Hindawi
Modelling and Simulation in Engineering
Volume 2017, Article ID 7470204, 12 pages
https://doi.org/10.1155/2017/7470204

*Research Article*

# A Fast Enhanced Secure Image Chaotic Cryptosystem Based on Hybrid Chaotic Magic Transform

**Srinivas Koppu[1] and V. Madhu Viswanatham[2]**

[1]*School of Information Technology and Engineering, VIT University, Tamil Nadu, India*
[2]*School of Computer Science and Engineering, VIT University, Tamil Nadu, India*

Correspondence should be addressed to V. Madhu Viswanatham; vmadhuviswanatham@vit.ac.in

Received 25 August 2016; Revised 26 October 2016; Accepted 20 November 2016; Published 4 January 2017

Academic Editor: Aiguo Song



An enhanced secure image chaotic cryptosystem has been proposed based on hybrid CMT-Lanczos algorithm. We have achieved fast encryption and decryption along with privacy of images. The pseudorandom generator has been used along with Lanczos algorithm to generate root characteristics and eigenvectors. Using hybrid CMT image, pixels are shuffled to accomplish excellent randomness. Compared with existing methods, the proposed method had more robustness to various attacks: brute-force attack, known cipher plaintext, chosen-plaintext, security key space, key sensitivity, correlation analysis and information entropy, and differential attacks. Simulation results show that the proposed methods give better result in protecting images with low-time complexity.

## 1. Introduction

With the rapid growth and application demand of multimedia data in open channels including Internet and wireless networks in recent decades, image security is one of the essential frameworks to provide the security for image transmission over the communication channels. Multimedia data have become one of the most popular media types and are now used extensively in various fields such as politics, economics, defense, and education. Then, because of data transmission of open channels, image transmission security is subject to potential attacks. Also exchange of medical image data has become a more important aspect of security in recent decades. For instance, radiological and surgical radios are more popular in the telemedicine. Patient medical reports are needed to be carried from one medical data storage system to another for better treatment. So if we do not have privacy for data while transmission, this may cause wrong diagnosis. When we are sharing the patient information over wireless or wired communication networks, the security is more prominent. General security services are confidentiality, authentication, and integrity [1]. There are security fields available to provide security for image such as image steganography, watermarking, cryptography, and hybrid algorithms. Image encryption and decryption techniques based on public cryptographic and private cryptographic methods are not optimized for medical image security due to intrinsic characters: being time-consuming and recovering image in the original image, due to more pixels replication, strong pixel relation between adjacent pixels, and so forth. DES, AES, RSA, IDEA, RC2, RC4, GOST, and SAFEN may not good for encryption and decryption in fast communication applications because they may require more computational resources in the form of hardware and software. DES, AES, and IDEA had low-level efficiency in encryption and decryption process. However, these algorithms are more useful in text based encryption. Telemedicine had benefits: restorative medical research, remote special clinical diagnosis, unexpected incidents handling in time, patient information on immediate demand, and enhancing the communication between partners in health care systems.

## 2. Literature Survey

The work by [2] employs a 3-dimensional cat map, to shuffle the image pixels and uses the logistic map to diffuse the image.

In this paper, the authors addressed attacks such as statistical and differential attacks. Spatial permutation does not fit for pixel value modification in the image, but it makes changes in pixel positions.

Reference [3] applied a point-based interaction methods effectively and feasibly to generate tangible textures from static images and implemented a haptic virtual environment based on the OpenGL and PHANTOM Omni haptic device for the size of input image $128 \times 128$. However, the proposed work did not concentrate on security issues.

The work by [4] explains a technique for image authentication, based on adding signal-dependent noise, while taking input image hidden noise was embedded into an image based on film grain noise model. Later, original image and noise are extracted for authentication purpose. Here, few attacks are addressed such as robust against content-preserving modifications, additive Gaussian noise, local denoising, and detecting of malicious tampering. Future work of this paper is to design an efficient noise filter for estimating the original image statistics.

In [5], the authors presented a 2D image encryption method based on balanced 2-Dimensional Cellular Automata (2DCA). Random image and original image are encrypted by pseudorandom number generator with a kernel value. The advantages are as follows: fast in encryption, low-cost, and large-size secret key. Attacks addressed are such as statistical analysis, correlation coefficients, histogram analysis, confusion analysis, NPCR analysis, and information entropy.

In [6], a new image encryption has been proposed based on chaotic Josephus matrix, which extends the conventional Josephus traversing method. The future work of this paper can be applied to audio and video files for security purpose. In [7], Lorenz Chaotic Scheme (LCS) and Chen's hyperchaotic (CHC) method along with DNA sequences for an image encryption algorithm that can dynamically select eight types of DNA encryption rules and eight types of DNA addition and subtraction rules are used. LCS was used to generate the chaotic sequences to scramble the image. CHC and DNA are used for image diffusion. Here, key size is $8.4 \times 10^{128}$. However, authors have not addressed security issues: histogram analysis, pixel correlation, chart test, and entropy. In [8], a new cross-layer unequal error protection (UEP) is introduced which reduces image encryption overhead and controls the image bit stream structure to deliver the image data in wireless sensor networks. This paper assures energy competence and image security and quality over the image transmission in wireless network channels. But, the authors did not express their works on security issues such as brute-force attack, key space analysis, histogram analysis, pixel correlation, chaotic test, and entropy.

Reference [9] concentrates on open source EHRs along with parameters such as strengths, weaknesses, opportunities, threats of Electronic Health Record (EHR) over open source EHRs, and security services which are also not addressed. The work explained by [10] uses chaos mapping function to improve sensitivity of the initial state, pixel position changed by iterative function, and XOR operations for diffusion. This paper combines chaos theory and iterative equations based balanced pixel algorithm to decide the number of iterations for the image encryption and resultant low speed in image encryption. The authors addressed in [11] tree proxy-based and service-oriented access control system (TPSACS) to fix secure detection of multimedia events in an online environment. 1000 objects set as event block have been proposed to fix the scale robust illustration issue in online services. The future work can be applied in action recognition. However, security services are not addressed.

Reference [12] proposed Tangent-Delay Ellipse Reflecting Cavity-Map System (TD-ERC), wavelet neural networks (WNN), and XOR operations on binary data that achieves cipher image. Here, addressed attacks are as follows: key size being 10195, histogram analysis, correlation analysis, and differential analysis. The proposed system can be applied to provide security for information. Reference [13] introduced symmetric chaotic economic map (CEM) with key space 1084, the entropy that closes to ideal value 8, and low coefficient correlation that closes to 0. Initially, CEM generated a chaotic sequence with fraction decimal values to integers. Addressed attacks are key sensitivity analysis, correlation analysis, and analysis of information entropy.

In 2016, Kanso and Ghebleh [14] selected chaotic cat map algorithm used for medical image security applications with $r$ rounds and each round has two phases: shuffling and masking, applied for block level as well as full image. The masking phase of each round uses a pseudorandom matrix of the same size as the input image to increase processing speed. Statistical cryptanalytic attacks such as key search and differential attacks are analyzed for medical image robustness. Same encryption and decryption technique are applied for ROI as well as for full image and also achieved the same level of security in ROI and full image. Analyzed brute-force attack by considering key space is large. However, the author has not addressed decrypted image quality and information entropy.

