Hindawi
Security and Communication Networks
Volume 2017, Article ID 6729896, 12 pages
https://doi.org/10.1155/2017/6729896

Research Article

A Hybrid Chaotic and Number Theoretic Approach for Securing DICOM Images

Jeyamala Chandrasekaran[1] and S. J. Thiruvengadam[2]

[1]*Department of Information Technology, Thiagarajar College of Engineering, Madurai, India*
[2]*Department of Electronics and Communication Engineering, Thiagarajar College of Engineering, Madurai, India*

Correspondence should be addressed to Jeyamala Chandrasekaran; jeyamala@tce.edu

Received 31 July 2016; Accepted 24 November 2016; Published 12 January 2017

Academic Editor: Ángel Martín Del Rey

The advancements in telecommunication and networking technologies have led to the increased popularity and widespread usage of telemedicine. Telemedicine involves storage and exchange of large volume of medical records for remote diagnosis and improved health care services. Images in medical records are characterized by huge volume, high redundancy, and strong correlation among adjacent pixels. This research work proposes a novel idea of integrating number theoretic approach with Henon map for secure and efficient encryption. Modular exponentiation of the primitive roots of the chosen prime in the range of its residual set is employed in the generation of two-dimensional array of keys. The key matrix is permuted and chaotically controlled by Henon map to decide the encryption keys for every pixel of DICOM image. The proposed system is highly secure because of the randomness introduced due to the application of modular exponentiation key generation and application of Henon maps for permutation of keys. Experiments have been conducted to analyze key space, key sensitivity, avalanche effect, correlation distribution, entropy, and histograms. The corresponding results confirm the strength of the proposed design towards statistical and differential crypt analysis. The computational requirements for encryption/decryption have been reduced significantly owing to the reduced number of computations in the process of encryption/decryption.

1. Introduction

Telemedicine is essentially the remote diagnosis and treatment of patients by means of telecommunications technology. The increasing adoption and usage of internet, smart phones, mobile health care devices, and wearable health technology have significantly impacted the growth of telemedicine over the years. Telemedicine involves large volume of storage and exchange of electronic health records among physicians, patients and health care professionals for better health services. Health records involve extensive usage of multimedia especially images, which are generated from various imaging technologies like conventional X-rays, ultrasound imaging, digital mammography, Computed Axial Tomography (CT), Positron Emission Tomography (PET), and Magnetic Resonance Imaging (MRI). These medical images are highly sensitive and are to be operated in a resource constrained environment characterized by lower band width, limited processing power, and limited memory. The strong privacy requirements of medical images with the operating constraints demand secure encryption algorithms with optimal processing requirements.

Text based algorithms like Advanced Encryption Standard, Elliptic Curve Cryptography, and RC4 are not preferred for encryption of medical images because of the complicated internal structure, memory requirements, and time delay incurred in the process of key generation and encryption/decryption. Few researches in the literature focus on the customization of the text based algorithms for encrypting medical images [1–4]. However reduction in computational time is not up to the desired level.

Substantial amount of research work in the literature have focused on application of chaotic maps for cryptography due to the high sensitivity to initial conditions, nonlinearity, and random and ergodic nature of chaotic maps. Fridrich [5] proposed the initial framework for chaos based image

encryption, which consists of two stages, namely, permutation/confusion and substitution/diffusion. A 2D chaotic map was used to control the parameters in both the stages. Following Fridrich, many researchers [6–11] have contributed significant enhancements for improving security in the field of chaos based image encryption.

Owing to the wide spread usage of telemedicine, many research works have been attempted to test the feasibility of chaotic maps for medical image encryption. Hu and Han [12] presented a pixel-based scrambling scheme based on simple XOR operation. The scrambling key is a true random number (TRN) sequence derived from the multiscroll chaotic attractors. Fu et al. [13] attempted to improve the efficiency of chaos based image cipher by introducing substitution in the permutation process itself. Arnold cat map and logistic map are chosen for permutation and substitution, respectively. Since pixel value mixing is contributed by both permutation and substitution stage, desired level of security could be achieved in fewer rounds. Liu et al. [14] used hash value of the pathological image and random number to generate the initial conditions of chaotic maps. Chebyshev maps are used to confuse the pixels. Since each block of the image is encrypted using the hash value of the previous block and random number, different cipher images are generated for different recipients. Praveenkumar et al. [15] proposed a trilayer cryptic system, which is a blend of Latin square image cipher, discrete Gould transform, and Rubik's encryption for encryption of DICOM images. Confusion, diffusion, tamper proofing, permutation, randomness, and ergodicity have been fused together to enhance security. Ravichandran et al. [16] employed bioinspired crossover and mutation unit to provide confusion and diffusion of pixels in a DICOM image. Logistic, tent, and sine maps are used for the second stage of encryption. Combined logistic tent maps and combined logistic sine maps are used to generate enlarged and elevated chaotic sequences, which are further enhanced by crossover and mutation strategies. To diffuse the effect of slight change in single pixel intensity of plain image over many pixels in cipher image, logical operations such as XOR and circular rotation are proposed by Yavuz et al. [17].

Though chaotic cryptosystems provide the required confusion and diffusion properties, they do have the limitations of low cycle lengths and are computationally less efficient because of floating point arithmetic. DICOM images are highly sensitive because even a small amount of visual degradation can lead to false diagnosis. Lima et al. [18] proposed a model for medical image encryption using Cosine Number Transform (CNT) to avoid round off errors. Their model provides zero tolerance effect since it involves only integer arithmetic. Dzwonkowski et al. [19] adopted Feistel network for encryption of DICOM images, wherein special properties of quaternions are used to perform rotations in 3D space for each of the cipher rounds.

The proposed work is an attempt to improve the computational efficiency of chaotic crypto systems by generating keys based on number theory. As the system design involves modular exponentiation for key generation, it completely eliminates round off errors in decryption and provides zero tolerance effect. To further enhance the level of security, a permutation stage is included, wherein the keys generated are chaotically permuted and controlled by Henon map. Permutation of key arrays based on Henon maps generates independent key arrays for encryption of every subimage which enhances the randomness of the keys. The security of the proposed algorithm is confirmed through statistical and differential crypt analysis. While the proposed algorithm ensures a high degree of security on par with the existing algorithms reported in the literature, the computational time and resources have been reduced significantly, because of simple structure in encryption/decryption. This makes the proposed algorithm suitable for real time applications.

2. Background

2.1. Discrete Logarithms

2.1.1. Primitive Roots. If "p" is a prime and "a" is any element in the residual set of $Z_p = \{1, 2, 3, \ldots, p-1\}$ and if $a \bmod p, a^2 \bmod p, a^3 \bmod p, \ldots, a^{p-1} \bmod p$ are distinct and consist of integers within the range $[1 : p-1]$, then "a" is called as the primitive root or generator of "p" [22, 23].

