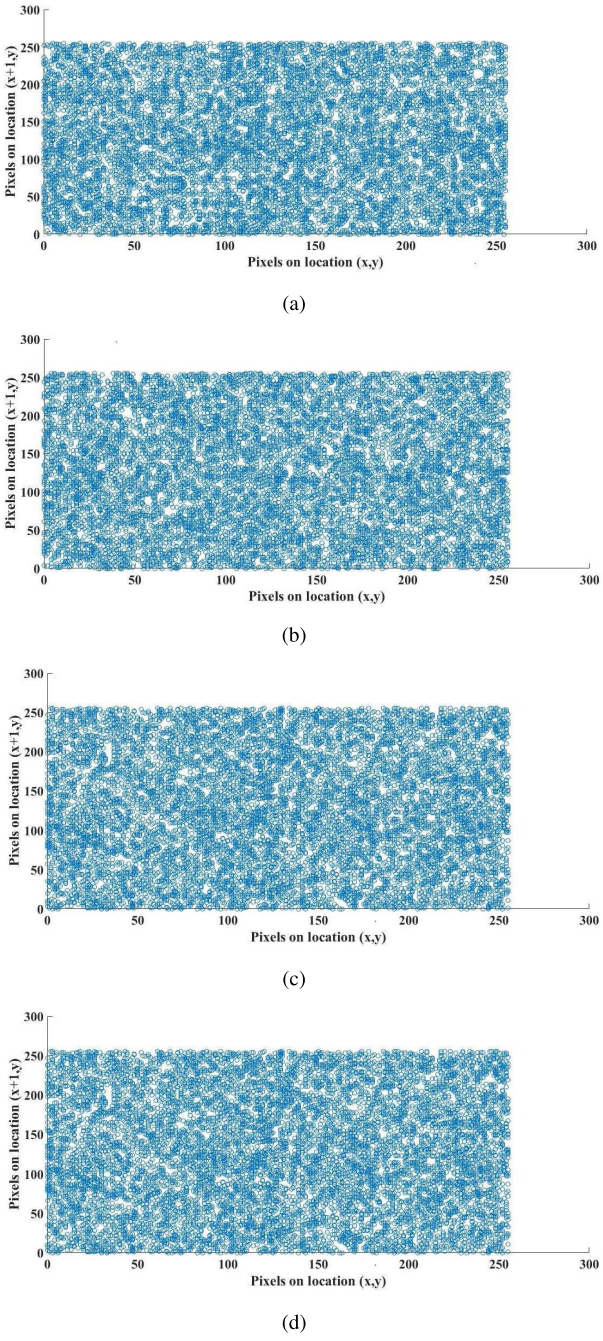

FIGURE 10. Correlation among neighboring pixels in cipher (a) CT Paranasal, (b) Cervical X-Ray, (c) CT Abdomen,(d) Knee X-Ray.

cipher image of FIGURE 6 (g), as shown in FIGURE 8 (a, b, c). The calculated values of PSNR for these modified cipher images are 25.34, 22.78 and 19.36 respectively. By observing the test results it can be seen that the encryption technique gives good performance for anti data loss and noise attacks.

10) COMPUTATIONAL COMPLEXITY

It is determined by analyzing the encryption scheme and sequence generation method. We analyze the complexity of various image encryption schemes by using the identical approach as adopted in [22] and then compare their complexities with our proposed encryption scheme. The overall complexity of our proposed encryption scheme is $O(3MN\log_2(MN) + 14MN)$, with the image size taken as $M \times N$.