In [15], 2-Dimensional Chaotic Map (2CDM) has been converted to 3-dimensional cat map (3DCM) for fast design and secure private image encryption with 128 bits. Generally, the good cipher image will have less correlation among pixels. Here, analyzed attacks are as follows: statistical and differential attacks. However, brute-force and correlation of image attacks are not addressed. This one is suitable for real-time Internet image security and telemedicine.

In [16], a novel image encryption Using 3-dimensional Arnold cat map defends brute-force attack, chosen-plaintext attack, statistical attack, and also image noise: salt and pepper noise, Gaussian noise, and low-pass filter attacks. Time taken for encryption and decryption process for Lenna image (with $256 \times 256$ sizes) was 0.007 and 0.012 seconds, respectively. But, chi-square test, pixels correlation, key space, and entropy are not addressed.

Reference [17] proposed pseudorandom permutation–substitution method for image encryption based on lossless symmetric block cipher. The main design of proposed method was to provide security for color image. Computation speed of encryption process has been increased by directly shuffling row by row and column by column instead of pixel by pixel. Security parameters are considered in the proposed method: the histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, and key

space analysis. Further, this method can be used in video encryption and grayscale images.

In [18], chaos based image encryption by using stream cipher and pseudorandom generator is based on cascade of chaotic maps. DES, AES, RSA, and IDEA may not be good for encryption in fast communication applications because they may require more computational resources in the form of hardware and software. In this method, initially, input image converts into binary bit stream and is masked with pseudorandom key generator; then encryption image was constructed. For fast pseudorandom key generator, finite precision exemplification and fixed point arithmetic are espoused. Resisted statistical attacks, color histogram for RGB Lenna image, correlation of adjacent pixels in vertical, horizontal, and diagonal directions, and brute-force attack are addressed by taking 192-bit key.

In [19], Region of Interest (ROI) is used as water marking and encrypted by linear feed backshift register using stream cipher mode with 64-bit private and public key, embedded into medical image by spread spectrum method. Second-time encryption had been done by Diffie-Hellman algorithm. In this paper, the authors have used medical images modalities: MRI, CT-scan, and X-ray. However, these approaches have a drawback as they could not recover original medical image.

In [20], high security visual encryption algorithms had been proposed with two-level encryption strategies: in first level, image pixels had been shuffled with row-wise and column-wise permutation based on tent map so that it affects visual perception. In second level, diffusion was applied for shuffled image with 4D hyperchaotic Chen systems. Pixel correlation was truncated and procured privacy for patient image with tent maps. Hyperchaotic security system had dynamic features compared with other conventional chaotic methods. Image security measurements considered are as follows: statistical analysis, chi-square test, pixels correlation, key space, and entropy. In this paper, authors used input image modalities: MRI images with $568 \times 568$, CT-scan abdomen image with $512 \times 512$, and X-ray angiography with $1024 \times 1024$ sizes for experiments and they suffered from low speed process.

In [21], DICOM image format is used to achieve security over Internet transmission. DICOM has two attributes: header attribute and pixel data. With help of digital signature, authenticity and integrity had been obtained on pixel data for basic level. However, confidentiality of the pixel data has not been addressed in confidentiality profile in DICOM. Advanced Encryption Standard-Galois Counter Mode (AES-GCM), the Whirlpool hash function, and the Elliptic Curve Digital Signature Algorithm provide confidentiality, authenticity, and integrity for header and pixel values of DICOM. With lack of confidentiality, sometimes, plain image will get interfered, condensed, and edited. With lack of digital signature, anyone may edit an image by using tools which may lead to improper result in diagnostic process for medical experts. Limitations in [21] are addressed by Kobayashi et al. [22] scheme. Data pixel confidentiality is achieved by using encryption standard in DICOM header. However, keys are stored in DICOM header without encryption, so it may not give confidentiality assurance. Kobayashi et al. scheme does not provide confidentiality, authenticity, and integrity for the DICOM header data. However, this approach takes more time for encryption and decryption on large-size IVUS images.

In [23], authenticity and integrity (AIDM) had four modules: preprocessing module, image hashing module, data encryption, and data embedding. RSAREF free tool kit was used for data encryption. Future work of the proposed algorithm is to improve the speed in encryption-decryption process and key management. Digital signature and MD5 are used for verification authenticity and integrity. [24] Symmetric encryption algorithms are used for electronic patient records (EPR). Bipolar TER Multiple Base was developed, which provides basic security services: integrity, authentication, and confidentiality. Time complexity is O (N). However, the proposed approach is suffering from lack of security.

In [25], AES-GCM is faster than conventional methods such as AES CBC + HMAC-SHA1, AES CBC + HMAC-SHA256, and RC4-SHA1. Whirlpool hash function is more powerful than MD5, SHA-1, SHA-224, SHA-256, and SHA-384. SHA-512 and Whirlpool had the same strengths in security. [1] Matrix Array symmetric-Key Encryption (MASK) was applied for image encryption based on a private key and it is faster than AES algorithm. 128 bits are used as key size and image block size. But, key size is less and leads to brute-force attack. In [26], McEliece public cryptosystems and Sequitur compression technique are used for medical images, yielding better efficiency than RSA cryptosystems. Authenticated image encryption was achieved without digital signature. McEliece public cryptosystem has better adeptness and security than RSA algorithm. However, the used methods did not analyze statistical and differential attacks, brute-force, and correlation.

Image is encrypted with secret key and secret key encrypted with public key technique [27]. The major issue is key distribution at the same time we have to transfer encrypted image and encrypted key over a network. In this paper, hybrid method is proposed based on cryptosystems and DCT water marking method. The image encryption has been done with either stream or block cipher. Sometimes block cipher is not feasible due to lack of robustness and homogenous regions. Stream ciphers are robust to adequate JPEG compression noise. Stream cipher examples are: RC4, one-time pad or Vernam cipher, and so forth. Result obtained with PSNR is 43.71 dB.

In [28], used digital envelope (DE), digital signature, and encrypted patient information from DICOM header are embedded as invisible water mark in image for authentication, confidentiality, integrity in atmosphere of picture archiving and communication systems (PACS). DE processing has taken more time to be embedded in image and DE is very expensive because of stream cipher encryption. However, this method did not concentrate on DICOM header security. Reference [29] proposed new 2D-sine logistic modulation maps (2D-SLMM) based on logistic and sine maps with efficient image pixel shuffling algorithm known as Chaotic Magic Transform (CMT) to derive random pixel property encryption image. In digital images, usually high redundancy data will be there, due to high correlation of

pixels, to break these correlations CMT used. CMT changes pixels values in random position. 2D chaotic maps have good performance in terms of generating chaotic sequence than 1D chaotic map, but they need relatively complex hardware structure and cost. CMT performance is better at shuffling than early chaotic maps. Chaotic performance is analyzed by the following parameters: trajectory, Lyapunov exponent, and Lyapunov dimension and Kolmogorov entropy surviving chaotic maps are broadly classified into 1D chaotic maps and high-dimensional maps. 1D map has one variable and few attributes with simple design structure, for example, logistic, sine, Gaussian, and tent maps. CMT-IEA is based on asymmetric cryptosystems. HD chaotic maps shall have minimum of two attributes with complex structure which gives more chaotic enactment, for example, Henon map, Lorenz map systems, and Chee-Lee systems.