2.1.2. Discrete Logarithm. If "l" is an arbitrary integer in $Z_p = \{1, 2, 3, \ldots, p-1\}$ and g is a primitive root of "p" then there exists exactly one number μ such that

$$l \equiv g^{\mu} \pmod{p}. \tag{1}$$

The number "μ" is then called the discrete logarithm [24] of "l" with respect to the base "g modulo p" and is denoted as

$$\mu \equiv \operatorname{ind}_g l \pmod{p}. \tag{2}$$

Discrete logarithm principle has been extensively used in the design of asymmetric algorithms like ElGamal Crypto systems and Diffie Hellman Key exchange. Elliptic curve version of discrete logarithm problem forms the foundation of Elliptic Curve Cryptography. Few researchers have extended discrete logarithms for symmetric text and image encryption [25, 26]. The strength of discrete logarithm is because of the fact that the forward process of calculation of exponentials modulo prime is easier even for very larger primes using fast modular exponentiation. However, the reverse process of calculation of discrete logarithms is considered infeasible for larger primes [23].

2.2. Henon Maps.

The Henon map is a two-dimensional discrete dynamical system introduced by Michael Henon [27]. Henon map takes a point (x_n, y_n) in the plane and maps it to a new point (x_{n+1}, y_{n+1}) as defined by the equations

$$\begin{aligned} x_{n+1} &= y_{n+1} + 1 - \alpha x_n^2, \\ y_{n+1} &= \beta x_n. \end{aligned} \tag{3}$$

The desired statistical properties can be obtained from the generated values if the input values are as follows:

"α" can be in the range of 1.16 to 1.41.

"β" can be in the range of 0.2 to 0.3.

"x_0" can be in the range of −1 to 1.

"y_0" can be in the range of −0.35 to 0.35.

Skip value can be in the range of 80 to 1000.

Henon map is found to exhibit good chaotic behavior for values $\alpha = 1.4$ and $\beta = 0.3$. A minute variation in the initial parameters even in ten-millionth place value of the Henon maps could yield widely divergent results. This extreme sensitiveness to initial conditions of the Henon map is exploited in various image encryption algorithms. Henon map has been tried for various applications in cryptography such as pseudo number generation [28], encryption of satellite imagery [29], and design of substitution boxes [30].

3. Proposed Methodology

The proposed methodology consists of three stages, namely,

(A) generation of two-dimensional key array based on modular exponentiation,

(B) permutation of key array based on Henon maps,

(C) encryption/decryption of DICOM images based on bitwise XOR of subimages with permuted key arrays.

(A) Generation of Two-Dimensional Key Array Based on Modular Exponentiation

(A1) Select a prime number "p" and generate all possible primitive roots of the prime. A primitive root of a prime "p" is an integer "g" such that "$g \bmod p$" has multiplicative order "$p - 1$".

(A2) If $g_1, g_2, g_3, \ldots, g_m$ are the primitive roots of the prime "p" then a two-dimensional array "k" of order "$R \times C$" is generated as follows:

where

"R" refers to the number of rows = number of primitive roots for the prime "p".

"C" refers to the number of columns = $p - 1$.

$$k = \begin{bmatrix} {g_1}^1 \bmod p & {g_1}^2 \bmod p & {g_1}^3 \bmod p & {g_1}^4 \bmod p & \cdots & {g_1}^{p-1} \bmod p \\ {g_2}^1 \bmod p & {g_2}^2 \bmod p & {g_2}^3 \bmod p & {g_2}^4 \bmod p & \cdots & {g_2}^{p-1} \bmod p \\ {g_3}^1 \bmod p & {g_3}^2 \bmod p & {g_3}^3 \bmod p & {g_3}^4 \bmod p & \cdots & {g_3}^{p-1} \bmod p \\ \vdots & \vdots & \vdots & \vdots & \cdots & \vdots \\ {g_m}^1 \bmod p & {g_m}^2 \bmod p & {g_m}^3 \bmod p & {g_m}^4 \bmod p & \cdots & {g_m}^{p-1} \bmod p \end{bmatrix}. \tag{4}$$

(B) Permutation of Key Matrix Based on Henon Maps

(B1) Exchange the parameters P_1, P_2, P_3, P_4, and P_5 using the public keys of the receiver for generation of permutation keys for rearranging the elements in the key pool.

(i) P_1: the parameters of the Henon map α, β and seed values x_0, y_0.

(ii) P_2: the number for decimal places of the mantissa that are to be supported by the calculating machines.

(iii) P_3: the number of iterations after which the first value is to be picked for generating keys.

(iv) P_4: the skip value to be maintained for picking successive values thereafter.

(v) P_5: increment value of seed for generating different permutation keys.

(B2) Iterate the two-dimensional equations of the Henon map with initial parameter settings as defined in P_1 for a predefined number of times. The number of iterations (N_c) is given by $P_3 + (l - 1)P_4$, where $l = \max(R, C)$.

(B3) Process the result in two one-dimensional arrays "$\mathbf{X}$" and "$\mathbf{Y}$" of length "l".

(B4) Encode the values generated by the Henon map to integer representation for locating row and column indices.

$$X'_n = (X_n - X_{\min})\left(\frac{(\text{row}_{\max} - \text{row}_{\min})}{(X_{\max} - X_{\min})}\right) + \text{row}_{\min},$$
$$Y'_n = (Y_n - Y_{\min})\left(\frac{(\text{col}_{\max} - \text{col}_{\min})}{(Y_{\max} - Y_{\min})}\right) + \text{col}_{\min}, \tag{5}$$

where X' and Y' correspond to the encoded version of X and Y. $X_{\min}$, $X_{\max}$, $Y_{\min}$, and $Y_{\max}$ are the minimum and maximum values of the two-dimensional Henon map equations generated in various iterations.

$\text{row}_{\min}$, $\text{row}_{\max}$, $\text{col}_{\min}$, and $\text{col}_{\max}$ are the minimum and maximum values of row and column indices respectively in the key matrix.

(B5) Permute the two-dimensional key array using the encoded arrays (X', Y') as the permutation key.

(B6) Repeat steps (B2) to (B5) with updated seed value $x'_0 = x_o + P_5$ for generating different permutation keys as required. The number of permutation keys is decided by the count of subimages.

Table 1: Description of image samples.

