Received: 1 June 2023 | *Revised:* 10 August 2023 | *Accepted:* 13 September 2023
DOI: 10.37917/ijeee.20.2.1 *Early View* | *December 2024*

Open Access

Iraqi Journal for Electrical and Electronic Engineering
Original Article

IJEEE University of Basrah College of Engineering

A Secure Image Cryptographic Algorithm Based on Triple Incorporated Ciphering Stages

Sura F. Yousif , Abbas Salman Hameed*, Dheyaa T. Al-Zuhairi
Collage of Engineering, University of Diyala, Diyala, Iraq

Correspondance
*Abbas Salman Hameed
Collage of Engineering, University of Diyala, Diyala, Iraq
Email: abbasfuture@yahoo.com, abbas_hameed_eng@uodiyala.edu.iq

Abstract
Lately, image encryption has stand out as a highly urgent demand to provide high security for digital images against use and unauthorized distribution. A lot of existing researches use chaotic systems, symmetric or asymmetric schemes for image encryption, but cryptosystem based on one encryption technique only, faces many challenges like weak security and low complexity. Therefore, incorporating two or more different ciphering methods yields a secure and efficient algorithm to protect image information. In this work, a new image cryptosystem is suggested by joining zigzag scan technique, RSA algorithm and chaotic systems. These three security factors introduce Triple Incorporated Ciphering stages system (TIC). Initially, the plaintext image is divided into 8×8 ***non-overlapping blocks, then the odd blocks are isolated from the even blocks. After that, a new modified zigzag scan in two different directions is adopted for shuffling pixels in the odd and even blocks. This operation effectively enhances the shuffling degree. Next, the RSA algorithm is utilized after combining the scrambled blocks in one matrix. Finally, chaotic systems are implemented on the resultant encrypted matrix to complete the ciphering process. The chaos is implemented in two steps; confusion and diffusion. Duffing map is exploited in the confusion stage, whereas Lü system is adopted on the shuffled matrix in the diffusion stage. The simulation results show the superiority of TIC in both security and attacks robustness compared to other cryptographic algorithms. Therefore, TIC can be exploited in real-time communication systems for secure image transmission.***

Keywords
Cryptography, Image encryption and decryption, Symmetric scheme, Asymmetric scheme, Zigzag scan, RSA mechanism, Chaotic system, Security analysis.

I. Introduction

The security of digital multimedia like audio, video and image files has become a substantial issue nowadays, especially with the prompt evolution in communication, and network multimedia. The protection of digital images became more significant because the transferring of these files throughout networks increased every day [1–3]. Encryption is one of the most common and efficient techniques that is used to assure the transmission security over open networks like Internet. Encryption safeguards the confidential image content from the adversary or illegal access by transforming the image information from its readable format to ambiguous format that is hard to understand. Generally, cryptosystems are categorized into two different sorts, symmetric and asymmetric cryptosystems [4, 5]. The symmetric or secret key cryptography employs only one individual key that is shared between the sender and receiver for secret data encryption and decryption. DES and AES are examples of symmetric ciphers [5, 6]. Meanwhile, two various keys are employed in the asymmetric or public key cryptography. Public key is utilized for the encryption operation, while private key is dedicated for the decryption operation.

El-Gamal, DH and RSA cryptographic algorithms are examples for asymmetric cryptosystems [5, 6]. The symmet-

ric or asymmetric schemes are not proper for digital image encryption because these techniques need high computation time, power and cost to execute complex processing processes like permutation/diffusion operations. Therefore, it is hard for these algorithms to meet the online communication demands when dealing with the properties of digital image such as bulk data capacity and strong correlation among pixels [7, 8]. To face these challenges, it is requisite to evolve hybrid security methods that integrate traditional ciphering schemes and new encryption technologies to build high efficiently and securely algorithms. Lately, many various encryption approaches have been presented such as chaos-based schemes [1, 7–14]. These algorithms provide an optimum balance between efficiency and security.

Chaotic system is a dynamic, nonlinear, disordered and deterministic system [10, 15]. These systems have several prominent features that are closely linked to cryptographic systems such as ergodicity, high sensitiveness to initial and control parameters values, non-periodicity, etc. [9, 10]. The structure of pseudo-random sequences generated by the chaotic systems is extremely complicated and difficult to be predicted or analyzed. Hence, utilizing these distinct chaotic properties in the cryptography leads to developing new and efficient methods for providing image security during transmission over sharing networks or any communication channel.

The exemplary ciphers rely upon the chaotic systems can be categorized into two major phases: confusion and diffusion. In the confusion phase, the pixels positions of the original image are changed, while in the diffusion phase, the pixels values are altered. The confusion process has good ciphering result, but the histogram of the plaintext image is still analogous to that of the cipher image, which makes the algorithm security threaten by the statistical analysis. For promoting the confusion phase, the diffusion process is proposed in order to ameliorate the security level [13]. Several researchers have merged these two stages to enhance the security of ciphering schemes. However, there are still some challenges that demand to be faced when utilizing chaos theory in the cryptography field. For example, some researchers apply one dimension chaotic maps in their ciphering algorithms. These maps produce one simple expected chaotic orbit. So, the opponent can facilely get the system parameters/initial values of the chaotic system. Additionally, one dimension maps suffer from weakened security and small key space. Therefore, employing higher dimensional chaotic systems raises the nonlinearity thereby improving the algorithm security [1, 6].

Various techniques have been developed by researchers in recent years for image encryption. Reza et al in 2013 [16] utilized scan pattern technology and XOR function for image encryption after dividing the input image into several blocks. To enhance the security, the plain image is enciphered by Xiaoheng et al in 2013 [17] via applying permutation/diffusion architecture of hyper-chaotic system. Qiang et al in 2013 [18] utilized four dimensional Chen system and DNA operations for image encryption/decryption. The image in binary form is encoded via DNA encoder before scrambling it by the chaotic sequences. An image cryptosystem is presented by Borislav and Krasimir in 2014 [19] based on Chebyshev and Duffing chaotic maps by employing permutation/substitution structure. To increase the randomness degree, 2D Baker chaotic map and cyclic shift technique in wavelet domain is implemented by Ensherah et al in 2014 [20] to protect the image content during storage and transmission. In order to reduce the processing time, Hongye et al in 2016 [21] introduced an image encryption method by exploiting high dimensional chaotic system and DNA coding/splicing model to modify the information of image drastically.

A simple encryption scheme is proposed by Shrija and Mohammad in 2017 [22] by adopting scan language for ciphering both color and gray images of different formats. The use of XOR operation between the original and key images in this scheme yields an encryption with a low security level. Xiuli et al in 2017 [23] integrated DNA computing and a new two dimensions chaotic map to encrypt the plaintext image so as to increase the complexity and security of the suggested approach. Another encryption method is suggested by Xiuli et al in 2018 [24] by employing a hybrid encryption approach via jointing compressive sensing, chaotic system and cellular automata mechanism in order to cipher the original image. The problem in this method is that the time required to obtain the optimal solution is long. Nasrullah et al in 2018 [25] described an encryption-compression method for digital images by merging chaotic maps with Kd-tree and set partitioning technologies. The two stages: confusion and diffusion of new 2D chaotic map are mixed by Xiaoling and Guodong in 2018 [26] to design a secure image cryptosystem.

An encryption system is explained by Zhenjun et al in 2019 [7] based on Henon, Lu chaotic maps in addition to spiral scan and random block partition mechanisms. Piecewise and Henon mapping are combined by Chunyuan and Qun in 2020 [27] to build a new 3D chaotic system for encrypting color images. Jannatul et al in 2021 [28] encrypted the input image such as miscellaneous or medical image by adopting two chaotic maps: Arnold and Logistic maps. Multiple chaotic maps along with XOR operation and S-box method are applied by Tahir and Rashid in 2022 [29] to construct a different image encryption algorithm.

Xinyu et al in 2022 [30] encrypted various sorts of images such as 2D and 3D images via scrambling-diffusion processes of 3D neuron chaotic model. A new study is designed by Nirmal et al in 2022 [31] relied upon AES and chaotic approaches for digital image encryption. This method is characterized by

weak security because of applying low dimensional chaotic map. Two layers of encryption are executed on the actual image by Zhiqiang et al in 2022 [32] to increase the system security. The first layer encrypts the specified image, whereas the second layer encrypts the whole image. Nehal et al in 2022 [33] performed the encoding/decoding processes by implementing Chen system and 3D quantum chaotic map. High chaotic dimensional systems are used to ensure the image information security during transmission.