The scrambling process of proposed encryption scheme consists of $3MN\log_2(MN) + 4MN$ times floating point sorting operations, while $10MN$ floating point operations are used in diffusion process. For time complexity computa-

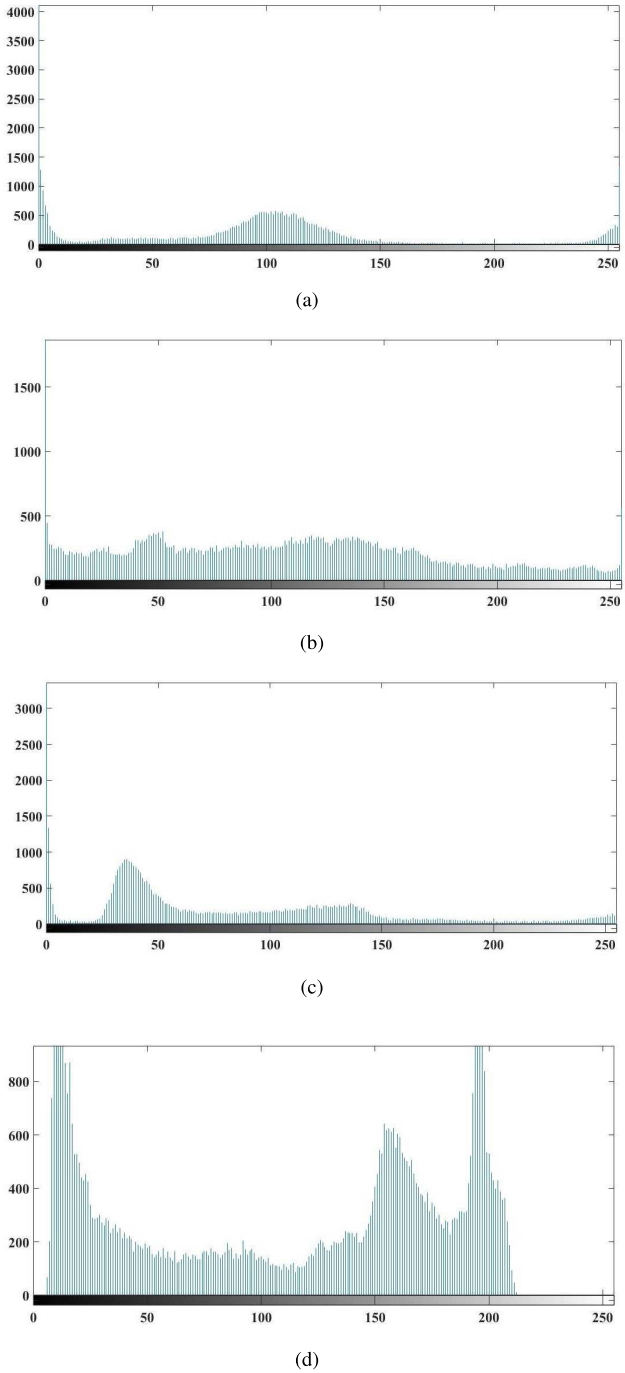

FIGURE 11. Histogram of (a) CT Paranasal image, (b) Cervical X-Ray image, (c) CT Abdomen image, (d) Knee X-Ray image.