Identifier	File name	Size	RGB/monochrome	Pixel depth
D_1	CT-MONO2-abdo	512 × 512	Monochrome	8
D_2	OT-MONO2-8-colon	512 × 512	Monochrome	8
D_3	OT-MONO2-8-hip	512 × 512	Monochrome	8
D_4	OT-MONO2-8-a7	512 × 512	Monochrome	8
D_5	US-RGB-8-epicard	640 × 480	RGB	8
D_6	US-RGB-8-esopscho	256 × 120	RGB	8
D_7	MR-MONO2-12-angioan1	256 × 256	Monochrome	12
D_8	MR-MONO2-16-head	256 × 256	Monochrome	16
D_9	MR-MONO2-16-knee	256 × 256	Monochrome	16

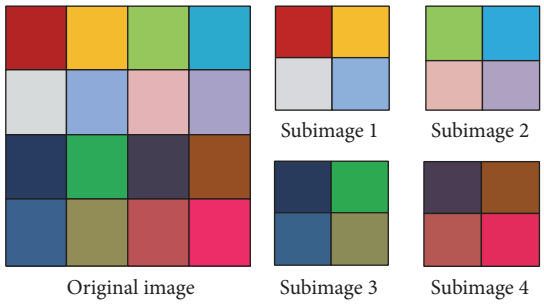

Figure 1: Splitting of plain images to subimages: Case 1.

(C) Encryption/Decryption of DICOM Images Based on Bitwise XOR of Subimages with Permuted Key Arrays

(C1) Read the input DICOM image of size $R'' \times C''$. The number of rows (R) in the two-dimensional key array is equal to the number of primitive roots of the prime (p). The number of columns (C) is given by ($p - 1$).

(C2) If R'' is greater than R and C'' is greater than C, divide the image into nonoverlapping subimages as follows.

Case 1. If R'' and C'' are exact multiples of R and C (i.e., $R'' = aR$ and $C'' = bC$ where a and b are integers), the image is split into subimages of order $R \times C$. The number of subimages (N_{SI}) is given by

$$N_{SI} = \frac{R'' \times C''}{R \times C}. \quad (6)$$

The process is illustrated by a simple example as depicted in Figure 1. Supposing the size of the two-dimensional key array is 2×2 and the size of the image is 4×4, the image is split into four subimages of size 2×2.

Case 2. If R'' and C'' are not exact multiples of R and C, the image is split into possible subimages of order $R \times C$. The pixels in the left out rows and columns form independent two-dimensional arrays whose size is less than $R \times C$. Supposing the size of the two-dimensional key array is 2×2 and size of the image is 5×5, the image is split up into four subimages of size 2×2, two arrays of order 2×1, two arrays of order 1×2, and an array with size 1×1. The process of splitting is depicted in Figure 2.

The pixels present in (m, n) location of the subimage array are XORed with the elements present at the location (m, n) of the key array, respectively.

(C3) Encrypt every subimage by bitwise XOR operation of the pixel with the corresponding element located in the same index in permuted key array. Integrate the subblocks to construct the ciphered image.

(C4) For decryption, divide the cipher image again into subimages as described in (C2). Decrypt every individual pixel of the cipher subimage by performing bitwise XOR with keys generated independently at the receiver. Recover the plain subimages independently and integrate to construct the original image. The block diagram of complete encryption of the image is represented in Figure 3.

4. Experimental Results

The proposed medical image encryption algorithm is implemented in MATLAB R2012a in Windows platform. The system configuration includes Intel core i3 Processor operating at 2.53 GHz and 3 GB RAM. DICOM samples downloaded from http://www.barre.nom.fr/medical/samples/ are used for validation and performance analysis. Description of the medical image samples are provided in Table 1.

Figure 4 represents the sample DICOM images and Figure 5 represents the corresponding encrypted DICOM images.

4.1. Statistical Analysis

4.1.1. Histogram Analysis. The histogram of an image is a plot showing the frequency of intensities of pixels. The statistical relationship between the plain and cipher image is exploited to launch statistical attacks on an image crypto system. Since the histograms of plain and encrypted DICOM images in Figures 6, 7(a), and 7(b) are completely different from each other, it can be concluded that the proposed image crypto system provides complete resistance towards statistical crypt analysis.

4.1.2. Correlation Distribution. A good image crypto system should completely destroy the relationship between adjacent

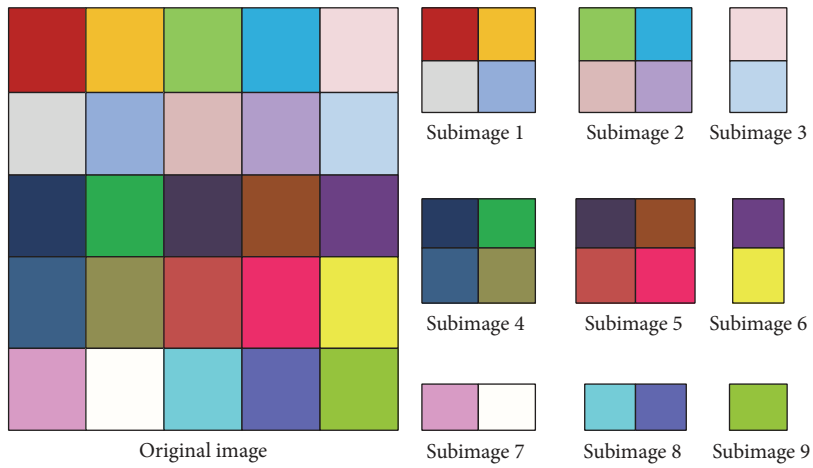

Figure 2: Splitting of plain images to subimages: Case 2.