Reference [30] used chaotic schema with linear congruence based on pseudorandom numbers generation, that is, coupling of chaotic function with XOR operations during encryption process to achieve randomness in cipher image and large key space to resist brute-force attack. If the image has high correlation with adjacent pixel values, they need to increase the quality of cipher image during encryption and decryption process. In order to address the high correlation problem, we need to mix and change the values of pixels simultaneously. However, authors did not concentrate on floating point values while doing encryption and decryption process.

In [31], chaos based cryptosystem was proposed in 1989. Chaos properties are as follows: sensitive dependence, initial conditions and system parameters, pseudorandom property, nonperiodicity, and topological transitivity. In this system, plan image is shuffled by logistic 1D map and encrypted with hyperchaotic systems which is based on Chen's chaotic system. Brute-force attack was considered. But, this paper suffers from statistical attack, histogram metric, entropy, and chi-square test. Most of the chaos based security techniques suffered from chosen-plaintext attack [32]. Based on three 1D chaotic methods, logistic, tent, and sine map, utilizing the same arrangement of security keys, the proposed method has the capacity to produce a totally diverse encrypted image every time when it is applied to the original image.

In [33], new parametric switching chaotic system using sine map and tent map is controlled by logistic map. The output of the logistic map decides to choose either the sine map or the tent map as a generator to deliver PSCS's output bit sequence. Some attacks addressed are as follows: brute-force attack, security key space, key sensitivity, correlation analysis and information entropy, differential attacks, Gaussian noise, salt and pepper noise, and so forth. However, chosen-plaintext and cipher plaintext were not addressed.

In [34], C.-J. Cheng and C.-B. Cheng proposed asymmetric image encryption method based on unified chaotic system, Lyapunov stability theory, and a cellular neural network-adaptive controller with its parameter update law. In this paper, the authors considered key space analysis, a sensitivity, test and statistical analysis. In [33, 34], chosen-plaintext and cipher plaintext were not addressed. However, simulations results are not shown in real-time applications.

In [35], chaotic map lattices (CML) had weakness: conversation of floating values into pixel value which leads to data loss in image. Improved CML was proposed by Jasteazebski and Kotulski based on CBC method but lacks from various security services such as noise attacks, differential attacks, and statistical attacks. Image encryption conceals some particular issues, for example, huge size of image pixels and redundancy. In some cases, the value of pixel in encryption process will depend on the neighboured pixel value, that is, pixels blocks. However, the key size is small, which may give brute-force attack. In this paper, the authors considered time complexity, space complexity, noise attacks, differential attacks, statistical attacks, and so forth. In medical image, encryption has been developed based on modular arithmetic operator [36]. In [37], the proposed technique has four differential chaotic systems, yielding image confusion. In [38], chaos based image encryption has been applied for bit planes based on pseudorandom binary number generator. The authors addressed speed and time issues. However, it lacks various security services such as noise attacks, differential attacks, and statistical attacks.

Baker map has been proposed [39] to represent real number while doing encryption and decryption process. Block level image encryption based on self-invertible matrices with two mere different keys [40]. Color images are divided into the three subband array of images: red, green, and blue are jumbled by Fibonacci Transformation (FT) and encrypted with hybrid cellular automata [41]. Medical image security is using Game of Life (GoL) and DNA sequence in DWT and spatial domain [42]. However, noise attacks, chosen-plaintext attacks, differential attacks, and statistical attacks are not addressed.

*2.1. Review.* Nowadays, most of the researchers have proposed a cryptographic system based on spatial and frequency domain image encryption methods which are not suitable for efficient image encryption. Chaotic research for an image encryption has a vital significance due to sensitive dependencies on initial conditions, system parameters, random behavior, nonperiodic and topological transitivity, and so forth; chaotic systems are used for image encryption that cannot be recognized by malicious users. Even if the attacker is intercepted, the image will not be identified so that it can transfer successfully over the Internet which guarantees the security of image communication. Most of the papers have not addressed security services such as pixel correlation, chosen-plaintext attack, cipher attack, histogram analysis, and entropy [24–28]. The proposed methods are described in Sections 3 and 4 along with experimental results. In Section 3, we have described hybrid CMT (HCMT) which gives more robustness for protecting the images from various attacks like key space analysis, key sensitivity, pixel correlation, histogram analysis, chosen-plaintext attack, cipher attack entropy, and noise analysis.

## 3. Proposed Method

The main idea to encrypt a plain image is to permutate the positions of pixels and to conceal the values of pixels via

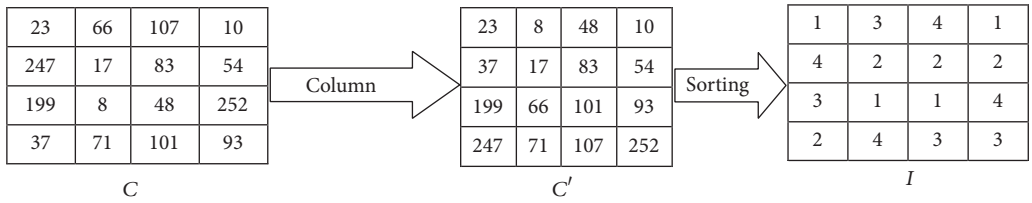


Figure 1: Generation of index matrix $I$.

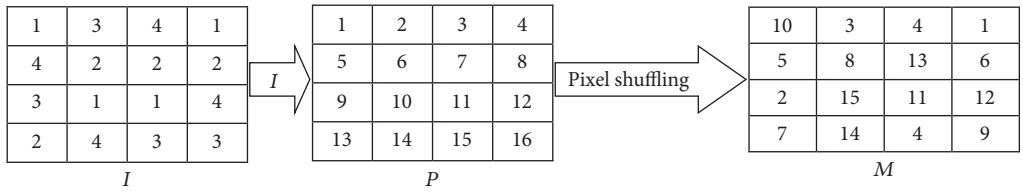


Figure 2: Pixel shuffling process.

different methods commonly. The two-dimensional feature of the image is employed in our encryption scheme compared with traditional encryption schemes. HCMT-EE is a lightweight image encryption method based on hybrid CMT with Lanczos algorithm. This shows better experimental results than [2, 6, 28, 42]. This paper presents Hybrid Chaotic Magic Transform (HCMT), liner congruential generator (LCG), and Lanczos algorithm to build a fast enhanced secure image chaotic cryptosystem. Input plain image $P$ is given to the HCMT as shown in Figure 3. HCMT has four steps: image column pixel values are sorted in ascending order and performed a row sorting. Pixel confusion phase achieves confusion property by randomly shuffling all pixel positions, obtaining confused image $M$.

The pseudorandom generator has used to generate key ($K$) with a size of host image $P$. This key ($K$) is given to the Lanczos algorithm to find the vector characteristics, which improve the key space and enhance security against the potential attacks. Cipher image ($Z$) is obtained by performing the multiplication operation between key vectors ($K$) and confused image ($M$).

*3.1. Hybrid Chaotic Magic Transform.* The aim of adapted encryption algorithm is to confuse the position of pixels for each block of the image based on the following steps:

Hybrid CMT (Chaotic Magic Transform) algorithm shuffles matrix $C$ [29]:

(1) Sort each column of $C$ in ascending order to obtain sorted matrix $C'$.