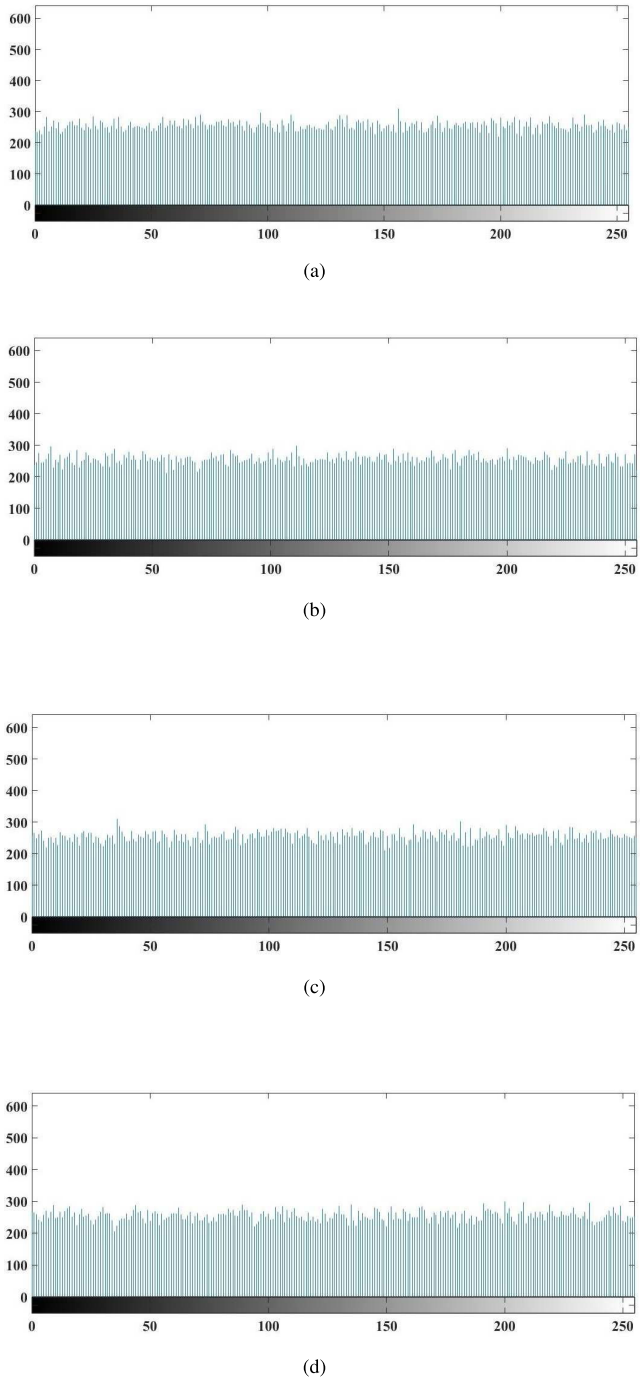

FIGURE 12. Histogram of cipher (a) CT Paranasal image, (b) Cervical X-Ray image, (c) CT Abdomen image, (d) Knee X-Ray image.

tion one time floating point operation indicates one bit level operation. By comparing the complexity of our proposed scheme in TABLE 10, with the schemes presented in [21], [22], [30], it can be seen that computational complexity of our proposed image encryption schemes exceeds by [21], [22]. It shows that the internal structure of proposed scheme is complex, hence resists against various attacks.

11) SPEED PERFORMANCE ANALYSIS

Beside the security features, the running time of an encryption algorithm is also considered an important feature. For this purpose the encryption part of the purpose scheme is tested on a personal computer having Windows 8.1 operating system, 4 GB of memory and intel core i3, 3110M with 2.4 GHz processor. The implementation of image encryption part is carried out on MATLAB R2016b (64 bit). The calculated

TABLE 10. Comparison of computational complexity with different encryption schemes.

Sr. no.	Schemes	Computational complexity	
		Scrambling	Diffusion
1	Ref [21]	$2MN + 2MN\log_2(MN)$	$2MN$
2	Ref [22]	$4MN + 2\log_2(MN)$	$2MN$
3	Ref [30]	$10MN + 2\log_2(MN)$	$2MN$
4	Ours	$4MN + 3MN\log_2(MN)$	$10MN$

TABLE 11. Comparison of encryption speed performance for 256 × 256 sized image.

Sr. no.	Encryption schemes	Encryption time (sec)
1	Ref [21]	6.3839
2	Ref [23]	0.6212
3	Ref [43]	0.4166
4	Ours	0.631

time for the encryption is 0.631 sec and the encryption time throughput is 2.4 Mb/sec. A comparison of encryption time for 256 × 256 sized image is portrayed in TABLE 11. In the proposed scheme the main time taken step is diffusion, where by using Henon map we have performed two dimensional (row-wise and column-wise) diffusion using chaotic generated matrices. Although the process is time consuming but it ensures good security results in cipher image.

B. SIGNCRYPTION ATTRIBUTES

The security components of proposed signcryption scheme are:

1) CONFIDENTIALITY

Confidentiality means to secure the message containing plain image from unauthorized sources. The proposed scheme is secure from unauthorized access as if some unauthorized party/user wants to find secret key component k' or k''. It is almost infeasible because for this he/she has to solve ECDLP and ECDHP.