Muhammad et al in 2023 [34] studied an image cryptosystem by using multiple chaotic maps. Confusion and diffusion stages are exploited to break the association among neighboring pixels in the original image. Kiran et al in 2023 [35] described the manipulation of pixel value/position by applying chaos theory and SCAN technology. This mechanism is implemented on medical images to protect the sensitive information of patients during transferring over public channels. Finally, an image ciphering approach is designed by Ammar in 2023 [36] to encrypt the gray image. This cryptosystem is based on Pascal's matrix and 7D hyper-chaotic system. The plain image is initially permuted via the chaotic system. Then, the diffusion stage is realized via the Pascal's matrix. The suggested approach is assessed by using many various metrics such as histogram and correlation analysis.

Based upon the above survey and to conquer the security flaws in several image encryption schemes, such as time consumption, inadequate security, attacks immunity, and key space limitation, an effective image ciphering algorithm that combines zigzag scan technology with RSA cryptosystem and high dimensional chaotic systems is designed in this article. Firstly, the input image is partitioned to equal blocks, each of size 8×8. Then, these blocks are separated into odd and even blocks according to their index. Next, both odd and even blocks are scrambled using a modified zigzag scan but in opposite directions. The modification includes changing the starting pixel location of the zigzag scan for each block depending on chaotic sequences. This step increases the permutation degree such that a newly mutated image is built. Secondly, after the scrambling phase, the RSA public key system is exploited so as to cipher the produced image. Finally, in order to accomplish the encryption phase, chaotic maps with high dimensions are applied on the resultant ciphered image to perform the confusion-diffusion stages. 2D Duffing map is adopted for the pixels confusion process, while 3D Lü system is employed for the pixels diffusion process to earn the eventual ciphered image. Integrating these two processes effectively improves the encryption performance. Thus, the proposed TIC algorithm can successfully cipher the input images and safeguard their information. The encrypted image can be readily retrieved by the receiver as soon as he obtains the secret keys from the sender. The presented method contributions are listed as follows: (1) Using three different ciphering technologies for image encryption: zigzag scan technique, RSA algorithm, and chaotic systems to ameliorate the cryptosystem security. (2) Enhancing significantly the shuffling process of original image pixels by applying modified zigzag scan in two different directions. (3) Adopting confusion-diffusing architecture in order to withstand known cryptographic attacks. (4) Employing high dimensions chaotic systems to improve the method robustness against exhaustive attacks by increasing the key space size. The proposed TIC algorithm performance is evaluated on different input grayscale images using many assessment metrics such as statistical analysis, differential analysis, exhaustive analysis, computational speed analysis, and robustness analysis. The outcomes of these tests point out the efficacy and superiority of the proposed algorithm thereby it can be used for image security applications.

II. Main Theory of The Proposed Algorithm

A. *Modified Zigzag Scan*

The typical zigzag scan technique is a well-known standard method for matrix transforming from two dimensions to one-dimension vector. By employing this technique, the adjacency relationship among pixels in the plain image is ruined thereby ameliorating the security degree of the cryptosystem. In the two dimensions image, the adjacent pixels are extremely correlated, whereas in the one-dimension vector, these pixels are vastly dispersed and separated [16, 22, 37]. The position of starting pixel is quite significant in the matrix for zigzag permutation; different positions can produce different permutation results [24]. For example, if the zigzag scan in Fig. 1b is implemented on the 4×4 sub-image in Fig. 1a and the position of starting pixel is located at the first row-first

TABLE I.
Nomenclature and Abbreviations List

Nomenclature	Abbreviation
RSA	Rivest-Shamir-Adleman
DES	Data Encryption Standard
AES	Advanced Encryption Standard
DH	Diffie–Hellman
XOR	Exclusive-OR
DNA	Deoxyribonucleic Acid
2D	Two dimensions
3D	Three dimensions
7D	Seven dimensions
Kd	k-dimensional
S-box	Substitution-box

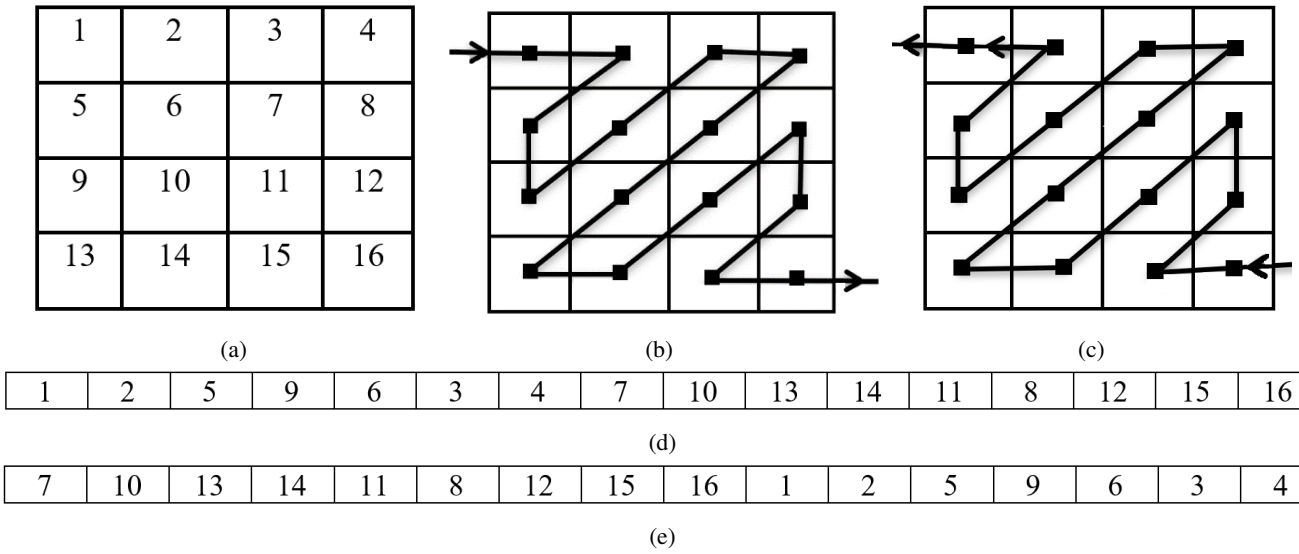


Fig. 1. Zigzag Scan Permutation (a) Input Sub-image (b) First Zigzag Scan Direction (c) Second Zigzag Scan Direction (d) Vector Generated by Applying the First Zigzag Scan Direction Started in Position Number 1 in (a) , (e) Vector Generated by Applying the First Zigzag Scan Direction Started in Position Number 7 in (a)

column, then the resulted vector is depicted in Fig. 1d. On the other hand, if the zigzag scan in Fig. 1b is implemented on the 4×4 sub-image in Fig. 1a and the position of starting pixel is located at the second row-third column, then the resulted vector is shown in Fig. 1e. A different vector will be produced if the location of the starting pixel is changed. In this work, the zigzag scan is modified such that the starting pixel location is variable for each scanned sub-image and it is selected based on chaotic sequences. Consequently, high permutation feature is achieved to strengthen the security level of TIC.

B. RSA Mechanism

Rivest, Shamir, and Adleman were the first three cryptologists who described RSA public key cryptosystem in 1978. RSA is utilized for providing authenticity, security and privacy of the digital information. It is used in several applications that demand data security, such as electronic mail security, electronic commerce on Internet and banking. This mechanism uses exponentiation modular multiplication. As in standard asymmetric cryptosystem, the RSA employed two separated keys; the public and secret keys. The public key is devoted for data encryption operation and can be sent to anyone inside the system. The secret key is consecrated for decryption process and should be remain confidential inside the RSA system. RSA security relies on the complexity of finding the prime factors of large prime integer numbers which is one of the most difficult problems in mathematics. The processes of RSA technique can be decomposed into three fundamental phases: key production, encryption and decryption operations [3, 14, 38].

1) Key Production Procedure:

- Two prime integer numbers p and q are chosen randomly.
- Compute n which represents the public modulus by: $n = pq$.
- Compute Euler's totient function $\phi(n)$ by: $\phi(n) = (p-1)(q-1)$.
- A third random integer e is selected such that gcd $(e, \phi(n)) = 1$ and $1 < e < \phi(n)$, where gcd represents greatest common divisor.
- Calculate the decryption key (d) by: $d = e^{-1} mod(\phi(n))$.
- (n, e) points to the public key, whereas (n, d) points to the secret key.