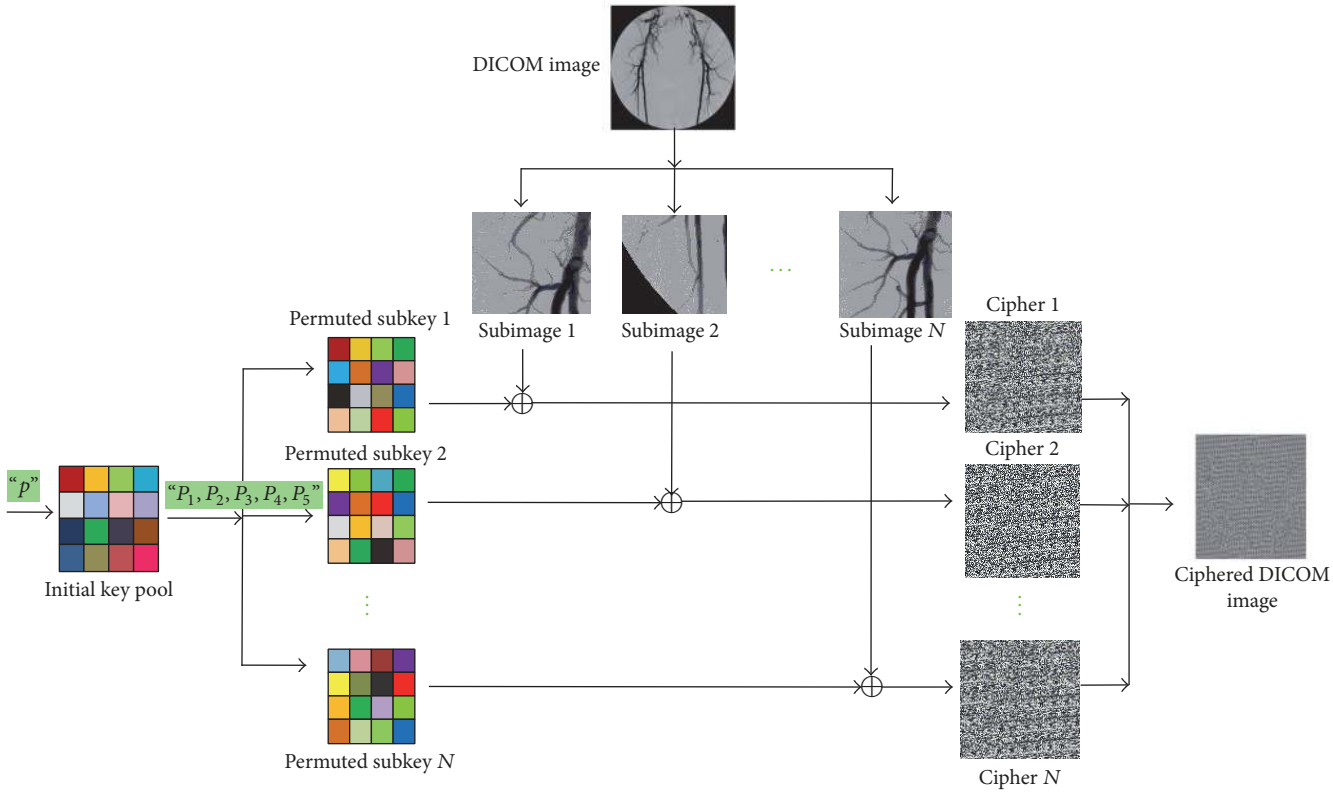

Figure 3: Block diagram of proposed encryption scheme.

pixels across horizontal, vertical, and diagonal directions thus providing no clue for crypt analysis. The horizontal, vertical, and diagonal correlation of the encrypted image samples are presented in Table 2. The horizontal, vertical, and diagonal correlation of a DICOM image are closely equal to one as the adjacent pixels are highly related to each other. The correlation values for the encrypted image are close to zero which confirms that the relationship between adjacent pixels of the encrypted image has been completely destroyed The correlation distribution of original and encrypted DICOM image sample is illustrated in Figure 8. It could be inferred that the statistical properties of the plain image have been randomly diffused in the cipher image thereby proving the strength of the algorithm against statistical crypt analysis.

4.1.3. Information Entropy. Information entropy is the statistical measure of randomness associated with an image. The probability of making predictions from the cipher image

Table 2: Correlation coefficient of original and encrypted image samples.

Image sample	Horizontal		Vertical		Diagonal	
	Original image	Encrypted image	Original image	Encrypted image	Original image	Encrypted image
D_1	0.9131	0.0075	0.8713	0.0142	−0.0057	0.0061
D_2	0.9872	−0.0032	0.9859	0.0016	0.9768	−0.0029
D_3	0.9868	0.0014	0.9892	−0.0009	0.9800	0.0065
D_4	0.9777	0.0081	0.9835	−0.0039	0.9707	0.0030
D_5	0.9231	0.0027	0.9436	0.0007	0.8995	−0.0040
D_6	0.9524	0.0019	0.8463	−0.0014	0.8295	−0.0027

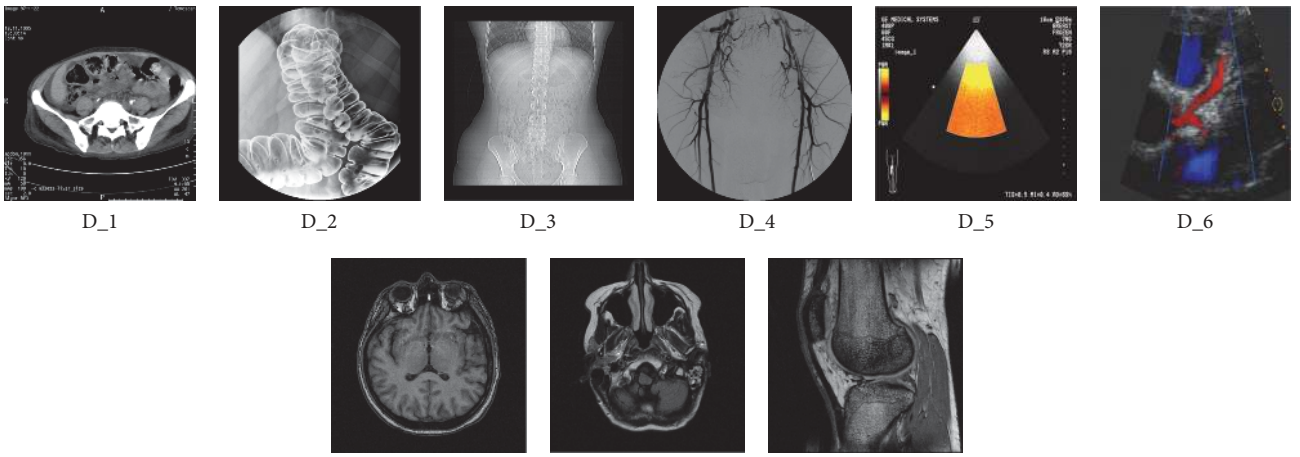

Figure 4: DICOM image samples.

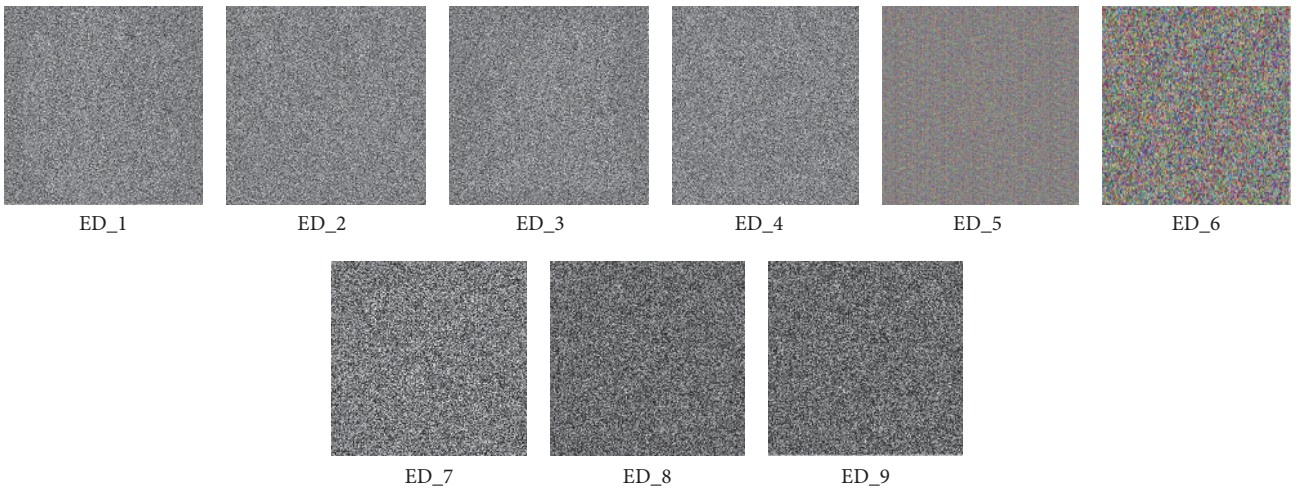

Figure 5: Encrypted DICOM image samples.

decreases with the increase in randomness. The entropy of plain and cipher medical image samples $H(m)$ are calculated using

$$H(m) = -\sum_{i=1}^{n} P(m_i) \log_2 P(m_i), \quad (7)$$

where $P(m_i)$ refers to the probability of occurrence of particular intensity. The results are tabulated in Table 3.