2) AUTHENTICATION

Authentication is the method by which receiver can authenticate the user by following the verification method. The authentication process works by using the comparison of hash values. If the comparison returns true results, then it means that the user and his sent medical image is authenticated.

In our proposed scheme the patient calculates hash value of image I, cipher image C and key K, then multiply with base point of elliptic curve G to get authentication parameter G'. Patient sends this G' to health-care authority. The authority decrypt C with K to get image I. The authority also calculates hash value of I, C and K, and multiply it with G to get A'. The patient along with his sent image I will be authenticated if $G' = A'$.

3) INTEGRITY

In this process data is maintained in its actual form, that could not be changed by adversary during its communication. In our proposed scheme

$$h = H(I, C, K) \quad \text{and } s = \frac{k}{h + P_a} \bmod q$$

are used in signcryption stage. If a fake user changes some contents of cipher image, then new cipher image will become C', so he sends (C', s, G') the related image I' is also changed, but one way hash function makes it in-feasible. Also the change will be detected at the time of verification, hence changed cipher image will be rejected. In this way the integrity of original image will be confirmed.

4) UNFORGEABILITY

In our proposed signcryption scheme, a fake user can try to forge the signcryption scheme as following:

1) He chooses k_1 and multiply it with health-care authority's public key P_b to get secret key K_f.
2) He takes the forged image I' and encrypt it with the hashed key as $C' = E_{H(K_f)}(I')$.
3) Then he computes h' and s' as:

$$h' = H(I', C', K_f), \quad s' = \frac{k_1}{h' + s'_a} \bmod q$$

4) He also computes authentication parameter

$$G'_1 = h'G$$

and sends (C', G'_1, s') to health-care authority.

The health-care authority receives (C', s', G'_1) from fake user. It tries to find key by using its private key s_b, patient's public key P_a, received digital signature s' and authentication parameter G'_1.

$$\begin{aligned} & s_b\, s'\, G'_1 + s_b\, s'\, P_a \\ &= s_b\, \frac{k_1}{h' + s'_a}\, h'\, G + s_b \frac{k_1}{h' + s'_a}\, s_a\, G \\ &= \frac{s_b\, k_1\, h'\, G}{h' + s'_a} + \frac{s_b\, k_1\, G\, s_a}{h' + s'_a} \\ &= \frac{(s_b\, k_1\, G)(h' + s_a)}{h' + s'_a} \\ &\neq (s_b\, k\, G) \text{ or } k\, P_b = K_f \end{aligned}$$

Hence the forged key is not rightly generated and image I cannot be decrypted rightly.

5) NON-REPUDIATION

Non-repudiation means that the sender cannot deny from something he had sent. In case of denial of sending the message by the sender, the recipient may send (C, s, G') requiring the judge to verify it. In judge verification process, the judge can decide that signature is generated by the sender if the equation

$$K = (k', k'') = s_b\, s\, G' + s_b\, s\, P_a,$$

holds. In our proposed signcryption scheme, digital signature

$$s = \frac{k}{h + s_a}$$

TABLE 12. Comparison of security properties of proposed signcryption scheme.

Signcrypt. schemes	Confidentiality	Unforgability	Integrity	Non-repudiation	F. Secrecy
Proposed scheme	**Yes**	**Yes**	**Yes**	**Directly**	**Yes**
Zheng [68]	Yes	Yes	Yes	Another protocol	No
Zheng and Lmai [69]	Yes	Yes	Yes	Another protocol	No
Deng and Bao [15]	Yes	Yes	Yes	Directly	No
Jung et al. [24]	Yes	Yes	Yes	Another protocol	Yes
Gamage et al. [18]	Yes	Yes	Yes	Directly	No

TABLE 13. Comparison of computational cost of proposed signcryption scheme.