2) Encryption Procedure:

The plaintext P is divided initially into string of blocks P_1, P_2, .., P_i, such that each block P_i satisfies the condition: $0 < P_i < n$. After that, the encryption process is performed on each plaintext block to obtain the ciphered text C as [3, 14, 38]:

$$C = P^e mod\, n \tag{1}$$

Then, the cipher text C is transmitted to the receiver.

3) Decryption Procedure:
The receiver can decrypt each ciphered text block C to retrieve the original plaintext P by utilizing the following formula [3, 14, 38]:

$$P = C^d \bmod n \tag{2}$$

C. Chaotic Generators

1) Duffing Map:
This chaotic map is a two-dimensional discrete system that can be expressed mathematically as:

$$x_{(n+1)} = y_n, \qquad y_{(n+1)} = -bx_n + ay_n - y_n^3 \tag{3}$$

where a and b represent the system constants which generate the chaotic behavior at the values 2.75 and 0.2, respectively [19].

2) Lü System:
Lü chaotic system is a three-dimensional continuous system which is considered a transitional state between Chen and Lorenz systems. This system is described mathematically via a set of ordinary nonlinear differential equations given by:

$$\dot{x} = a(y-x), \qquad \dot{y} = cy - xz, \qquad \dot{z} = xy - bz \tag{4}$$

where a, b and c denote to the control system parameters and they produce chaotic status when their values are 36, 3 and 20, respectively [39, 40].

III. TIC ALGORITHM STRUCTURE

The block diagram of the suggested encryption image scheme is exhibited in Fig. 2. The major stages of TIC involve zigzag scan, RSA algorithm and chaotic systems. In the first stage, the plaintext image is divided into 8×8 non-overlapping blocks. The direction of image splitting into blocks starts from top to bottom till it reaches to the last block. Then, these blocks are separated to odd and even blocks according to their indices. The pixels in the odd blocks are scrambled by applying zigzag scan with a variable starting point at first direction (Fig. 1b), whereas the pixels in the even blocks are scrambled by applying zigzag scan with a variable starting point at second direction (Fig. 1c). The starting point is determined by the generated two Lü chaotic sequences. The specific sequences are quantized to have values in the range [1-8], which represent the row and column numbers of the zigzag operation starting pixel. Therefore, in each block, the zigzag scan starts at a pixel location which is different from those of other blocks. This step is the most significant step in this work because it helps to lessen the correlation between the original image pixels thereby increasing the value of entropy in the ciphered image. Next, the output vectors from this stage are merged together in a new permutated matrix. In the second stage, RSA coding technique is exploited to cipher the permutated image from the first stage by utilizing the public key (e, n). Eventually, primeval processes in cryptography like confusion/diffusion are performed using chaotic Duffing and Lü systems. These two systems produce the confidential keys for the suggested work by the means of their control parameters/initial conditions. Confusion is executed for randomly scrambling image pixel locations; this process is implemented via 2D Duffing map. On the other hand, diffusion is executed for varying image pixel values; this operation is performed via 3D Lü system. The details of encryption and decryption procedures are outlined in the following subsections.

A. Encryption Procedure

The specific steps for encryption process according to Fig. 2 are illustrated as follows:
Step 1: The input image $A(m, m)$ is divided into (8×8) non-overlapping blocks.
Step 2: The odd blocks, for instance $(block_1, block_3, block_5, \ldots, block_{(k-1)}$ are joined in one matrix $M(8 \times 8 \times k/2)$, where k represents the total blocks number and it is assumed as an even value in this work.
Step 3: The even blocks, for instance $(block_2, block_4, block_6, \ldots, block_k)$ are joined in one matrix $N(8 \times 8 \times k/2)$.
Step 4: Produce three chaotic sequences u, v and w with m^2 elements for each sequence, by using (4) after setting the initial conditions/system parameters values (x_0, y_0, z_0, a, b, c).
Step 5: Choose the first k elements of the quantized v and w sequences to determine the starting pixel position, where each pair of (v_i, w_i), $i = 1, 2, \ldots, k$, represents the starting pixel row and column in the i^{th} block, respectively.
Step 6: Depending on the selected starting pixel, apply zigzag scan according to the direction in Fig. 1b on the matrix M to acquire the vector Y_1 of $64k/2$ elements.
Step 7: Depending on the next selected starting pixel, apply zigzag scan according to the direction in Fig. 1c on the matrix N to acquire the vector Y_2 of $64k/2$ elements.
Step 8: Concatenate Y_1 and Y_2 in a new vector Y' with $64k$ elements.
Step 9: Reshape Y' into 2D matrix $Y_1{}'$ with the same size of plain image A.
Step 10: Perform the RSA encryption algorithm after determining the value of public key (n, e) on the matrix $Y_1{}'$ via (1) to obtain F as:

$$F(i, j) = [Y_1{}'(i, j)]^e \bmod n \tag{5}$$

Step 11: Produce two chaotic sequences x and y with m^2 elements for each sequence, by using (3) for Duffing map

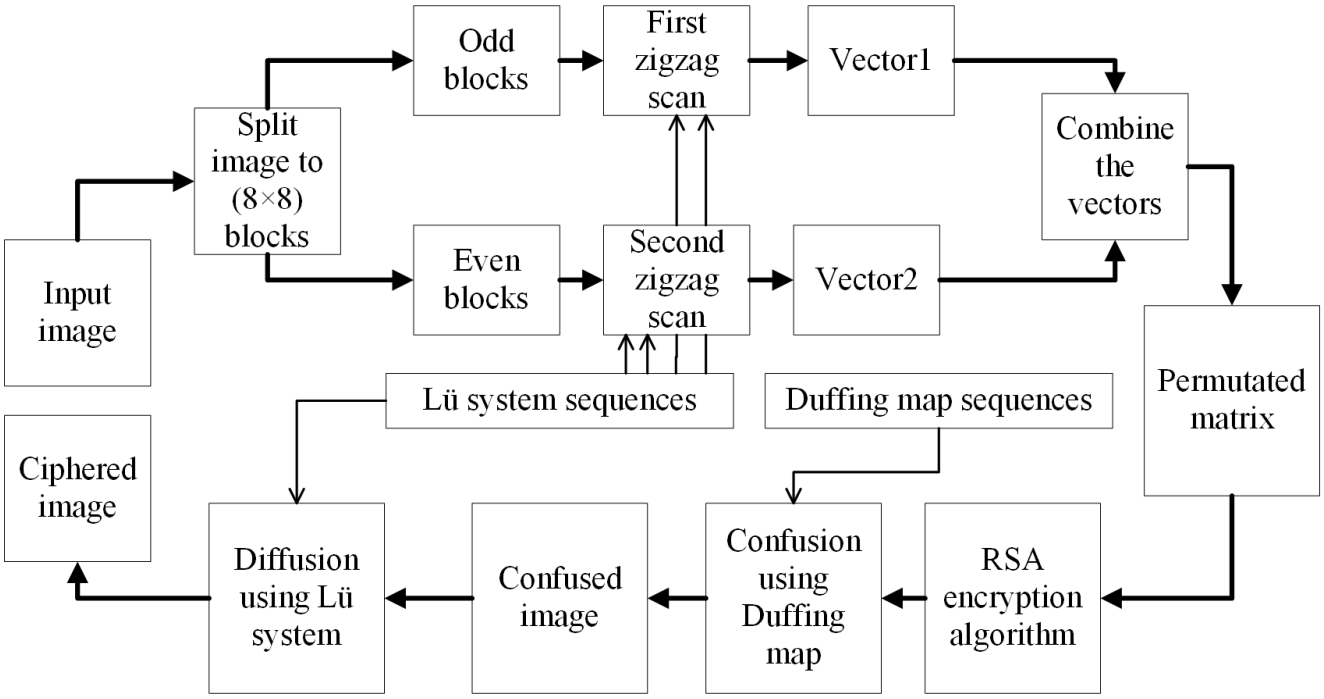


Fig. 2. Block Diagram of The Suggested Encryption Scheme

after determining the initial conditions/system parameters values (x_0, y_0, a, b).