The entropy of encrypted images is close to the theoretical value of 8, thereby ensuring that no information is made available for launching cryptographic attacks.

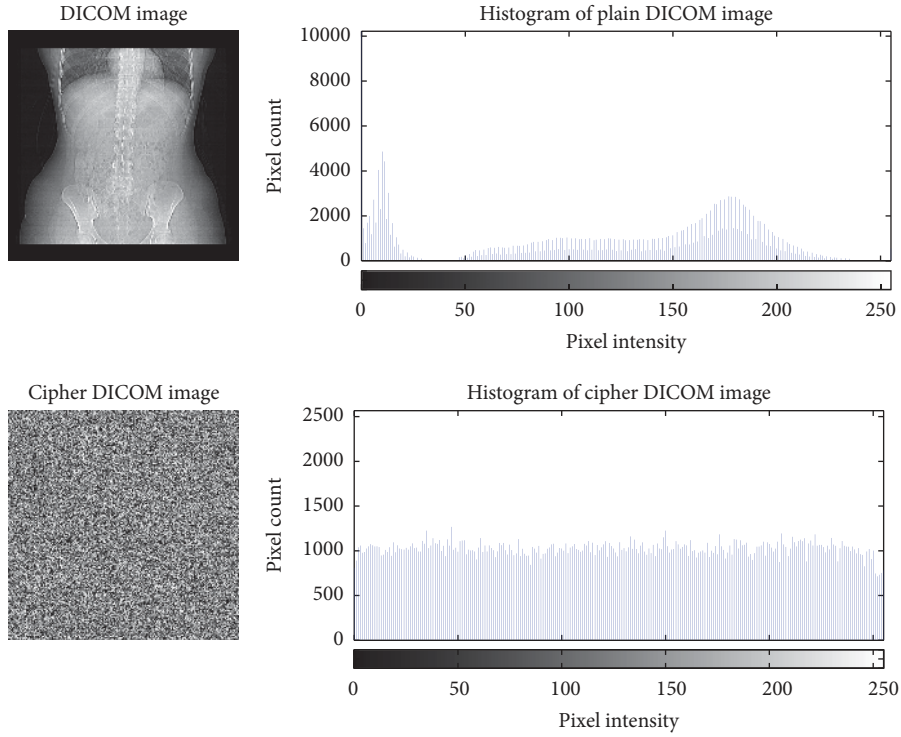

Figure 6: Histograms of plain (D_3) and encrypted DICOM sample (ED_3).

Table 3: Entropy of plain and cipher DICOM samples.

DICOM samples	Entropy	Encrypted images	Entropy
D_1	3.7368	ED_1	7.9788
D_2	5.5491	ED_2	7.9944
D_3	6.4002	ED_3	7.9957
D_4	4.9314	ED_4	7.9924
D_5	2.9540	ED_5	7.9869
D_6	2.5898	ED_6	7.9682
D_7	6.2935	ED_6	7.9902
D_8	5.7043	ED_6	7.9887
D_9	7.0741	ED_6	7.9939

4.2. Differential Analysis. The immunity of an image cryptosystem towards differential attack is measured by Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI), which are calculated as follows:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100,$$
$$\text{UACI} = \frac{1}{W \times H} \sum_{i,j} \frac{|c1(i,j) - c2(i,j)|}{255} \times 100, \quad (8)$$

where W and H are the width and height of the medical image, and $c1$ and $c2$ are two encrypted images with slightly different keys. $D(i, j)$ is a bipolar array with the same size as that of $c1$ and $c2$. If $c1(i, j)$ and $c2(i, j)$ are identical, then $D(i, j)$ is set to 0; else set to 1. Sample DICOM images were encrypted with keysets which differ by a very small magnitude in the initial conditions of Henon map. NPCR and UACI were measured for the corresponding cipher images and are presented in Table 4. The NPCR measures the percentage of different pixel numbers between the two encrypted images. The UACI measures the average intensity of differences between the two encrypted images. On an average, the NPCR and UACI values are 99.60001% and 33.4738%, respectively, which are close to the theoretical values specified by Wu et al. [31]. Higher magnitude of NPCR and UACI ensures that the proposed system offers sufficiently large resistance towards differential attack.

4.3. Key Space Analysis. Decrypting the cipher image with all possible keys to recover the original image is known as the brute force attack. The key space of the cryptosystem must be sufficiently large to withstand brute force attack. In the proposed cryptosystem, the size of the key pool generated increases with the increase in magnitude of the prime "p". The key pool is once again permuted for every encryption of every subimage by Henon map, which is extremely sensitive to initial conditions. The permutation keys generated are totally different even for ten millionth differences in decimal places of the initial conditions of the Henon map. The choice for the key values (p, P_1, P_3, P_4, P_5) are as follows.

(i) Prime (p):

by experimentation it has been observed that, for an image with 8-bit pixel depth, the algorithm produces satisfactory