(2) Generate shuffled index matrix $I$ by connecting the pixels in $C$ with locations $(l(i,1),1),(l(i,2),2),(l(i,3),3),(l(i,4),4),\ldots,(l(i,n),n)$ with respect to CO.

(3) The pixel shuffling process is done by shuffling the pixels $P$ positions to the right in the clockwise directions.

HCMT used the right direction in the clockwise directions which enables shuffling image pixels quickly in both the row and column directions at the same time. Experimental results and security analysis show that the proposed HCMT-EE can encrypt different types of digital images with a high level of security with low-time complexity. Image pixel shifting has four steps: in the first iteration, we have shifted only one pixel position to the right. In the second iteration, we have shifted to two pixel positions in the right direction. In the third iteration, three pixel positions are shifted. In the fourth iteration, four pixel positions are shifted. The clockwise direction pixel shifting gave more image randomness than left clockwise shifting method with fast encryption speed.

(4) The resultant shuffled matrix is $M$.

The shuffling process is done by using the hybrid CMT algorithm; here, random chaotic matrix $C$ with size $m \times n$ is used to produce the shuffled index matrix $C'$ of size $m \times n$, where index matrix $I$ is defined by

$$I(i,j) = k \quad \text{for } C'(i,j) = C(k,j). \tag{1}$$

Let $O$ be the original image with size $m \times n$ and $M$ be the resultant shuffled image. The pixel shuffling process of the original image is defined by

$$F(P,I) = M. \tag{2}$$

Figures 1 and 2 are the example of CMT process. Figure 1 shows the generation of shuffled indexed matrix $I$ from chaotic matrix $C$. As shown in Figure 1, sorted matrix $C'$ is generated by sorting each column of chaotic matrix $C$ in ascending order. The index matrix shows the position of data $C'$ where they are permuted from chaotic matrix $C$. Figure 2 shows the pixel shuffling process where $P$ is the original image matrix and $M$ is the resultant shuffled matrix obtained from HCMT.

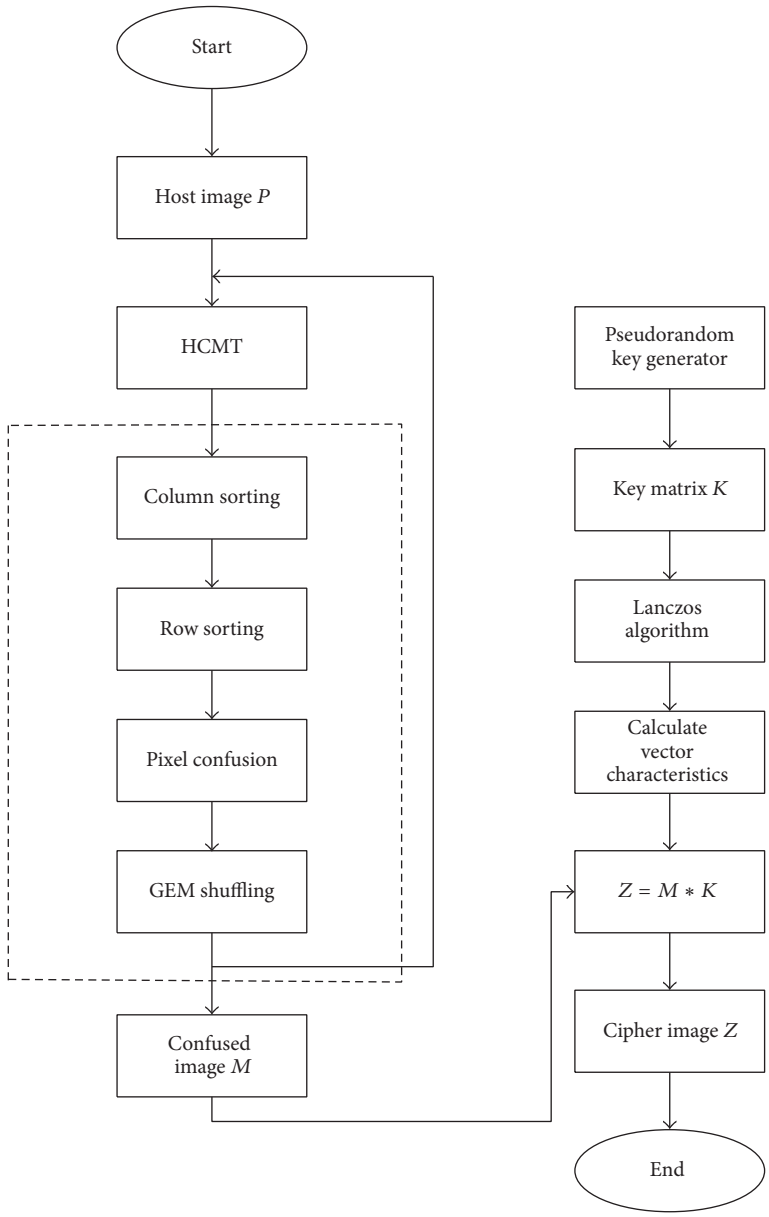


Figure 3: Proposed framework for image encryption.

*3.2. Pseudorandom Generator.* A linear congruential generator (LCG) is used to generate $m \times n$ pseudorandom numbers by using

$$X_{n+1} = (aX_n + b) \bmod m, \tag{3}$$

where $a$ and $b$ are integers and $m$ is the start value.

*3.3. Lanczos Algorithm [43].* The application of Lanczos algorithm is to perform normalization on large eigenvalues and eigenvectors. It was invented by Cornelius Lanczos [43]. We used $q_1$ as the random vector, matrix "$k$." $W_m$ is the characteristic roots and $\alpha_m$ is the characteristic vectors, for loops being used to calculate eigenvalues and eigenvectors. Lanczos algorithm is as follows:

Start:

Initialization:

$q_1$ = random vector with norm 1.

$q_0 = 0$

$\beta_1 = 0$

Step 1:

for $i = 1, 2, 3, \ldots m - 1$

Step 1-1: $w^1{}_i \leftarrow kq_i$

Step 1-2: $\alpha_i \leftarrow w^1{}_i \cdot q_i$

Step 1-3: $w_i \leftarrow w^1{}_i - \alpha_i q_i - \beta_i q_{i-1}$

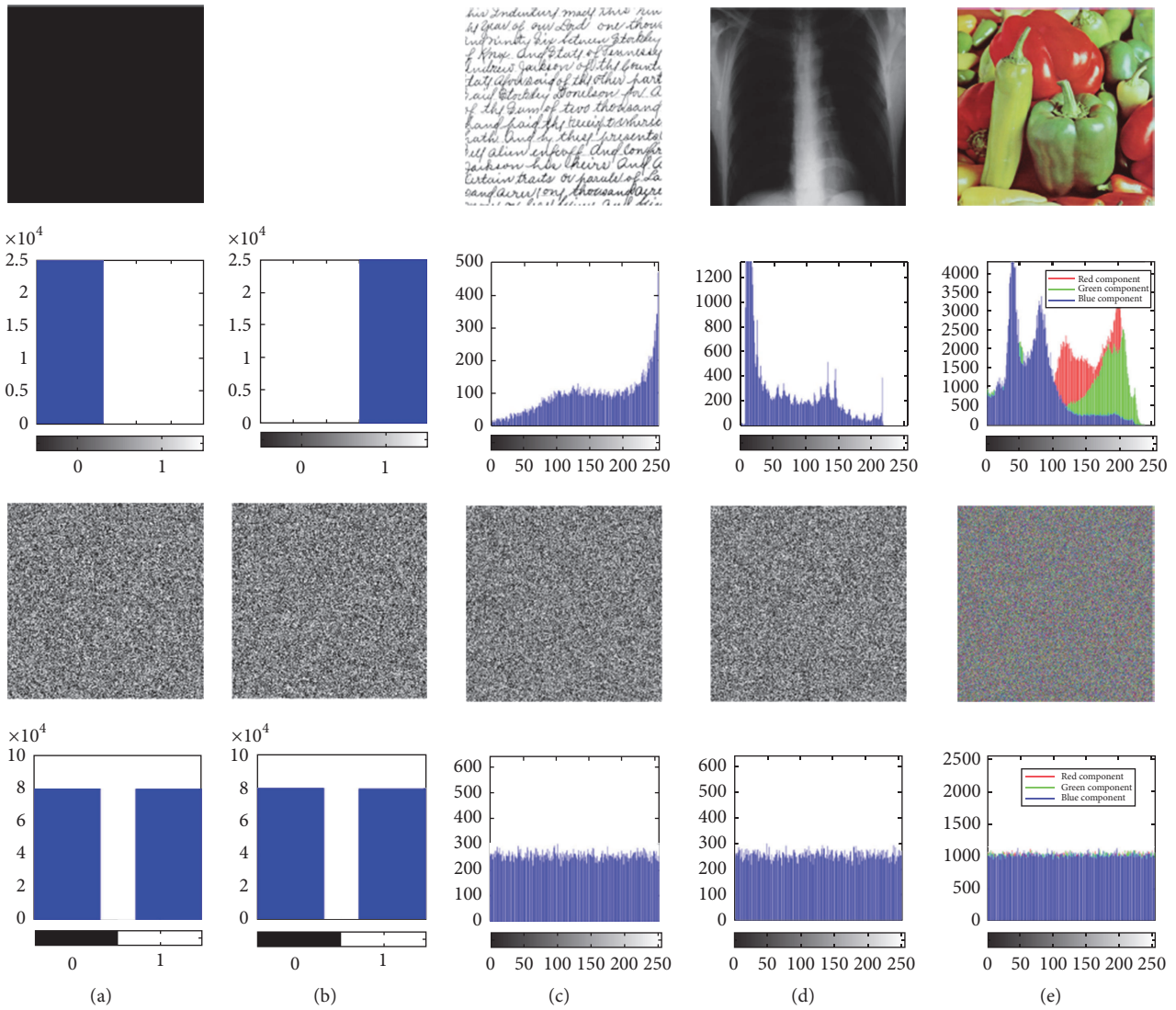


FIGURE 4: This figure shows simulation results of various images with their histograms: (a) all-zero pixel image; (b) all-one pixel image; (c) image with text; (d) medical image; (e) color image.

Step 1-4: $\beta_{i+1} \leftarrow \|w_i\|$
Step 1-5: $q_{i+1} \leftarrow w_i/\beta_{i+1}$

End for
Step 2: $q_m \leftarrow kq_m$
Step 3: $A_m \leftarrow w_m \cdot q_m$
Return

## 4. Simulation Results Analysis

The proposed method HCMT-EE has ephemeral encryption and decryption process for the USC-SPI "Miscellaneous" dataset. The experimental results are performed using MATLAB R2015a on a personal computer with a Intel® core™ i5-4200U CPU 1.60 GHz, 8 GB memory, and 500 GB hard-disk capacity and Microsoft Windows 8.1 64-bit operating system. Our simulation results are shown in Figures 4 and 5. Figures 4(a)–4(e) show histogram simulation results for image with all-zeros, all-ones image, image with text, medical image, and color image. HCMT-EE shows enhanced performance for image encryption by transforming arbitrary and homogeneous distribution to the entire image into cipher image or unpredictable form. Figures 5(a)–5(h) show the key space analysis: (a) Input plain image ($P$); (b) encrypted image $E_1 = \text{Enc}(P, K^1)$; (c) encrypted image $E_2 = \text{Enc}(P, K^2)$; (d) difference of encrypted image: $E_1 - E_2$; (e) decrypted image $D_1 = \text{Dec}(E_1, K^1)$; (f) decrypted image $D_2 = \text{Dec}(E_1, K^2)$; (g) decrypted image $D_3 = \text{Dec}(E_1, K^3)$; (h) difference of decrypted image: $E_2 - E_3$.

*4.1. Time Complexity.* HCMT-EE method has high speed encryption results compared to [29, 44–47]. All input images are tested using MATLAB from the USC-SIPI "Miscellaneous" dataset which is not random dataset. Table 1 shows the

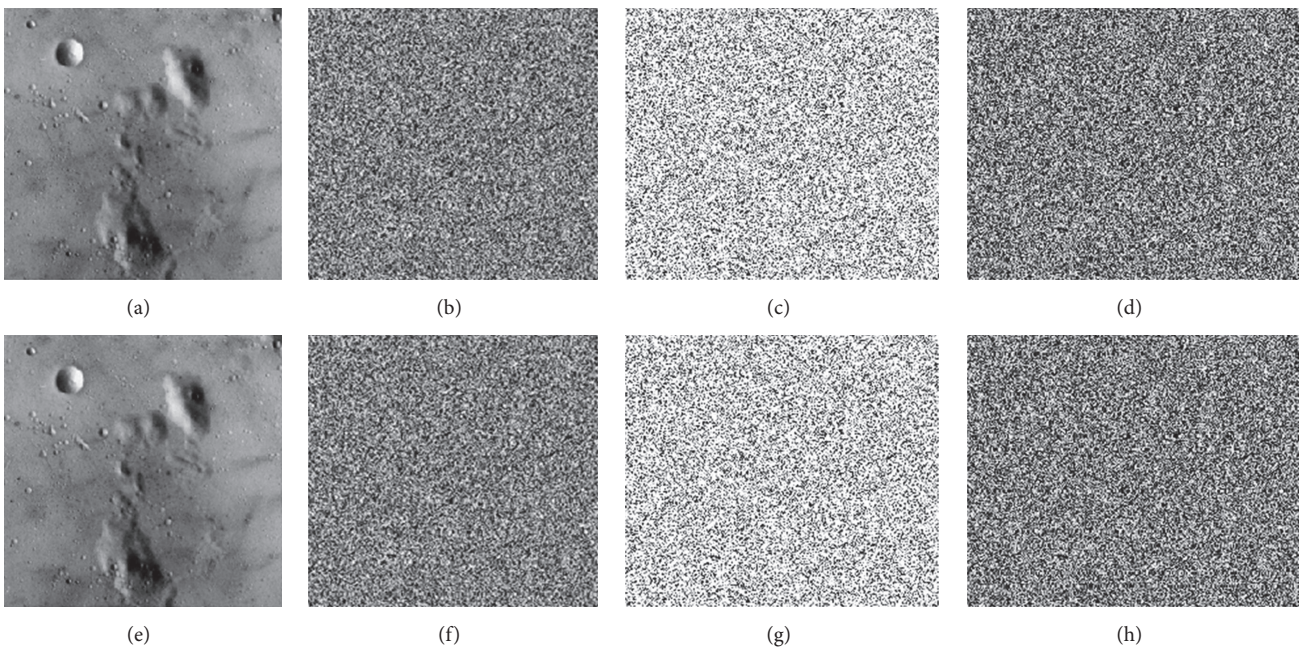


Figure 5: Key space analysis: (a) input plain image ($P$); (b) encrypted image $E_1 = \text{Enc}(P, K^1)$; (c) encrypted image $E_2 = \text{Enc}(P, K^2)$; (d) difference of encrypted image: $E_1 - E_2$; (e) decrypted image $D_1 = \text{Dec}(E_1, K^1)$; (f) decrypted image $D_2 = \text{Dec}(E_1, K^2)$; (g) decrypted image $D_3 = \text{Dec}(E_1, K^3)$; (h) difference of decrypted image: $E_2 - E_3$.