Step 12: Reshape x and y to the same size of matrix F to generate the two matrices x_1,y_1, then x_1 and y_1 are sorted in ascending order:

$$[L_1, d_1] = sort(x_1), [L_2, d_2] = sort(y_1) \tag{6}$$

where d_1, d_2 represent the new sequences, and L_1,L_2 denote the index values of d_1 and d_2, respectively.

Step 13: Choose (L_1) combination for shuffling F to get the confused image $E_1 as$:

$$E_1(i, j) = F(L_1(i, j)) \tag{7}$$

Step 14: Choose u of Lü chaotic sequence to perform the diffusion process after reshaping it to the same size of matrix E_1 to generate u_1 matrix. The diffused image E_2 is generated according to the formula:

$$E_2(i, j) = E_1(i, j) \oplus u_1(i, j) \tag{8}$$

where E_2 represents the earned ciphered image. If the plain image is a color image (RGB image), $A(m, m, 3)$, then A is divided into three layers: $R(m, m)$,$G(m, m)$ and $B(m, m)$. After this, the encryption Steps (1-14) are implemented on each layer separately to get the three ciphered images. The ultimate step is concatenating them to acquire the final encrypted image $E_2(m, m, 3)$.

In addition, the proposed work is applied on images of equal dimensions, $A(m, m)$. But if the input image is not square, $A(m, n)$, then a particular technique (interpolation technique) should be applied to avoid falling-off out of range during splitting the image into (8×8) non-overlapping blocks. Algorithm 1 illustrates the encryption steps of the proposed cryptosystem with more details.

B. Decryption Procedure

The procedure of image decryption can be executed by applying the encryption stages in the inverted order. The receiver gets the correct secret keys from the sender. The deciphered image is gained according to contrary process of the above explained steps. The decryption process begins from the encrypted image E_2 and finishes up with the original image A.

IV. Implementation Results and Security Analysis

The experiments of encryption-decryption operations of TIC algorithm are implemented using MATLAB (R2013a), 64-bit Windows 7, on HP personal Laptop computer with Processor Intel (CORE i3), 4 GB RAM memory, and 2.40GHz

Algorithm 1: The proposed image encryption method.

// A: Input image of size (m,m).
// E_2: Output image of size (m,m).
// k: Total blocks number (even value).
1: Divide A into 8×8 non-overlapping blocks from top to bottom.
2: Join the odd blocks of A to get M. % M of size $(8\times 8\times \frac{k}{2})$
3: Join the even blocks of A to get N. % N of size $(8\times 8\times \frac{k}{2})$
4: Set $x_0,\ y_0,\ z_0, a, b,\ c$ values of Lü System.
5: Produce $u,\ v, w$ according to (4). % $u,\ v,\ w$ of size (m^2)
6: Quantize v, w to obtain $v^{'}, w^{'}$.
7: Choose the first k elements of $v^{'}, w^{'}$ to form the pair of $(v_i^{'}, w_i^{'})$. % $i = 1,2,\ldots,k$
8: Select the starting pixel position (row, column) according to $(v_i^{'}, w_i^{'})$.
9: Apply zigzag scan (Fig. 1b) according to $(v_{2i-1}^{'},\ w_{2i-1}^{'})$ on each block of M to get Y_1. % Y_1 of size ($64\frac{k}{2)}$
10: Apply zigzag scan (Fig. 1c) according to $(v_{2i}^{'},\ w_{2i}^{'})$ on each block of N to get Y_2 . % Y_2 of size ($64\frac{k}{2)}$
11: Concatenate Y_1 and Y_2 to get $Y^{'}$. %$Y^{'}$ of size ($64k$)
12: Reshape $Y^{'}$ to get $Y_1^{'}$. %$Y_1^{'}$ of size (m,m)
13: Apply RSA according to (5) on $Y_1^{'}$ to gain F.
14: Set $x_0,\ y_0, a, b$ values of Duffing map.
15: Produce x, y according to (3). % x, y of size (m^2)
16: Reshape $x,\ y$ to gain $x_1,\ y_1$. % $x_1,\ y_1$of size (m,m)
17: Sort $x_1,\ y_1$in ascending order according to (6) to obtain $(L_1,\ d_1)$ and $(L_2,\ d_2)$.
18: Scramble F via $(L_1,\ d_1)$ to get E_1(confusion) according to (7).
19: Quantize and reshape u to gain $u^{'}$. % $u^{'}$of size (m,m)
20: Diffuse E_1 via $u^{'}$ to get E_2(diffusion) according to (8). % $E_2$of size (m,m)

CPU. For the performance assessment, six different standard grayscale images are used as test images, each of size 256×256. The images are chosen from USC-SIPI image database (http://sipi.usc.edu/database/). The image files are: Cameraman, Lena, Baboon, Barbara, Boat and Peppers, which are displayed in Fig. 3. The RSA secret parameters are: 33, 7 and 3 for n, e and d, respectively. For duffing map, the values of initial conditions and system parameters are: 0.11, -0.6, 2.75 and 0.15 for x_0, y_0, a and b, respectively. For Lü system, the values of secret keys are: 0.4, -0.5, 0.7, 36, 3 and 13 for x_0, y_0, z_0, a, b and c, respectively. The ciphered version of Cameraman image produced via the presented image cryptosystem is given in Fig. 4a, whereas the deciphered image result using the assigned secret keys is shown in Fig. 4b. It is obvious that the ciphered image comprises no beneficial information in comparison with its corresponding original one; it is meaningless and a noise-like. On the other hand, the deciphered and the plain images are identical, which manifests that TIC can cipher and decipher images effectively.

A. Statistical Analysis

1) Histogram Analysis:

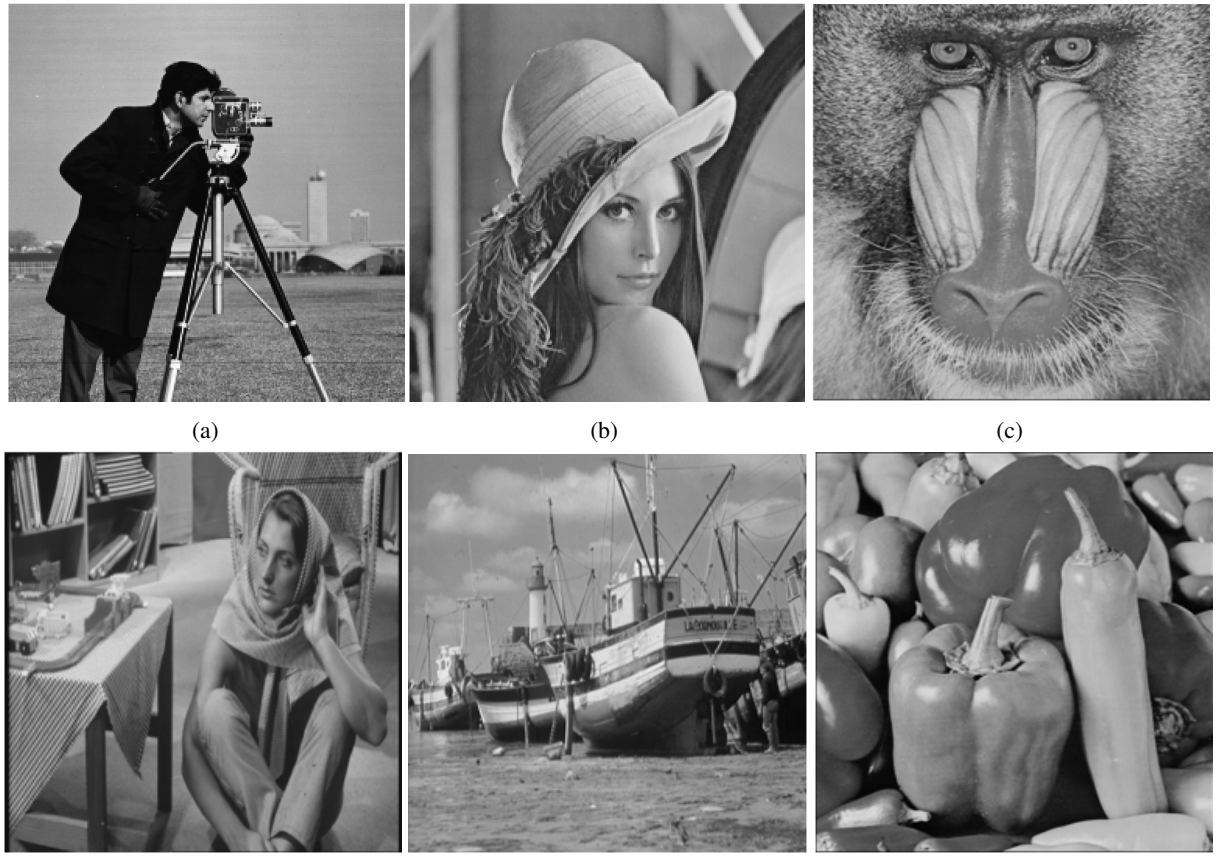
Histogram is a kind of bar diagram that illustrates the pixel values distribution of the image at particular intensity. It is usually utilized for measuring the cryptosystem performance. In general, an efficient ciphering system has a uniform histogram [8]. The outcomes of histogram analysis achieved by TIC are clarified in Fig. 5 . Figs. 5a and 5b represent the histograms of the Cameraman grayscale plain image and its corresponding encrypted image, respectively. Fig. 5a reveals that the plain image pixels values are concentrated at some values, whereas the encrypted image, Fig. 5b, pixels values are fairly uniform, flat and completely distinct from that of the original image. Moreover, the histogram of the recovered image in Fig. 5c is similar to that of the plain text image. No helpful data about the original image can be assembled by histogram analysis, which points that the TIC has enough ability to endure the statistical attacks.