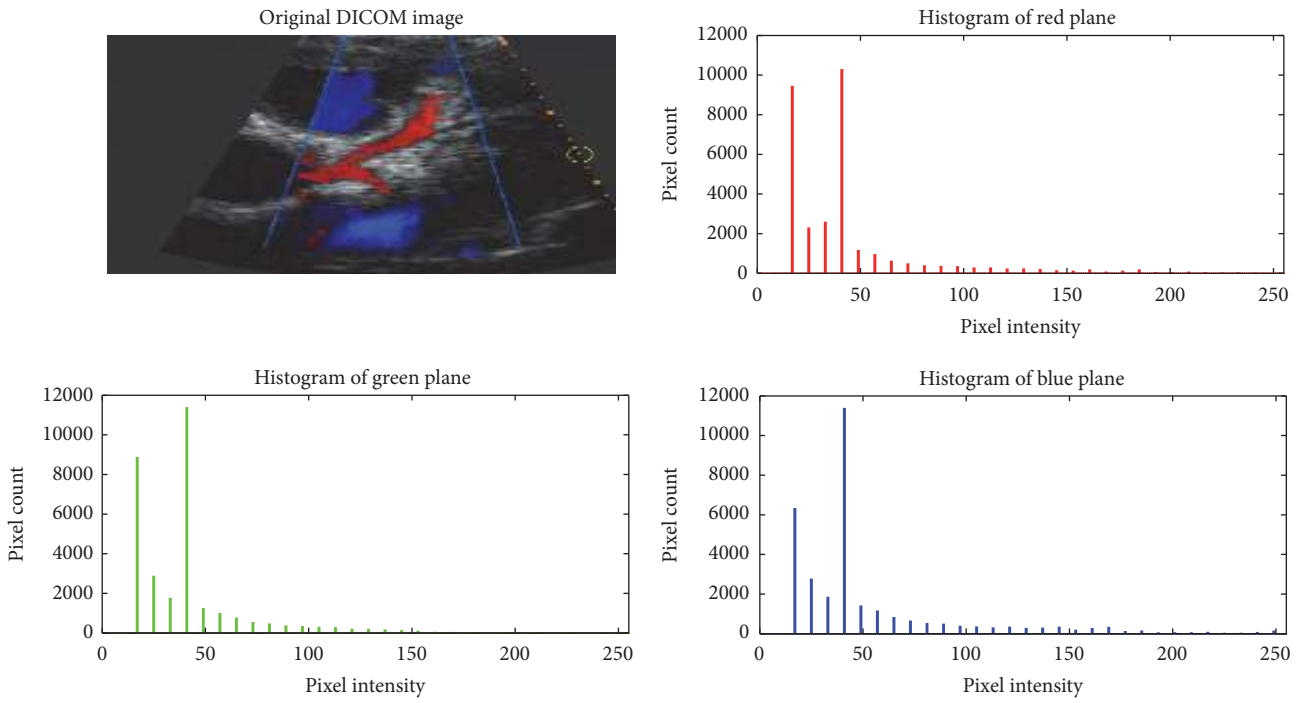

FIGURE 7: (a) Histograms of red, green and blue planes of plain DICOM image sample: D_6. (b) Histograms of red, green, and blue planes of encrypted DICOM image sample: ED_6.

results for primes greater than 223. Hence the choice of prime can range from 223 to infinity.

(ii) Parameters of Henon map (P_1):

(a) "α" can be in the range of 1.16 to 1.41,
(b) "β" can be in the range of 0.2 to 0.3,
(c) "x_0" can be in the range of −1 to 1,
(d) "y_0" can be in the range of −0.35 to 0.35.

(iii) The number of iterations after which the first value is to be picked for generating keys (P_3):

"P_3" can be any integer value greater than 300.

Table 4: NPCR and UACI of encrypted image samples with slightly different keys.

DICOM images	Encrypted DICOM images	Key values	NPCR (in %)	UACI (in %)
D_1	ED_1	$\{p = 257, \alpha = 1.4, \beta = 0.3, x_0 = 0.6313, y_0 = 0.1894\}$	99.624	33.4712
	E′D_1	$\{p = 257, \alpha = 1.4, \beta = 0.3, x_0 = 0.63130000000009, y_0 = 0.18940000000009\}$		
D_2	ED_2	$\{p = 271, \alpha = 1.4, \beta = 0.3, x_0 = 0.6313, y_0 = 0.1894\}$	99.1382	33.6820
	E′D_2	$\{p = 271, \alpha = 1.4, \beta = 0.3, x_0 = 0.63130000000009, y_0 = 0.18940000000009\}$		
D_3	ED_3	$\{p = 241, \alpha = 1.4, \beta = 0.3, x_0 = 0.6313, y_0 = 0.1894\}$	99.5777	33.0944
	E′D_3	$\{p = 241, \alpha = 1.4, \beta = 0.3, x_0 = 0.63130000000009, y_0 = 0.18940000000009\}$		
D_4	ED_4	$\{p = 271, \alpha = 1.4, \beta = 0.3, x_0 = 0.6313, y_0 = 0.1894\}$	99.236	33.2985
	E′D_4	$\{p = 271, \alpha = 1.4, \beta = 0.3, x_0 = 0.63130000000009, y_0 = 0.18940000000009\}$		
D_5	ED_5	$\{p = 269, \alpha = 1.4, \beta = 0.3, x_0 = 0.6313, y_0 = 0.1894\}$	99.6076	33.9995
	E′D_5	$\{p = 269, \alpha = 1.4, \beta = 0.3, x_0 = 0.63130000000009, y_0 = 0.18940000000009\}$		
D_6	ED_6	$\{p = 263, \alpha = 1.4, \beta = 0.3, x_0 = 0.6313, y_0 = 0.1894\}$	99.5822	33.5912
	E′D_6	$\{p = 263, \alpha = 1.4, \beta = 0.3, x_0 = 0.63130000000009, y_0 = 0.18940000000009\}$		
D_7	ED_7	$\{p = 997, \alpha = 1.4, \beta = 0.3, x_0 = 0.6313, y_0 = 0.1894\}$	99.8809	33.4301
	E′D_7	$\{p = 997, \alpha = 1.4, \beta = 0.3, x_0 = 0.63130000000009, y_0 = 0.18940000000009\}$		
D_8	ED_8	$\{p = 967, \alpha = 1.4, \beta = 0.3, x_0 = 0.6313, y_0 = 0.1894\}$	99.8947	33.2369
	E′D_8	$\{p = 997, \alpha = 1.4, \beta = 0.3, x_0 = 0.63130000000009, y_0 = 0.18940000000009\}$		
D_9	ED_9	$\{p = 811, \alpha = 1.4, \beta = 0.3, x_0 = 0.6313, y_0 = 0.1894\}$	99.8596	33.4612
	E′D_9	$\{p = 811, \alpha = 1.4, \beta = 0.3, x_0 = 0.63130000000009, y_0 = 0.18940000000009\}$		