Table 1: Encryption speed (seconds) of various encryption algorithms.

| Image size | 64 × 64 | 128 × 128 | 256 × 256 | 512 × 512 | 1024 × 1024 |
|---|---|---|---|---|---|
| Wu et al.'s [47] | 0.2503 | 1.3412 | 5.6544 | 27.1702 | 109.9320 |
| Zhou et al.'s [32] | 0.0174 | 0.0549 | 0.1967 | 0.6547 | 3.2415 |
| Wu et al.'s [46] | 0.0161 | 0.0582 | 0.2368 | 0.8587 | 3.5037 |
| Liao et al.'s [45] | 0.0546 | 0.1415 | 0.5630 | 2.2597 | 9.0046 |
| CMT-IEA [17] | 0.0042 | 0.0130 | 0.0538 | 0.2338 | 1.1494 |
| HCMT-EE | 0.0042 | 0.0129 | 0.0542 | 0.1814 | 0.9144 |

comparison of various encryption and decryption algorithms along with their input image sizes ranging from 64 × 64 to 1024 × 1024 and observed HCMT-EE has the high encryption/decryption speed. The speed of the encryption process was improved for images with a large-size 512 × 512 and 1024 × 1024 is 0.1814 and 0.9144, respectively. Hence, HCMT-EE had less time complexity for large-size images.

Table 1, shows a comparison of [29, 44–47] enhanced experimental encryption/decryption speed results tested on several input images using MATLAB.

*4.2. Histogram Analysis.* The histogram is used to show the number of pixels per gray level. The histograms of the encrypted images are plotted in Figure 4. It shows that the histogram of the cipher image is uniform which defends against statistical attack. In Figure 4, the first row shows all original images which include grayscale images and color images. The second row shows histogram of the original images. The third row shows encrypted images of original images. The fourth row gives a histogram of encrypted images that are very relatively uniform.

*4.3. Pixel Correlation.* In digital images, usually high redundancy data will be there, thus giving high correlation among the neighbour pixels. A good cryptosystem can reduce the correlation between pixels which resist statistical attack. Data correlation is defined in [29]

$$C_{rr} = \frac{E\left(X - \mu_X\right)\left(Y - \mu_Y\right)}{\sigma_X \sigma_Y}, \tag{4}$$

where $C_{rr}$ is the correlation, $X$ and $Y$ are datasets, and $\mu$ is the mean value in the standard deviation. If $X$ and $Y$ have a high correlation, their $C_{rr}$ value is close to 1. Otherwise, it is close 0. To analyze and compare the correlation of the adjacent pixels in the plain and cipher image, 2500 random pair pixels are chosen in each direction from plain image and cipher image. The correlation of two adjacent pixels in three directions is shown in Table 2. Equation (4) is used to calculate correlation among two adjacent pixels which gives better results than [15, 29].

*4.4. Entropy.* Entropy gives uncertainty present in the cipher image. If the entropy of the cipher image is high, image has high randomness and high confidentiality [29].

$$H\left(k\right) = -\sum_{i=1}^{n} P_r\left(k_i\right) \log_2 P_r\left(k_i\right), \tag{5}$$

where $k$ is the collection of pixels, $k_i$ $i$th is possible value in $k$, $P(k_i)$ is the probability of $k_i$. Input images 5.1.09~7.2.01 are

Table 2: This table shows pixel correlation of Lenna image with CMT, 3D chaotic map algorithm, and HCMT-EE.

| Method | Images | Horizontal | Vertical | Diagonal |
|---|---|---|---|---|
| CMT [29] | Original image | 0.9659 | 0.9366 | 0.9153 |
| | Cipher image | 0.0023 | −0.0085 | 0.0402 |
| 3D chaotic map [15] | Original image | 0.91765 | 0.95415 | 0.90205 |
| | Cipher image | 0.01183 | 0.00016 | 0.01480 |
| HCMT-EE | Original image | 0.7705 | 0.6596 | 0.6195 |
| | Cipher image | −0.0049 | −0.0638 | −0.0012 |

tested using MATLAB from the USC-SIPI "Miscellaneous" dataset. The results are listed in Table 3. It is obvious that the entropies of the cipher images are close to the ideal value 8, which means that the probability of accidental information leakage is very small.

*4.5. Peak Signal Noise Ratio.* Peak Signal Noise Ratio measures the similarity between original image and received image. If the PSNR value is high, the correlation between original image and received image is high:

$$\text{PSNR} = 10 * \log_{10} \frac{255^2}{\text{MSE}} \text{ dB}. \tag{6}$$

*4.6. MSE (Mean Square Error).* In this method, the quality of the image is calculated by averaging the squared intensity values of difference of modified image and host image:

$$\text{MSE} = \frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left( f(x, y) - f'(x, y) \right)^2, \tag{7}$$

where $M \times N$ is the size of the image, $f(x, y)$ is the original image value at $(x, y)$ pixel, and $f'$ is the decrypted image values at $(x, y)$ pixel.

*4.7. Key Space Analysis.* The strength of the key depends on the size of the key which is used for encryption and decryption of the image. In proposed method, we consider that the key size is 256 bits and thus key space is $2^{256}$. This is sufficiently substantial to oppose brute-force attack. In encryption process, we have used two sensitive encryption keys, yielding totally different cipher image. In part of decryption process, we have two sensitive decryption keys to recover encrypted image, and the recovered images are completely dissimilar. Figure 5 shows that, using $K^1$ key derived two keys $K^2$ and $K^3$ with one-bit difference, to encrypt plain image into random image, input plain image (a) is encrypted using $K^1$ & $K^2$ and results in (b) and (c) are completely different as shown in (d). Encrypted image (b) completely is decrypted as shown in (e). Cipher images are decrypted in (f) and (g) with two keys of one-bit difference from $K^1$ being totally different. Hence, the proposed system is excellent in key sensitive process of encryption and decryption.

*4.8. Noise Analysis.* During the public transmission of image over the Internet or devices, the noise may attack images that may degrade the quality of the image: salt and pepper, Gaussian, and low-pass filter attack are general noise attacks [3].