2) Information Entropy Analysis:

Information entropy $H(X)$ is a significant measure employed for measuring the randomness or uncertainty of information in the plain image [23]. This metric is calculated as:

$$H(X) = -\sum_{i=0}^{L-1} P(x_i) log_2 P(x_i) \tag{9}$$

where X symbolizes a random variable, and $P(x_i)$ is the occurrence probability of x_i. For a random grayscale image



(a) (b) (c)

(d) (e) (f)

Fig. 3. The Test Images (a) Cameraman (b) Lena (c) Baboon (d) Barbara (e) Boat (f) Peppers

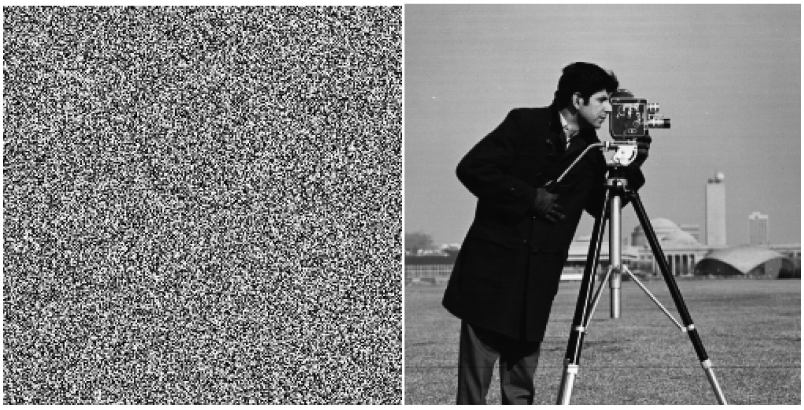
of 256 gray levels ($L = 256$), the maximum ideal value for information entropy is 8. Usually, higher values of entropy imply a more secure ciphering system. The computed results of information entropy for the six test original images and their corresponding ciphered images are given in Table II. From the obtained values in this table, it is obvious that the entropy values for all the ciphered images are extremely near to the optimal value. This indicates that the encrypted images produced by the TIC cryptosystem are so close to random sources and therefore the suggested algorithm can withstand the entropy attack.

3) Correlation Analysis:

There is a strong correlation among adjoin pixels in the ordinary image along three directions due to the massive amount of redundancy data. In contrary, less correlation between the adjacent pixels in the encrypted image indicates a strong image cipher. Several couples of adjacent pixels are chosen to compute the correlation coefficient value in a particular direction. The correlation coefficient r_{xy} is described according to the following mathematical equations [17]:

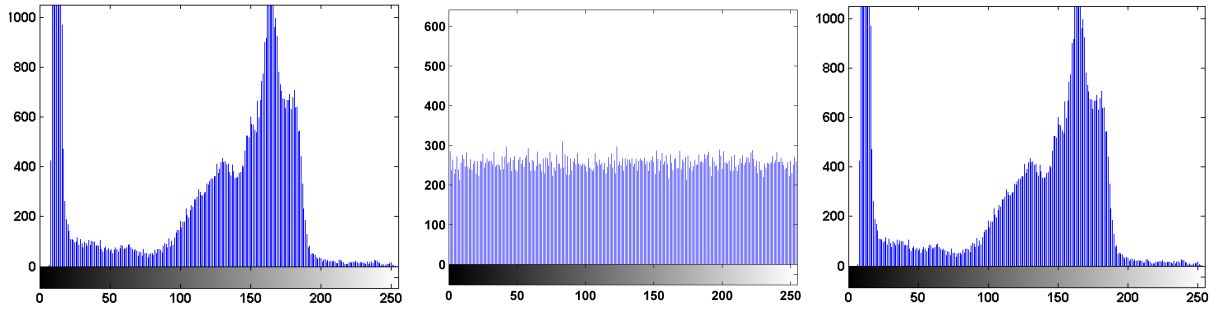
$$\begin{aligned} E(x) &= \frac{1}{N} \sum_{i=1}^{N} x_i \\ D(x) &= \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x_i))^2 \\ cov(x,y) &= \frac{1}{N} \sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \\ r_{xy} &= \frac{cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \end{aligned} \tag{10}$$

where x and y are two adjoin pixels in the image, $E(x)$, $D(x)$ and $cov(x,y)$ indicate the mean, variance and covariance, respectively. The range of r_{xy} is in the interval [-1, 1]. If the value of r_{xy} is high, then the correlation between two neighboring pixels is strong and vice versa. Any two couples of adjoining pixels in the plain image commonly possess a potent correlation. An effective ciphering technique should weaken or break this correlation. In the TIC algorithm experiments,



(a) (b)

Fig. 4. (a)The Ciphered Image (b) The Deciphered Image



(a) (b) (c)

Fig. 5. Images Histograms (a) Plain Image (b) Cipher Image (c) Decipher Image

5000 couples of neighboring pixels are randomly chosen in the three directions: vertical, horizontal and diagonal from the same position of the original and its ciphered images for computing the correlation coefficient values. The outcomes of correlation coefficients between neighboring pixels for the six test images and their ciphered versions are displayed in Table III. It can be noticed from Table III that the values of correlation coefficients at the three directions of the input image are almost one, whereas these values are approximately zero in the output ciphered images. The diagrams of pixel distribution over horizontal, vertical and diagonal directions from the input and its corresponding cipher images for Lena image are shown in Fig. 6. The results manifest that most pixel couples in the plain image are grouped about the main diagonal, while these couples are almost equally distributed over the entire level in the ciphered image. It can be concluded from Table III and Fig. 6, that the TIC scheme can effectively remove the correlation among the adjoin pixels in the original image and therefore it possesses a sturdy capability of tolerating the statistical analysis.

4) Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) Analysis:

For assessing the security and efficiency of TIC, two common metrics are utilized: MSE and PSNR. These metrics are described as [24, 25]:

$$MSE = \frac{1}{N \times N} \sum_{i=1}^{N} \sum_{j=1}^{N} [X(i,j) - Y(i,j)]^2 \tag{11}$$

$$PSNR = 10 \times log_{10} \left(\frac{255 \times 255}{MSE} \right) \tag{12}$$

where $X(i,j)$and $Y(i,j)$ represent the pixels values of the plain and ciphered/deciphered images, respectively. N represents the image size. Higher MSE and lower PSNR values indicate lesser similarity between the original and the ciphered images, while lower MSE and higher PSNR values imply higher similarity between the original and deciphered images. The values of MSE and PSNR between the original and the encrypted images are listed in Table II. The outcomes in this table suggest that the values of MSE are extremely high and the PSNR