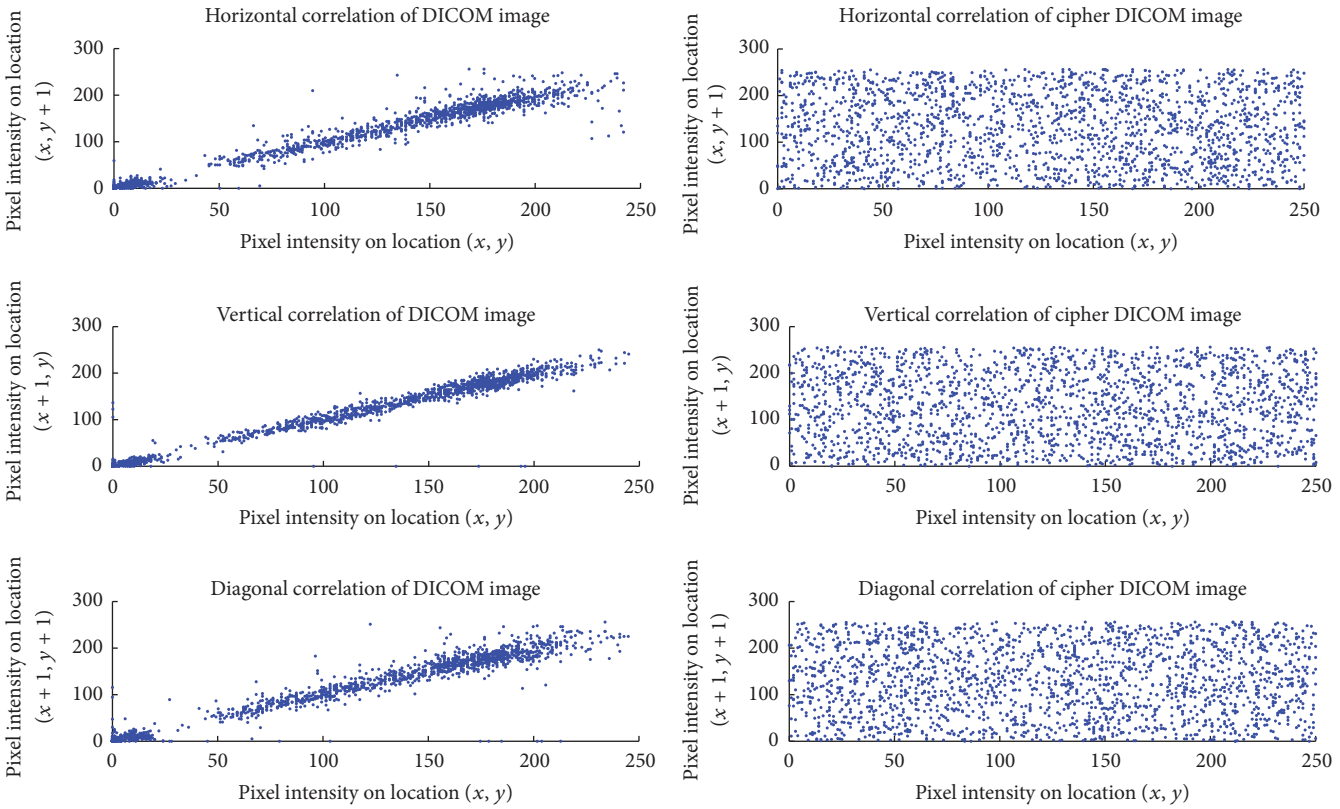

Figure 8: Correlation distributions of plain and encrypted DICOM image sample: D_3 and ED_3.

Figure 9: Encrypted DICOM image of sample D_3 with slightly differing keys.

Figure 10: Differences in encrypted images produced by slightly differing keys.

(iv) The skip value to be maintained for picking successive values (P_4):

"P_4" can be any integer value between 80 to 1000.

(v) Increment value of seed for generating different permutation key arrays (P_5).

Even small variations from one tenth to one millionth value of seed values of Henon map as specified in "P_5" generate diverging keys.

Decryption of the cipher image is possible only if the exact values of all the parameters of the keys are known. The probability of finding the accurate values of all the parameters is close to zero since the combined key space of all the parameters is extremely large. Hence it could be confirmed that launching brute force attack is computationally infeasible on the proposed image encryption algorithm.

4.4. Key Sensitivity Analysis. Any efficient cryptosystem should be highly sensitive to keys; that is, cipher images generated on encryption with slightly varying keys should be completely different from each other. The proposed methodology has been examined for key sensitivity with encryption of image sample (D_3) with three slightly different encryption keys as follows:

Key 1: $\{p = 251, \alpha = 1.4, \beta = 0.3, x_0 = 0.6313, y_0 = 0.1894\}$

Key 2: $\{p = 251, \alpha = 1.4, \beta = 0.3, x_0 = 0.631300000009, y_0 = 0.189400000009\}$

Key 3: $\{p = 251, \alpha = 1.4, \beta = 0.3, x_0 = 0.631300000001, y_0 = 0.189400000001\}$

The three keys differ only in the seed values. The results of encryption are shown in Figure 9. Figure 10 represents the deviation between the encrypted images which is measured by computing of pixel differences between the cipher images. It can be inferred that the proposed system exhibits good avalanche effect as even a minor change in inputs has produced significantly differing cipher images.

The cipher images must be highly sensitive to the keys. The cipher images should not be correctly decrypted, even if there is a slight difference in the key. The results of an attempt to decrypt a cipher image with slightly different keys are illustrated in Figure 11 which confirms that the proposed idea is highly sensitive to keys thereby ensuring its security. It could also be inferred that decryption with the correct key has produced no visual degradation because of integer arithmetic involved in modular exponentiation during key generation.

Table 5: PSNR of DICOM and its encrypted samples.

DICOM samples	PSNR (in dB)
D_1	5.9770
D_2	6.9877
D_3	7.1099
D_4	8.2950
D_5	6.8298
D_6	5.2229

4.5. Peak Signal to Noise Ratio. Peak signal to noise ratio can be used to quantify the depth of degradation introduced upon encryption. The higher the amount of degradation, the more strong the crypto system. The PSNR computed for various DICOM image samples are as shown in Table 5. It could be inferred that the PSNR values of original and encrypted samples are well within the satisfactory limit of 11 dB.

Decrypted ED_3 with key 3 | Decrypted ED_3 with key 2 | Decrypted ED_3 with key 1

Figure 11: Decryption by slightly differing keys.

Table 6: Performance comparison.

	Horizontal correlation	Vertical correlation	Diagonal correlation	NPCR (in %)	UACI (in %)	Entropy
Ravichandran et al. [16]	−0.0519	−0.0385	0.00046	99.996	33.37	7.9992
Praveenkumar et al. [15]	0.0033	−0.0033	0.0117	99.62	33.45	7.9975
Zhang et al. [20]	0.0193	−0.0154	0.0032	NA	NA	NA
Chen et al. [21]	0.0122	−0.0061	−0.0197	NA	NA	7.993
Fu et al. [13]	0.0037	0.0018	−0.0011	99.61	33.45	7.9992
Proposed work (Average)	0.0030	0.0017	0.0010	99.6001	33.4738	7.9976

Table 7: Computational time analysis.

DICOM samples	Size	Time taken (in sec)
D_1	512 × 512	4.5477
D_2	512 × 512	4.5204
D_3	512 × 512	4.5020
D_4	512 × 512	4.3977
D_5	480 × 640 × 3	4.5290
D_6	120 × 250 × 3	4.0818

4.6. Comparison with Existing Work. The performance of the proposed algorithm has been compared with the existing works [13, 15, 16, 20, 21] in the literature and is reported in Table 6. It could be inferred that the security level of the proposed algorithm is on par with the works reported in the literature but with significant reduction in computational requirements. The computational time taken for encryption is significantly reduced as the design has reduced number of rounds and iterations in encryption/decryption. In order to speed up the process of encryption/decryption for real time applications, the key generation and key permutation can be carried out as a preprocessing step. The time taken for key generation and encryption for different sized image samples is presented in Table 7.