In the proposed method, while shuffling the pixels to various positions in the image, image value positions can be changed automatically; it makes chosen-plaintext infeasible. In proposed strategy, while rearranging the pixels to different positions in the image, naturally image qualities can be changed; it makes chosen-plain text unfeasible

## 5. Conclusion

This paper proposed HCMT-EE which shows excellent simulation results for time complexity, key space analysis, various noise attacks, pixel correlation, and so forth; we have observed the performance of HCMT-EE in image security applications. Lanczos algorithm has been used to find eigenvector and eigenvalues in low-time complexity. GEM shifting has been used for image pixel shifting. The proposed HCMT-EE may apply in rain image recovery applications and 3D-medical image security.

## Abbreviations

AES: Advanced encryption standard
AIDM: Authenticity and integrity for mammography
CBC: Cipher block chaining
CML: Chaotic map lattices
CMT: Chaotic Magic Transform
CT-scan: Computerized tomography scan
DCT: Discrete cosine transform
DES: Data encryption standard
DICOM: Digital imaging and communications in medicine
DSA: Digital Signature Algorithm
DWT: Discrete wavelet transform
EPR: Electronic patient records
FT: Fourier transform
GCM: Galois Counter Mode
GoL: Game of Life
HMAC: Hashed message authentication code
IDEA: International data encryption algorithm
IVUS: Intravascular ultrasound
MASK: Matrix Array symmetric-Key Encryption
MD5: Message Digest-128 bits
MRI: Magnetic resonance imaging
PACS: Picture archiving and communication system
PSNR: Peak Signal to Noise Ratio
RC2: Rivest Cipher 2

Table 3: This table shows pixel correlation of the line image with CMT, 3D chaotic map algorithm, and HCMT-EE.

| File name | Wu et al.'s [46] | Zhou et al.'s [33] | Liao et al.'s [45] | Zhang et al.'s [44] | CMT-IEA [29] | HCMT-EE |
|---|---|---|---|---|---|---|
| 5.1.09 | 7.901985 | 7.903354 | 7.903764 | 7.904191 | 7.902127 | 7.902227 |
| 5.1.10 | 7.902731 | 7.902443 | 7.901801 | 7.902731 | 7.903402 | 7.903201 |
| 5.1.11 | 7.902446 | 7.902756 | 7.903306 | 7.900799 | 7.902687 | 7.902478 |
| 5.1.12 | 7.902556 | 7.901526 | 7.904478 | 7.903374 | 7.901906 | 7.901752 |
| 5.1.13 | 7.902688 | 7.904563 | 7.904657 | 7.904566 | 7.902825 | 7.902613 |
| 5.1.14 | 7.903474 | 7.902954 | 7.902874 | 7.903111 | 7.90234 | 7.902324 |
| 5.2.08 | 7.903953 | 7.902356 | 7.903218 | 7.901762 | 7.903327 | 7.903110 |
| 5.2.09 | 7.902233 | 7.899853 | 7.903089 | 7.905854 | 7.901765 | 7.901673 |
| 5.2.10 | 7.900714 | 7.902654 | 7.902077 | 7.902768 | 7.902748 | 7.902614 |
| 5.3.01 | 7.902727 | 7.902647 | 7.902108 | 7.90104 | 7.901772 | 7.901452 |
| 5.3.02 | 7.903182 | 7.910474 | 7.904169 | 7.903328 | 7.900981 | 7.900847 |
| 7.1.01 | 7.902173 | 7.902634 | 7.901965 | 7.902145 | 7.901305 | 7.901205 |
| 7.1.02 | 7.900879 | 7.901634 | 7.90497 | 7.902157 | 7.901578 | 7.901337 |
| 7.1.03 | 7.902543 | 7.905423 | 7.891503 | 7.900645 | 7.903099 | 7.902930 |
| 7.1.04 | 7.901126 | 7.902125 | 7.903399 | 7.904141 | 7.902607 | 7.902135 |
| 7.1.05 | 7.903579 | 7.883653 | 7.901301 | 7.900027 | 7.905305 | 7.904203 |
| 7.1.06 | 7.90193 | 7.902356 | 7.903367 | 7.901736 | 7.902695 | 7.902425 |
| 7.1.07 | 7.903000 | 7.902364 | 7.899556 | 7.900802 | 7.902896 | 7.902423 |
| 7.1.08 | 7.903197 | 7.904456 | 7.883531 | 7.900944 | 7.901632 | 7.901634 |
| 7.1.09 | 7.902308 | 7.903012 | 7.903201 | 7.905658 | 7.903173 | 7.902653 |
| 7.1.10 | 7.899542 | 7.901598 | 7.901542 | 7.893848 | 7.901524 | 7.901410 |
| 7.2.01 | 7.902772 | 7.901989 | 7.904945 | 7.904525 | 7.902454 | 7.902104 |
| boat.512 | 7.901908 | 7.901879 | 7.903091 | 7.900712 | 7.903088 | 7.902745 |
| elaine.512 | 7.901122 | 7.902989 | 7.901859 | 7.90203 | 7.90172 | 7.901679 |
| gray21.512 | 7.90017 | 7.905107 | 7.901832 | 7.902149 | 7.902688 | 7.902677 |
| numbers.512 | 7.903615 | 7.892351 | 7.902144 | 7.903579 | 7.901657 | 7.901437 |
| ruler.512 | 7.903265 | 7.903001 | 7.901937 | 7.901428 | 7.903052 | 7.903045 |
| testpat.1k | 7.902806 | 7.901681 | 7.903856 | 7.903343 | 7.902752 | 7.902378 |
| Mean | 7.902308 | 7.901923 | 7.903764 | 7.902167 | 7.902488 | 7.902169 |
| Pass rate | 18/28 | 20/28 | 17/28 | 11/28 | 26/28 | 26/28 |

ROI: Region of Interest
RSA: Rivest-Shamir-Adleman algorithm
SHA-1: Secure Hashing Algorithm.

## Competing Interests

The authors declare that there are no competing interests regarding the publication of this paper.

## References

[1] A. J. Paul, P. Mythili, and K. Paulose Jacob, "Matrix based cryptographic procedure for efficient image encryption," in *Proceedings of the IEEE Recent Advances in Intelligent Computational Systems (RAICS '11)*, pp. 173–177, Trivandrum, India, September 2011.

[2] K. Wang, W. Pei, L. Zou, A. Song, and Z. He, "On the security of 3D Cat map based symmetric image encryption scheme," *Physics Letters A*, vol. 343, no. 6, pp. 432–439, 2005.

[3] J. Li, A. Song, and X. Zhang, "Haptic texture rendering using single texture image," in *Proceedings of the 3rd International Symposium on Computational Intelligence and Design (ISCID '10)*, pp. 7–10, October 2010.

[4] X. Cindy Guo and D. Hatzinakos, "Image authentication using added signal-dependent noise," *Journal of Electrical and Computer Engineering*, vol. 2007, Article ID 47549, 5 pages, 2007.

[5] X. Zhang, C. Wang, S. Zhong, and Q. Yao, "Image encryption scheme based on balanced two-dimensional cellular automata," *Mathematical Problems in Engineering*, vol. 2013, Article ID 562768, 10 pages, 2013.

[6] G. Yang, H. Jin, and N. Bai, "Image encryption using the chaotic Josephus matrix," *Mathematical Problems in Engineering*, vol. 2014, Article ID 632060, 13 pages, 2014.