Signcrypt. schemes	Entity	*EPCM*	*ECPA*	*EXP*	*DIV*	*MUL*	*ADD*	*HASH*
Proposed scheme	sender	2	-	-	1	2	1	2
	receiver	3	-	-	-	-	1	1
Zheng [68]	sender	-	-	1	1	-	1	2
	receiver	-	-	2	-	2	-	2
Zheng and Lmai [69]	sender	1	-	-	1	1	1	2
	receiver	2	1	-	-	2	-	2
Deng and Bao [15]	sender	-	-	2	1	-	1	3
	receiver	-	-	3	-	1	-	3
Gamage et al. [18]	sender	-	-	2	1	-	1	2
	receiver	-	-	3	-	1	-	2
Jung et al. [24]	sender	-	-	2	1	-	1	2
	receiver	-	-	3	-	1	-	2

The number of operations used for: ECPM (elliptic curve point multiplication), ECPA (elliptic curve point addition), EXP (modular exponentiation), DIV (modular division), MUL (modular multiplication), ADD (modular addition), HASH (one-way hash functions).

TABLE 14. Comparison of average computation time of main operations used.

Signcrypt. schemes	Sender Average computation time(ms)	Recipient Average computation time(ms)
Proposed scheme	$3 \times 83 = 249$	$4 \times 83 = 332$
Deng and Bao [14]	$2 \times 220 = 440$	$3 \times 220 = 660$
Gamage et al. [18]	$2 \times 220 = 440$	$3 \times 220 = 660$
Jung et al. [22]	$2 \times 220 = 440$	$3 \times 220 = 660$
Zheng [68]	$1 \times 220 = 220$	$2 \times 220 = 440$
Zheng and Lmai [69]	$1 \times 83 = 83$	$2 \times 83 = 166$

contains private key s_a of the sender. Digital signature cannot be generated without sender's compliance. Therefore sender cannot deny from sending at any stage.

6) FORWARD SECRECY

It means that attacker cannot recover sender's previous message even if he gets access to the sender's private key s_a and (C, s, G'). Because a random number k is used for key generation. Which is known only to the sender. For the generation of secret key anyone has to solve the following equation:

$$K = k\, P_b$$

Here P_b is the public key of receiver and k is the random number chosen by the sender. Attacker does not know about k, hence cannot find key K and decrypt C to get plain image I.

Our proposed scheme shows good result against authentication, confidentiality, integrity, unforgeability and forward secrecy. The comparison of signcryption attributes of proposed scheme with other signcryption schemes is shown in TABLE 12.

7) ANALYSIS OF COMPUTATIONAL COST

In proposed signcryption scheme, we have calculated computational cost for sender and receiver. TABLE 13 gives a comparison for operations used by the sender and receiver, while TABLE 14 shows average computational time of mainly used operations. Sender uses only 2 elliptic curve point multiplications, while receiver takes 3 elliptic curve point multiplications hence it is more efficient than the schemes presented in [15], [18], [24].

The elliptic curve point multiplication requires 83 ms, while modular exponentiation needs 220 ms as average computational time on infineon's SLE66CUX640P [6]. The computational time is calculated in TABLE 14 and compared with other signcryption schemes. Our proposed scheme provides

some added functions like forward secrecy and non repudiation without using another protocols with less computational cost.

C. MAN IN THE MIDDLE ATTACK

We consider an unauthorized user say "Mallory" insert himself in communication between patient and health-care authority. He intercepts (C, s, G') sent by patient. Then produces his own secret key and uses it for the generation of cipher image (C'), signature (s') and authentication parameter (G''). He alters patient sent parameters (C, s, G') by his generated tuple (C', s', G'') and sends it to the health-care authority. The authority works for the the generation of secret key K^* to decrypt received C'. This key does not provide any help to reveal the secret image. Also the signature generated by the attacker will not be verified by signcryption algorithm. Hence it can be seen that, man in the middle attack is not applicable for the proposed scheme.

V. CONCLUSION

In this research, a novel medical image signcryption scheme is proposed. It uses hybrid cryptographic technique for the signcryption of image based data. Firstly patient uses his private key and health-care authority's public key to make symmetric encryption key and then he uses its hash value for chaos based medical symmetric image encryption. The health-care authority also uses the same key for decryption. Hash value of cipher image is signed and exchanged for authentication of communication.