5. Conclusion and Future Work

This research work employs the concept of modular exponentiation and Henon maps for securing DICOM images. The use of modular exponentiation of primitive roots of prime over its residual elements generates session keys which involves only integer arithmetic and is free from round off errors. Henon maps are used for permuting the keys to be used in encryption of subimages. Permutation of keys introduces an additional level of randomness and thus enhances the security of the system. Experimental results confirm the strength and resistivity of the algorithm again, statistical and differential crypt analysis, brute force attack, and key sensitivity analysis. Reduced number of rounds and operations of encryption/decryption results in significant reduction in time in comparison with text based crypto systems. Future work includes the performance analysis of the proposed system in mobile and cloud environments. The feasibility of enabling parallel encryption in the proposed design using MapReduce framework in Hadoop environment can also be tested.

Competing Interests

The authors declare that there is no conflict of interests regarding publication of the paper

References

[1] S. V. Sathyanarayana, M. Aswatha Kumar, and K. N. Haribhat, "Symmetric key Image Encryption Scheme with key sequences derived from random sequence of cyclic elliptic curve points," *International Journal of Network Security*, vol. 12, no. 3, pp. 137–150, 2013.

[2] C.-H. Yuen and K.-W. Wong, "A chaos-based joint image compression and encryption scheme using DCT and SHA-1," *Applied Soft Computing Journal*, vol. 11, no. 8, pp. 5092–5098, 2011.

[3] A. Al-Haj, G. Abandah, and N. Hussein, "Crypto-based algorithms for secured medical image transmission," *IET Information Security*, vol. 9, no. 6, pp. 365–373, 2015.

[4] A. Kannammal and S. Subha Rani, "Two level security for medical images using watermarking/encryption algorithms,"

International Journal of Imaging Systems and Technology, vol. 24, no. 1, pp. 111–120, 2014.

[5] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 6, pp. 1259–1284, 1998.

[6] N. Bourbakis and C. Alexopoulos, "Picture data encryption using scan patterns," *Pattern Recognition*, vol. 25, no. 6, pp. 567–581, 1992.

[7] J.-X. Chen, Z.-L. Zhu, C. Fu, H. Yu, and L.-B. Zhang, "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 3, pp. 846–860, 2015.

[8] G. Zhou, D. Zhang, Y. Liu, Y. Yuan, and Q. Liu, "A novel image encryption algorithm based on chaos and Line map," *Neurocomputing*, vol. 169, pp. 150–157, 2015.

[9] Q. Liu, P.-Y. Li, M.-C. Zhang, Y.-X. Sui, and H.-J. Yang, "A novel image encryption algorithm based on chaos maps with Markov properties," *Communications in Nonlinear Science and Numerical Simulation*, vol. 20, no. 2, pp. 506–515, 2015.

[10] M. A. Murillo-Escobar, C. Cruz-Hernández, F. Abundiz-Pérez, R. M. López-Gutiérrez, and O. R. Acosta Del Campo, "A RGB image encryption algorithm based on total plain image characteristics and chaos," *Signal Processing*, vol. 109, pp. 119–131, 2015.

[11] W. Zhang, H. Yu, Y.-L. Zhao, and Z.-L. Zhu, "Image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 118, pp. 36–50, 2016.

[12] J. Hu and F. Han, "A pixel-based scrambling scheme for digital medical images protection," *Journal of Network and Computer Applications*, vol. 32, no. 4, pp. 788–794, 2009.

[13] C. Fu, W.-H. Meng, Y.-F. Zhan et al., "An efficient and secure medical image protection scheme based on chaotic maps," *Computers in Biology and Medicine*, vol. 43, no. 8, pp. 1000–1010, 2013.

[14] G. Liu, J. Li, and H. Liu, "Chaos-based color pathological image encryption scheme using one-time keys," *Computers in Biology and Medicine*, vol. 45, no. 1, pp. 111–117, 2014.

[15] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. Balaguru Rayappan, "Medical data sheet in safe havens—a tri-layer cryptic solution," *Computers in Biology and Medicine*, vol. 62, pp. 264–276, 2015.

[16] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, 2016.

[17] E. Yavuz, R. Yazici, M. C. Kasapbaşi, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Computers and Electrical Engineering*, vol. 54, pp. 471–483, 2014.

[18] J. B. Lima, F. Madeiro, and F. J. R. Sales, "Encryption of medical images based on the cosine number transform," *Signal Processing: Image Communication*, vol. 35, pp. 1–8, 2015.

[19] M. Dzwonkowski, M. Papaj, and R. Rykaczewski, "A new quaternion-based encryption method of DICOM images," *IEEE Transactions on Image Processing*, vol. 24, no. 11, pp. 4614–4622, 2015.

[20] S. Zhang, T. Gao, and L. Gao, "A novel encryption frame for medical image with watermark based on hyperchaotic system," *Mathematical Problems in Engineering*, vol. 2014, Article ID 240749, 11 pages, 2014.

[21] J.-x. Chen, Z.-l. Zhu, C. Fu, L.-b. Zhang, and Y. Zhang, "An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach," *Communications in Nonlinear Science and Numerical Simulation*, vol. 23, no. 1-3, pp. 294–310, 2015.

[22] http://mathworld.wolfram.com/PrimitiveRoot.html.

[23] W. Stallings, *Cryptography and Network Security*, Prentice Hall, 5th edition, 2011.

[24] http://mathworld.wolfram.com/DiscreteLogarithm.html.

[25] R. Ramasamy, A. P. Muniyandi, and I. Devi, "A new algorithm for encryption/decryption for field applications," *Computer Standards & Interfaces*, vol. 31, no. 6, pp. 1069–1072, 2009.

[26] J. Chandrasekaran and T. S. Jayaraman, "A fast and secure image encryption algorithm using number theoretic transforms and discrete logarithms," in *Proceedings of the IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES '15)*, Kerala, India, February 2015.

[27] M. Suneel, "Cryptographic pseudo-random sequences from the chaotic Hénon map," *Sadhana*, vol. 34, no. 5, pp. 689–701, 2009.

[28] F. Zheng, X.-J. Tian, J.-Y. Song, and X.-Y. Li, "Pseudo-random sequence generator based on the generalized Henon map," *Journal of China Universities of Posts and Telecommunications*, vol. 15, no. 3, pp. 64–68, 2008.

[29] M. Usama, M. K. Khan, K. Alghathbar, and C. Lee, "Chaos-based secure satellite imagery cryptosystem," *Computers and Mathematics with Applications*, vol. 60, no. 2, pp. 326–337, 2010.

[30] J. Chandrasekaran and S. J. Thiruvengadam, "Ensemble of chaotic and naive approaches for performance enhancement in video encryption," *The Scientific World Journal*, vol. 2015, Article ID 458272, 11 pages, 2015.

[31] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications*, vol. 2, pp. 31–38, 2011.