[7] J. Zhang, D. Hou, and H. Ren, "Image encryption algorithm based on dynamic DNA coding and Chen's hyperchaotic system," *Mathematical Problems in Engineering*, vol. 2016, Article ID 6408741, 11 pages, 2016.

[8] W. Wang, D. Peng, H. Wang, H. Sharif, and H.-H. Chen, "Energy-constrained quality optimization for secure image transmission in wireless sensor networks," *Advances in Multimedia*, vol. 2007, Article ID 25187, 9 pages, 2007.

[9] I. Maglogiannis, "Towards the adoption of open source and open access electronic health record systems," *Journal of Healthcare Engineering*, vol. 3, no. 1, pp. 141–161, 2012.

[10] J. Zhang and Y. Zhang, "An image encryption algorithm based on balanced pixel and chaotic map," *Mathematical Problems in Engineering*, vol. 2014, Article ID 216048, 7 pages, 2014.

[11] C. Liu, B. Lu, and H. Li, "Secure access control and large scale robust representation for online multimedia event detection," *The Scientific World Journal*, vol. 2014, Article ID 219732, 12 pages, 2014.

[12] K. Zhang and J.-B. Fang, "Color image encryption algorithm based on TD-ERCS system and wavelet neural network," *Mathematical Problems in Engineering*, vol. 2015, Article ID 501054, 10 pages, 2015.

[13] S. S. Askar, A. A. Karawia, and A. Alshamrani, "Image encryption algorithm based on chaotic economic model," *Mathematical Problems in Engineering*, vol. 2015, Article ID 341729, 10 pages, 2015.

[14] A. Kanso and M. Ghebleh, "An efficient and robust image encryption scheme for medical applications," *Communications in Nonlinear Science and Numerical Simulation*, vol. 24, no. 1–3, pp. 98–116, 2015.

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

[16] P. Tian-Gong and L. Da-Yong, "A novel image encryption using arnold cat," *International Journal of Security and Its Applications*, vol. 7, no. 5, pp. 377–386, 2013.

[17] V. Patidar, N. K. Pareek, G. Purohit, and K. K. Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption," *Optics Communications*, vol. 284, no. 19, pp. 4331–4339, 2011.

[18] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos, Solitons & Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.

[19] V. K. Kushwaha and K. Anusudha, "Based double encryption approach for secure transaction of medical images," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 2, no. 4, pp. 1418–1423, 2013.

[20] M. Ahmad and T. Ahmad, "A framework to protect patient digital medical imagery for secure telediagnosis," *Procedia Engineering*, vol. 38, pp. 1055–1066, 2012.

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

[22] L. O. M. Kobayashi, S. S. Furuie, and P. S. L. M. Barreto, "Providing integrity and authenticity in DICOM images: a novel approach," *IEEE Transactions on Information Technology in Biomedicine*, vol. 13, no. 4, pp. 582–589, 2009.

[23] X. Q. Zhou, H. K. Huang, and S. L. Lou, "Authenticity and integrity of digital mammography images," *IEEE Transactions on Medical Imaging*, vol. 20, no. 8, pp. 784–791, 2001.

[24] H.-M. Chao, C.-M. Hsu, and S.-G. Miaou, "A data-hiding technique with authentication, integration, and confidentiality for electronic patient records," *IEEE Transactions on Information Technology in Biomedicine*, vol. 6, no. 1, pp. 46–53, 2002.

[25] S. Gueron, "AES-GCM for efficient authenticated encryption," in *Proceedings of the Workshop on Real-World Cryptography*, pp. 1–32, January 2013.

[26] D. Brat Ojha, A. Sharma, A. Dwivedi, B. Kumar, and A. Kumar, "An authenticated two-tier security on transmission of medical image using codebase cryptosystem over teeming channel," *Internationnal Journal of Computer Applications*, vol. 12, no. 9, pp. 22–26, 2011.

[27] W. Puech and J. M. Rodrigues, "A new crypto-watermarking method for medical images safe transfer," in *Proceedings of the 12th European Signal Processing Conference (EUSIPCO '04)*, pp. 1481–1484, Vienna, Austria, 2004.

[28] F. Cao, H. K. Huang, and X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," *Computerized Medical Imaging and Graphics*, vol. 27, no. 2-3, pp. 185–196, 2003.

[29] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.

[30] M. François, T. Grosges, D. Barchiesi, and R. Erra, "A new image encryption scheme based on a chaotic function," *Signal Processing: Image Communication*, vol. 27, no. 3, pp. 249–259, 2012.

[31] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, no. 4, pp. 394–400, 2008.

[32] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.

[33] Y. Zhou, L. Bao, and C. L. P. Chen, "Image encryption using a new parametric switching chaotic system," *Signal Processing*, vol. 93, no. 11, pp. 3039–3052, 2013.

[34] C.-J. Cheng and C.-B. Cheng, "An asymmetric image cryptosystem based on the adaptive synchronization of an uncertain unified chaotic system and a cellular neural network," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, no. 10, pp. 2825–2837, 2013.

[35] K. Jasteazebski and Z. Kotulski, "On improved image encryption scheme based on chaotic map lattices," *Engineering Transcations*, vol. 69, no. 84, 2009.

[36] 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.

[37] C. K. Huang and H. H. Nien, "Multi chaotic systems based pixel shuffle for image encryption," *Optics Communications*, vol. 282, no. 11, pp. 2123–2127, 2009.

[38] S. Som and S. Sen, "A non-adaptive partial encryption of grayscale images based on chaos," *Procedia Technology*, vol. 10, pp. 663–671, 2013.

[39] G. Alvarez and S. Li, "Breaking an encryption scheme based on chaotic baker map," *Physics Letters, Section A: General, Atomic and Solid State Physics*, vol. 352, no. 1-2, pp. 78–82, 2006.

[40] N. Kumar and H. T. Panduragha, "Advanced partial image encryption using two-stage hill cipher technique," *Iternational Journal of Computer Applications*, vol. 60, no. 16, pp. 14–19, 2012.

[41] X. W. Li, S. J. Cho, and S. T. Kim, "High security and robust optical image encryption approach based on computer-generated integral imaging pickup and iterative back-projection techniques," *Optics and Lasers in Engineering*, vol. 55, pp. 162–182, 2014.

[42] C. Ye, Z. Xiong, Y. Ding, X. Zhang, G. Wang, and F. Xu, "Joint fingerprinting/encryption for medical image security," *International Journal of Security and Its Applications*, vol. 9, no. 1, pp. 409–418, 2015.

[43] https://en.wikipedia.org/wiki/Lanczos_algorithm.

[44] J. Zhang, D. Fang, and H. Ren, "Image encryption algorithm based on DNA encoding and chaotic maps," *Mathematical Problems in Engineering*, vol. 2014, Article ID 917147, 10 pages, 2014.

[45] X. Liao, S. Lai, and Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," *Signal Processing*, vol. 90, no. 9, pp. 2714–2722, 2010.

[46] Y. Wu, J. P. Noonan, and S. Agaian, "A wheel-switch chaotic system for image encryption," in *Proceedings of the International Conference on System Science and Engineering (ICSSE '11)*, pp. 23–27, Guiyang, China, June 2011.

[47] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, "Image encryption using the two-dimensional logistic chaotic map," *Journal of Electronic Imaging*, vol. 21, no. 1, Article ID 013014, 2012.