The proposed signcryption scheme provides confidentiality, authentication, integrity, unforgability and non-repudiation. While chaos-based symmetric image encryption is checked against key space analysis, key sensitivity, correlation analysis, NPCR and UACI, local and global Shannon entropy analysis, histogram analysis, noise and data loss attacks, complexity and speed performance.

On the basis of results obtained from all these analysis, we believe that the proposed signcryption scheme is efficient and robust, providing good security for sensitive medical images.

REFERENCES

[1] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, "A novel selective encryption scheme for medical images transmission based on JPEG compression algorithm," in *Proc. Int. Conf. Knowl. Based Intell. Inf. Eng. Syst. (KSE)*, vol. 112, 2017, pp. 369–379.

[2] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Process.*, vol. 160, pp. 45–58, Jul. 2019.

[3] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Process.*, vol. 164, pp. 249–266, Nov. 2019.

[4] T. S. Ali and R. Ali, "A new chaos based color image encryption algorithm using permutation substitution and Boolean operation," *Multimedia Tools Appl.*, Mar. 2020, doi: 10.1007/s11042-020-08850-5.

[5] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *Int. J. Bifurcation Chaos*, vol. 16, no. 8, pp. 2129–2151, Aug. 2006.

[6] L. Batina, S. B. Örs, B. Preneel, and J. Vandewalle, "Hardware architectures for public key cryptography," *Integration*, vol. 34, nos. 1–2, pp. 1–64, May 2003.

[7] S. K. Bhopi, N. M. Dongre, and R. R. Gulwani, "Binary key based permutation for medical image encryption," in *Proc. Int. Conf. Inventive Comput. Technol. (ICICT)*, vol. 3, Aug. 2016, pp. 1–6.

[8] (2005). *ECC Brainpool Standard Curves and Curve Generation*. [Online]. Available: http://www.ecc-brainpool.org/download/Domain-parameters.pdf

[9] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Process.*, vol. 132, pp. 96–109, Mar. 2017.

[10] X. Chen and C.-J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping," *Saudi J. Biol. Sci.*, vol. 24, no. 8, pp. 1821–1827, Dec. 2017.

[11] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004.

[12] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. London, U.K.: Chapman & Hall, 2005.

[13] M. Crampin and B. Heal, "On the chaotic behaviour of the tent map," *Teaching Math. Appl.*, vol. 13, no. 2, pp. 83–89, 1994.

[14] U.S. Department of Health and Human Services (HHS). *Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information*. Accessed: Feb. 5, 2020. [Online]. Available: https://ocrportal.hhs.gov/ocr/breach/breach-report.jsf

[15] R. Deng and F. Bao, "A signcryption scheme with signature directly verifiable by public key," in *Public Key Cryptography* (Lecture Notes in Computer Science), vol. 1431. Berlin, Germany: Springer-Verlag, 1998, pp. 55–59.

[16] B. Desjardins, Y. Mirsky, M. P. Ortiz, Z. Glozman, L. Tarbox, R. Horn, and S. C. Horii, "DICOM images have been hacked! Now what," *Amer. J. Roentgenol.*, vol. 214, no. 4, pp. 1–9, 2019.

[17] M. M. Abd-Eldayem, "A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine," *Egyptian Informat. J.*, vol. 14, no. 1, pp. 1–13, Mar. 2013.

[18] C. Gamage, J. Leiwo, and Y. Zheng, "Encrypted message authentication by firewalls," in *Proc. Int. Workshop Public Key Cryptogr. (PKC)*, in Lecture Notes in Computer Science, vol. 1560. Kamakura, Japan: Springer-Verlag, 1999, pp. 69–81.

[19] Public Health Emergency. (Jun. 2017). *Health Care Industry Cybersecurity Task Force Report on Improving Cybersecurity in the Health Care Industry*. [Online]. Available: https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf

[20] Z. Hua, F. Jin, B. Xu, and H. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Process.*, vol. 149, pp. 148–161, Aug. 2018.

[21] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted-sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.