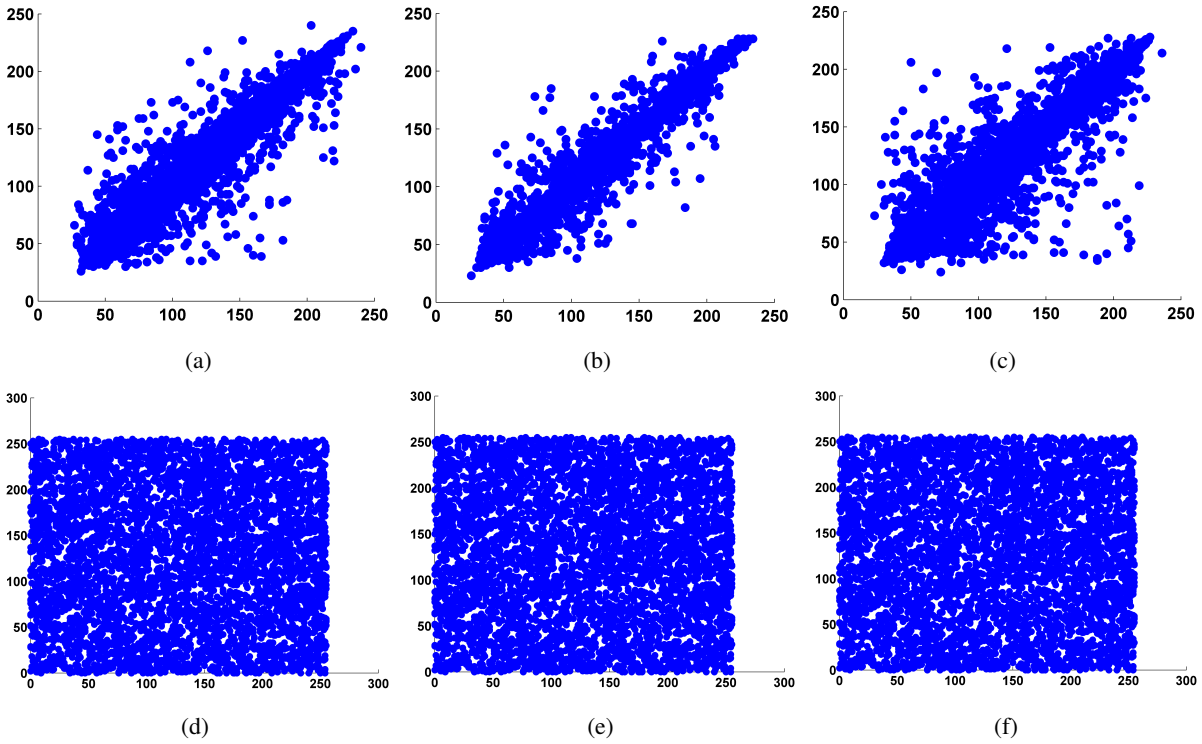


Fig. 6. Correlation of Neighbor Pixels for Lena Image (a) and (d) in Horizontal Direction for Plain and Cipher Images, Respectively (b) and (e) in Vertical Direction for Plain and Cipher Images, Respectively (c) and (f) in Diagonal Direction for Plain and Cipher Images, Respectively

values are quite low between the plaintext and encrypted images, which exhibits that the TIC can encrypt images with high quality.

B. Differential Analysis

One of the most desired attributes in an image ciphering system is its sensibility level to a trivial alteration in the plaintext image. An adversary usually tries to make tenuous modification in the input image such as changing only one pixel and then monitoring the alteration in the output ciphered image. The adversary expects by this way to find a beneficial relation between the input image and the encrypted image. If a slight alteration in the original image yields a totally different cipher image, then the differential analysis will be virtually infeasible. Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are the two common criteria utilized to examine the impact of changing one pixel on the ciphered image. These two criteria are given as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{13}$$

$$UACI = \frac{1}{M \times N}\left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100\% \tag{14}$$

$$D(i) = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{15}$$

where C_1 and C_2 indicate the to two ciphered images whose corresponding plain images with only one-pixel difference, M and N represent the width and height, respectively of C_1 or C_2. For grayscale image, the optimal values for UACI and NPCR are: 33.4635 % and 99.6094 %, respectively [20, 41–44]. The UACI and NPCR results generated via the TIC are reported in Table II. It can be observed from this table that all obtained NPCR and UACI values are close to the expected values. This demonstrates that the TIC possesses an extreme sensibility to pixel modulation in the original image and therefore it can effectively counter the differential attack.

TABLE II.
RESULTS OF INFORMATION ENTROPY, PSNR, MSE, UACI AND NPCR FOR THE TEST IMAGES

Image	Plain entropy	Cipher entropy	UACI (%)	NPCR (%)	PSNR (dB)	MSE
Cameraman	7.0097	7.9974	33.9472	99.61	6.3604	1.5033×10^4
Lena	7.4318	7.9971	33.3258	100	6.6813	1.3962×10^4
Baboon	7.2285	7.9970	33.2240	99.99	6.4303	1.4793×10^4
Barbara	7.3913	7.9974	33.7393	99.90	6.9521	1.3118×10^4
Boat	7.1583	7.9969	33.9939	99.86	5.8159	1.7041×10^4
Peppers	7.5647	7.9970	33.5428	99.74	6.4938	1.4578×10^4

TABLE III.
RESULTS OF CORRELATION COEFFICIENTS BETWEEN TWO NEIGHBORING PIXELS IN THE PLAIN AND ENCRYPTED IMAGES OVER THREE DIRECTIONS FOR THE TEST IMAGES

Image	Horizontal		Vertical		Diagonal	
	Plain image	Cipher image	Plain image	Cipher image	Plain image	Cipher image
Cameraman	0.9289	-9.6603×10^{-5}	0.9124	-3.9055×10^{-4}	0.9113	3.9393×10^{-4}
Lena	0.9492	4.9266×10^{-4}	0.9356	-3.6102×10^{-4}	0.9126	2.6482×10^{-4}
Baboon	0.8751	4.2133×10^{-5}	0.7643	-9.5688×10^{-4}	0.7780	-9.4679×10^{-4}
Barbara	0.9467	6.7268×10^{-4}	0.9345	4.7278×10^{-4}	0.9245	4.9117×10^{-4}
Boat	0.9506	-4.0670×10^{-4}	0.9140	1.7182×10^{-5}	0.9145	-5.4659×10^{-4}
Peppers	0.9424	-8.4578×10^{-4}	0.9122	-7.1571×10^{-4}	0.8963	6.2330×10^{-4}

C. Exhaustive Analysis

1) Key Space Analysis:

The most significant feature of any cryptography algorithm is the key space. Ideal cryptosystem should possess a large key space in order to defeat the exhaustive attack. Broadly, the key space size should be larger than 2^{100} [45–47]. The key space includes all the secret keys that have been utilized in the ciphering process. For the current method, the secret keys of RSA algorithm are p,q and d. In the confusion stage, Duffing map is adopted with two initial values: x_0, y_0, and two system parameters: a,b. In the diffusion stage, Lü system is exploited with three initial values: x_0, y_0, z_0, and three control parameters: a,b, c. Hence, there are totally 13 secret keys. If the computational accuracy of each secret key is 10^{-14}, then the key space size is equal to: $\left(10^{13}\right)^{14} = 10^{182} \approx 2^{605}$. So, this technique possesses an adequate large key space to counter the exhaustive attacks.

2) Key Sensitivity Analysis:

Ideal image cryptosystem should possess a high sensitivity to all of its secret keys used in both ciphering and deciphering phases to withstand the brute force attacks. This implies that a tenuous alteration in one of the utilized secret keys should yield a great deformation in the decrypted images. To test the keys sensitivity, Barbra image is encrypted using the TIC and the resultant ciphered image is clarified in Fig. 7a. Then, one secret key is changed (as example, the initial parameter (x_0 of Duffing map) with variation of $\Delta = 10^{-14}$, while preserving other keys values. This changed key is employed for deciphering the encrypted image to analyze the key sensibility in the decryption phase. The corresponding reconstructed images using these inaccurate keys are explained in Figs. 7c-7i, whereas the decrypted image by employing the right keys is displayed in Fig. 7b. It is explicit that the output decrypted images in these figures are quite distorted and any helpful information about the input image cannot be revealed even if a slight error occurred in the secret keys. Moreover, the cryptosystem is validated by calculating the PSNR, UACI, NPCR and correlation coefficient between the input image Barbara (Fig. 3d) and the other resultant decrypted images obtained from slightly altered keys (Figs. 7c- 7i) as listed in Table IV. The UACI and NPCR values in this table demonstrate that the differences between the original image (Fig. 3d) and the retrieved images (Figs. 7c-r7i) are more than 99 %, which means that almost all pixels are modulated as compared with the plaintext image. Additionally, the values of PSNR and the correlation are extremely small. From the results in Fig. 7 and Table IV, it can be disclosed that any trivial variation in the decryption keys yields a noisy restored image, which proves the algorithm sensibility to the decryption secret keys.

D. Computational Speed Analysis

Ciphering and deciphering speeds of any cryptographic system are significant criterion of security demands in order to

TABLE IV.
RESULTS OF KEY SENSITIVITY AT DECRYPTION WITH SLIGHTLY MODIFIED KEYS

Modified secret keys by adding Δ	UACI (%)	NPCR (%)	PSNR (dB)	r_{xy}
(d) of RSA algorithm	38.3964	99.62	9.1753	0.0024
(x_0) of Duffing map	35.1154	99.63	10.5947	-0.0068
(a) of Duffing map	35.0457	99.60	10.6220	-0.0191
(a) of Lü system	34.8304	99.61	7.6114	-0.0104
(b) of Lü system	34.8787	99.59	7.6073	-0.0212
(x_0) of Lü system	35.0486	99.64	7.5778	-0.0064
z_0 of Lü system	34.9767	99.57	7.5902	-0.0232

analyze the algorithm performance. The algorithm speed relies upon the time needed for both ciphering/deciphering operations. The required time for these two processes depends on several parameters like operating system used and its configuration, code optimization, and the utilized programing language [32, 33]. The information about the utilized environment for experiential findings has been mentioned in Section IV. The six test grayscale images with different sizes are utilized for assessing the TIC speed performance. The ciphering and deciphering time required for each image size are listed in Table V. It is observed from Table V that the requisite time for encryption and decryption stages is influenced by the image size, which implies that big image requires longer time. As an example, the proposed scheme needs 0.154946 s and 0.670657 s, respectively to cipher/decipher the Cameraman test image with size 256×256, while this time is increased to be 1.580442 s and 2.502797 s, respectively for the same image with size 1024×1024. Also, the decryption time is more than the encryption time for all test images. For instance, the time needed to encrypt the Lena image of size 256×256 is 0.162288 s, whereas the time required to decrypt the same image of same size is 0.643419 s. Based on the computed encryption/decryption time outcomes in Table V, it can be found that the ciphering time obtained by the presented work is considered very short for system having three stages of encryption: zigzag shuffling, RSA and chaotic maps with two phases: confusion and diffusion. Therefore, the TIC is efficient and fast to be utilized in practical applications to encrypt/decrypt images of various sizes throughout open networks.

E. Robustness Analysis

1) Noise Attack Analysis:

Robustness of the ciphered image to noise is an essential requirement for an efficient encryption scheme. Gaussian noise is the most common noise that may impact on the encrypted image during transmission [20]. This noise with different levels is added at the simulation to the encrypted image Boat for assessing the current algorithm performance. The cipher version of Boat is influenced by various densities of Gaussian noise (0.1, 0.05, 0.02, 0.01 and 0.006, respectively), and the obtained noisy decrypted images corresponding to the attacked cipher images are presented in Fig. 8. Furthermore, PSNR and correlation between the noisy restored images and original image Boat against noise density are shown in Fig. 9 to test the deciphered image quality at the receiver. It can be watched in these figures that the visual quality of the reconstructed image increases progressively as the noise intensity decreases, but the manifestation of the plain image can be readily recognized from the retrieved image even at high level of noise density in the ciphered image. Additionally, it is evident from Fig. 9 that PSNR and correlation values increase gradually with noise intensity decreasing, such that PSNR and correlation change from 14.8482 dB to be 26.6204 dB, and from 0.6977 to be 0.9242, respectively when the noise intensity varies from 0.1 to 0.006. It can be manifested from the above simulation outcomes that in the existence of noise, the deciphered image is shown visibly in spite of the high degree of noise density. Hence, the TIC can successfully resist the noise attack.

2) Cropping Attack Analysis:

Cropping attack analysis intends to evaluate the robustness of cryptosystem against cutting parts of the encrypted image through transmission [47]. The cipher image Peppers is attacked by cutting parts of various sizes from it to produce the attacked cipher images as exhibited in Figs. (10a-10e). Then, the attacked cipher images are deciphered to get the restored outcomes as revealed in Figs. (10f-10j), whereas the results of PSNR and correlation between the input and deciphered images for Peppers test image are tabulated in Table VI. It is obvious in these figures that when the cropping size is large (for example, 1/2 of the cipher image), the visible quality of deciphered image decreased; this quality is enhanced as the cropping size becomes small (for example, 1/8 of the cipher image). In addition, PSNR and correlation values in Table VI increase with the decreasing of crop size, such that these values vary from 10.0189 dB and 0.3957 to be 18.9409 dB

TABLE V.
RESULTS OF ENCRYPTION/DECRYPTION TIME MEASURED FOR TEST IMAGES WITH DIFFERENT SIZES

Image	Size	Encryption time (Second)	Decryption time (Second)
Cameraman	256x256	0.154946	0.670657
	512x512	0.527656	1.686384
	1024x1024	1.580442	2.502797
Lena	256x256	0.162288	0.643419
	512x512	0.378125	1.590626
	1024x1024	1.466533	2.325564
Baboon	256x256	0.131102	0.697361
	512x512	0.384833	1.627816
	1024x1024	1.453171	2.238646
Barbara	256x256	0.132878	0.728806
	512x512	0.390394	1.66202
	1024x1024	1.426099	2.303133
Boat	256x256	0.149949	0.672086
	512x512	0.339793	1.670934
	1024x1024	1.508857	2.39036
Peppers	256x256	0.143553	0.650492
	512x512	0.356593	1.628605
	1024x1024	1.462144	2.261963

TABLE VI.
RESULTS OF PSNR AND CORRELATION BETWEEN INPUT AND RECONSTRUCTED IMAGES UNDER CROPPING ATTACK.

Size of Cropping	PSNR (dB))	Correlation
Cropping ½	10.0189	0.3957
Cropping ¼ in bottom right	12.9694	0.6001
Cropping ¼ in top left	13.1048	0.6026
Cropping ¼ in center	13.1152	0.6241
Cropping 1/8 in top left	18.9409	0.8577

and 0.8577, respectively for PSNR and correlation. Also, different outcomes are obtained when changing the cropping location. For instance, cropping 1/4 from the bottom right of the cipher image yields 12.9694 dB and 0.6001 for PSNR and correlation, respectively, cropping 1/4 from the top left yields 13.1048 dB and 0.6026 for PSNR and correlation, respectively, while cropping 1/4 from the center part yields 13.1152 dB and 0.6241 for PSNR and correlation, respectively. Hence, the reconstructed image conserves the significant data included in the original image even if the cutting size reaches to half size of the cipher image thereby the TIC endures efficiently the cropping attack.

F. Case Study of the Proposed TIC Method

Table VII is presented in order to show the effect of each encryption stage of the proposed TIC algorithm in terms of information entropy, correlation coefficient in horizontal direction, MSE, PSNR, UACI, and NPCR. The results of these metrics are computed for Lena image of size 256×256. It can be noticed from the outcomes in this table that the entropy score after the zigzag scan stage remains constant (7.4318 in Table II, while this value increases after the second and third encryption stages to: 7.9950 and 7.9971, respectively. Also, the correlation value decreases from 0.9492 (Table III to: 0.1330, 0.0204 and 4.9266×10^{-4}, respectively after the first, second and third ciphering stages. Further, the value of MSE after the zigzag scan is 4.5449×10^3 . Then, this value increases to: 7.7540×10^3 and 1.3962×10^4, respectively after applying the RSA and chaotic systems. Contrariwise, the PSNR score decreases from 11.5556 at the first layer (zigzag scan) to: 9.2356 and 6.6813, respectively after employing the other encryption phases. Finally, for the UACI and NPCR, their values increase gradually from 27.4992 and 99.37, respectively to: 33.3258 and 100, respectively after implementing the RSA and chaotic maps.

From Table VII, it can be concluded that each technique has a significant role in the encryption process. The modified zigzag scan does not effect on the entropy value, but it is obviously effect on the other metrics. The impact of RSA mechanism on the increasing the entropy, MSE, UACI, NPCR values, and decreasing the correlation and PSNR values is extremely clear. Finally, the high dimension chaotic maps with confusion/diffusion processes can further improve the

results. Thus, the combination of these three encryption methods (zigzag scan, RSA and chaos) makes the proposed TIC cryptosystem quite strong and robust.