[22] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 144, pp. 134–144, Mar. 2018.

[23] M. Hénon, "A two-dimensional mapping with a strange attractor," in *The Theory of Chaotic Attractors*. New York, NY, USA: Springer, 1976, pp. 94–102.

[24] H. Y. Jung, K. S. Chang, D. H. Lee, and J. I. Lim, "Signcryption schemes with forward secrecy," in *Proc. WISA*, 2001, pp. 403–475.

[25] HIPAA Journal. (Aug. 20, 2018). *Court Approves Anthem 115 Million Data Breach Settlement*. [Online]. Available: https://www.hipaajournal.com/court-approvesanthem-115-million-data-breach-settlement/

[26] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[27] 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, May 2010.

[28] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.

[29] E. N. Lorenz, "Deterministic non-periodic flow," *J. Atmos. Sci.*, vol. 20, no. 6, pp. 130–141, 1963.

[30] S. Ma, Y. Zhang, Z. Yang, J. Hu, and X. Lei, "A new plaintext-related image encryption scheme based on chaotic sequence," *IEEE Access*, vol. 7, pp. 30344–30360, 2019.

[31] A. B. Mahmood and R. D. Dony, "Segmentation based encryption method for medical images," in *Proc. Int. Conf. Internet Technol. Secured Trans.*, 2011, pp. 596–601.
[32] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, pp. 459–467, Jun. 1976.
[33] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Cryptograph. Techn.*, Berlin, Germany: Springer, 1985, pp. 417–426.
[34] Y. Mirsky, T. Mahler, I. Shelef, and Y. Elovici, "Malicious tampering of 3D medical imagery using deep learning," Jun. 2019, *arXiv:1901.03597*. Accessed: Jul. 2, 2019. [Online]. Available: https://arxiv.org/abs/1901.03597
[35] M. A. Mohamed, F. W. Zaki, and A. M. El-Mohandes, "Novel fast encryption algorithms for multimedia transmission over mobile WiMax networks," *Int. J. Comput. Sci. Issues*, vol. 9, no. 6, p. 60, 2012.
[36] T. A. Morgan, D. E. Avrin, C. D. Carr, K. J. Dreyer, A. E. Flanders, R. Khorasani, C. P. Langlotz, and R. L. Arenson, "Meaningful use for radiology: Current status and future directions," *Radiology*, vol. 269, no. 2, pp. 318–321, Nov. 2013.
[37] *Digital Imaging and Communications in Medicine (DICOM) Standard*, Standard ISO 12052, National Electrical Manufacturers Association, 2016.
[38] National Electrical Manufacturers Association. (2003). *Digital Imaging and Communications in Medicine (DICOM)*. [Online]. Available: http.//medical.nema.org/
[39] CBS News. (Feb. 14, 2019). *Hackers are Stealing Millions of Medical Records and Selling them on Dark Web*. [Online]. Available: https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web
[40] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, Sep. 2006.
[41] C. Pan, G. Ye, X. Huang, and J. Zhou, "Novel meaningful image encryption based on block compressive sensing," *Secur. Commun. Netw.*, vol. 2019, pp. 1–12, Nov. 2019.
[42] K. Pearson, "Notes on regression and inheritance in the case of two parents," *Proc. Roy. Soc. London*, vol. 58, nos. 347–352, pp. 240–242, 1895.
[43] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Comput. Biol. Med.*, vol. 72, pp. 170–184, May 2016.
[44] L. Schencker. (Mar. 8, 2019). *Hackers Target Health Data: 82% of Hospital Tech Experts Reported 'Significant Security Incident' in Last Year*. Chicago Tribune. [Online]. Available: https://www.chicagotribune.com/business/ct-biz-hospital-databreaches-20190307-story.html
[45] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul./Oct. 1948.
[46] A. Shukla, J. Shah, and N. Prabhu, "Image encryption using elliptic curve cryptography," *Int. J. Student Res. Technol. Manage.*, vol. 1, no. 2, pp. 115–117, 2015.
[47] L. D. Singh and K. M. Singh, "Image encryption using elliptic curve cryptography," *Procedia Comput. Sci.*, vol. 54, pp. 472–481, Jan. 2015.
[48] Verizon Enterprise. (2018). *2018 Data Breach Investigations Report*. [Online]. Available: https://enterprise.verizon.com/resources/reports/2018/DBIR-2018-Report.pdf
[49] X. Wang, Y. Peng, L. Lu, Z. Lu, M. Bagheri, and R. M. Summers, "ChestX-ray8: Hospital-scale chest X-ray database and benchmarks on weakly-supervised classification and localization of common thorax diseases," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jul. 2017, pp. 3462–3471.
[50] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, Nov. 2010.
[51] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.
[52] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.
[53] 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.
[54] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Inf. Sci.*, vol. 507, pp. 16–36, Jan. 2020.
[55] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*. London, U.K.: Chapman & Hall, 2008.
[56] N. Whitehead and A. Fit-Florea, "Precision & performance: Floating point and IEEE 754 compliance for NVIDIA GPUs," *rn (A + B)*, vol. 21, no. 1, pp. 18749–19424, 2011.
[57] S. T. G. Wong, "A cryptologic based trust center for medical images," *J. Amer. Med. Inform. Assoc.*, vol. 3, no. 6, pp. 410–421, Nov. 1996.
[58] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J., Multidisciplinary J. Sci. Technol., J. Sel. Areas Telecommun.*, vol. 1, no. 2, pp. 31–38, 2011.
[59] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.
[60] Nist. (1999). *Recommended Elliptic Curves for Federal Government Use*. [Online]. Available: http://csrc.nist.gov/csrc/fedstandards.html
[61] E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Comput. Electr. Eng.*, vol. 54, pp. 471–483, Aug. 2016.
[62] E. Yavuz, "A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme," *Opt. Laser Technol.*, vol. 114, pp. 224–239, Jun. 2019.
[63] G. Ye, C. Pan, X. Huang, and Q. Mei, "An efficient pixel-level chaotic image encryption algorithm," *Nonlinear Dyn.*, vol. 94, no. 1, pp. 745–756, Oct. 2018.
[64] G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, pp. 45–53, Aug. 2017.
[65] J. Zaman and R. Ghosh, "Review on fifteen statistical tests proposed by NIST," *J. Theor. Phys. Cryptogr.*, vol. 1, pp. 18–31, Nov. 2012.
[66] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft Comput.*, vol. 26, pp. 10–20, Jan. 2015.
[67] Y. Q. Zhang and X. Y. Wang, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.
[68] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost(encryption)," in *Proc. Annu. Int. Cryptol. Conf.* Berlin, Germany: Springer, 1997, pp. 165–179.
[69] Y. Zheng and H. Imai, "How to construct efficient signcryption schemes on elliptic curves," *Inf. Process. Lett.*, vol. 68, no. 5, pp. 227–233, Dec. 1998.
[70] M. Zia and R. Ali, "Cryptanalysis and improvement of an elliptic curve based signcryption scheme for firewalls," *PLoS ONE*, vol. 13, no. 12, pp. 1–11, 2018.
[71] M. Zia and R. Ali, "Cryptanalysis and improvement of blind signcryption scheme based on elliptic curve," *Electron. Lett.*, vol. 55, no. 8, pp. 457–459, Apr. 2019.

TAHIR SAJJAD ALI received the M.Phil. degree from Riphah International University, Islamabad, Pakistan. He is currently pursuing the Ph.D. degree with the Faculty of Computing, Capital University of Science and Technology, Islamabad. His research interests include chaos theory and its applications in information security, cryptanalysis of image encryption schemes, and algebraic cryptography.

RASHID ALI (Member, IEEE) received the Ph.D. degree from the Faculty of Information and Mathematics, University of Passau, Germany, in 2011. He is currently working as an Associate Professor with the Faculty of Computing, Capital University of Science and Technology, Pakistan. He is mainly involved in the research work on algebraic cryptography, cryptanalysis, and fixed point theory in fuzzy metric spaces.