G. Comparison of Cryptosystem Performance with Related Methods

TIC performance is compared with many related existing image cryptosystems in order to evince its superiority. The sample images of size 256×256 are used in this comparison and the outcomes are illustrated in Tables VIII-X. Table VIII shows the security comparison in terms of information entropy, PSNR, UACI, NPCR, and correlation values along the three directions. Table IX gives the key space comparison, and Table X lists the speed analysis comparison with other approaches.

For Table VIII, it can found that the presented scheme achieves higher entropy scores or equal to those outcomes acquired via other approaches except for Ref. [44] at Lena image, Ref. [34] at Baboon and Peppers image, and Ref. [36] at Baboon, Boat and Peppers images. Also, the PSNR values generated by the introduced algorithm are smaller than the other current methods. Besides, this technique attains better values in terms of NPCR except for Ref. [34] at Cameraman image. Moreover, the UACI results produced by this cryptosystem are larger or closer to those gained by other algorithms expect for Ref. [44] at Lena image. Finally, the correlation coefficients scores obtained via this mechanism along three directions are lower or nearer in comparison with the existing references.

Table IX reveals that the key space size of the proposed technology is the largest as compared with other methods. This is because using high dimensional Duffing and Lü chaotic systems with multiple initial conditions/control parameters. Furthermore, the described mechanism possesses the shortest ciphering time among the compared references as clarified in Table X except for Ref. [16] at Cameraman, Lena, Barbara and Peppers images of size (512×512), and Ref. [26] at Boat image of size (256×256). It can be deduced from Tables VIII-X that the TIC possesses a superior security performance and high speed. Therefore, it is suitable for satisfying real-time communication applications.

V. Conclusion

This article presents a new efficient image encryption strategy based on combining zigzag scan, RSA coding and chaotic systems. After splitting the input image into a specific number of non-overlapping blocks, the zigzag scan is modified to be with a variable starting pixel, then it is implemented in two different directions in order to shuffle the image pixels. Asymmetric key RSA algorithm is applied secondly on the scrambled image. Finally, chaotic systems are utilized to implement the confusion-diffusion processes. The important conclusions about the proposed work can be summarized as follows:

- Appling the zigzag scan in two different directions and with a variable starting pixel on the non-overlapping blocks yields a higher secure scrambling degree.
- Appling the RSA technique increases the security level of the TIC by selecting a large prime number modulo which requires an extremely long time to break it.
- Adopting higher dimensional chaotic maps improves the resistance against the exhaustive attack since the size of key space depends on the values of system parameters/initial conditions.
- The proposed TIC is very sensitive to the key alteration such that the differences between the original and deciphered images are more than 99 % for a tiny change in one of the TIC keys values.
- The presented cryptosystem is evaluated based on comprehensive performance analysis and comparison analysis with several common existing methods; the results prove the encryption effectiveness of the TIC for all the tested images.
- In summary, the TIC possesses a high sensibility to the key change, a large key space, a high immunity to the cryptographic attacks, and fast processing time. Therefore, the presented approach provides a perfect candidate for secure image applications such as online wireless communication.
- For future work, the proposed technique can be applied upon other types of digital images like color images, medical images, biometric images or remote sensing images. Also, the decryption time of the suggested cryptosystem is slightly longer than the encryption time; this time can be improved to make it more adequate for real-time cryptographic applications.

Conflict of Interest

The authors have no conflict of relevant interest to this article.

References

[1] A. S. Hameed, "Speech scrambling based on synchronization of jointed dynamic parameter chaotic map," *Telecommunications and Radio Engineering*, vol. 80, no. 8, 2021.

TABLE VII.
RESULTS OF PERFORMANCE METRIC FOR LENA IMAGE AT EACH ENCRYPTION STAGE.

Encryption stage	Entropy	Correlation (H)	MSE	PSNR (dB)	UACI (%)	NPCR (%)
Zigzag scan	7.4318	0.1330	4.5449×10^3	11.5556	27.4992	99.37
Zigzag scan and RSA	7.9950	0.0204	7.7540×10^3	9.2356	30.3229	99.61
Zigzag scan, RSA and Chaotic systems	7.9971	4.9266×10^{-4}	1.3962×10^4	6.6813	33.3258	100

TABLE VIII.
INFORMATION ENTROPY, PSNR, UACI, NPCR, AND CORRELATION COFFICIENT COMPARISON

Image	Method	Entropy	PSNR	UACI (%)	NPCR (%)	Correlation Coefficients		
						Horizontal	Vertical	Diagonal
Cameraman	Ref. [17]	7.9974	-	-	-	- 0.0009180	0.0036695	0.0002067
	Ref. [23]	7.9969	-	33.46	99.61	-0.0011	0.0114	-0.0032
	Ref. [34]	7.9968	9.2118	33.4538	99.6521	0.0149	0.0162	-0.0168
	Proposed	7.9974	6.3604	33.9472	99.61	-9.6603×10^{-5}	-3.9055×10^{-4}	3.9393×10^{-4}
Lena	Ref. [17]	7.9968	-	-	-	-	-	-
	Ref. [18]	7.9968	-	-	-	0.0012	0.0026	0.0021
	Ref. [21]	7.9971	-	33.5053	99.5712	0.0015	0.0018	0.0018
	Ref. [26]	7.9970	-	33.3537	99.6109	-	-	-
	Ref. [28]	7.9762	9.808	26.51	99.54	-0.00011	0.0024	-0.0012
	Ref. [34]	7.9969	9.2198	33.4271	99.6460	0.0222	0.0354	0.0006
	Ref. [44]	7.9980	-	38	99.61	0.0036	0.0023	0.0039
	Proposed	7.9971	6.6813	33.3258	100	4.9266×10^{-4}	-3.6102×10^{-4}	2.6482×10^{-4}
Baboon	Ref. [28]	7.9434	10.747	23.77	99.49	-0.00021	0.0022	0.0033
	Ref. [34]	7.9976	9.1916	33.4309	99.6426	0.0346	0.0205	-0.0049
	Ref. [36]	7.9973	-	33.35	99.58	- 0.0040	0.0007	0.0015
	Proposed	7.9970	6.4303	33.2240	99.99	4.2133×10^{-5}	-9.5688×10^{-4}	-9.4679×10^{-4}
Boat	Ref. [17]	7.9967	-	-	-	-	-	-
	Ref. [36]	7.9975	-	33.40	99.61	0.0047	0.0007	0.0007
	Proposed	7.9969	5.8159	33.9939	99.86	-4.0670×10^{-4}	1.7182×10^{-5}	-5.4659×10^{-4}
Peppers	Ref. [34]	7.9976	9.2210	33.4078	99.6475	0.0017	0.0222	0.0076
	Ref. [36]	7.9974	-	33.42	99.58	-0.0038	0.0084	-0.0017
	Proposed	7.9970	6.4938	33.5428	99.74	-8.4578×10^{-4}	-7.1571×10^{-4}	6.2330×10^{-4}

TABLE IX.
KEY SPACE COMPARISON

Method	Key space
Ref. [17]	2^{213}
Ref. [18]	2^{233}
Ref. [19]	2^{375}
Ref. [23]	2^{325}
Ref. [26]	2^{186}
Ref. [27]	2^{216}
Ref. [29]	2^{398}
Ref. [30]	2^{435}
Ref. [33]	2^{392}
Ref. [34]	9×2^{528}
Ref. [41]	2^{256}
Ref. [42]	2^{455}
Ref. [44]	2^{239}
Ref. [47]	2^{465}
Proposed	2^{605}

[2] O. A. Imran, S. F. Yousif, I. S. Hameed, W. N. A.-D. Abed, and A. T. Hammid, "Implementation of el-gamal algorithm for speech signals encryption and decryption," *Procedia Computer Science*, vol. 167, pp. 1028–1037, 2020.

[3] S. F. Yousif, "Encryption and decryption of audio signal based on rsa algorithn," *International Journal of Engineering Technologies and Management Research*, vol. 5, no. 7, pp. 57–64, 2018.

[4] S. F. Yousif, "Secure voice cryptography based on diffie-hellman algorithm," in *IOP Conference Series: Materials Science and Engineering*, vol. 1076, p. 012057, IOP Publishing, 2021.

[5] S. F. Yousif, A. J. Abboud, and H. Y. Radhi, "Robust image encryption with scanning technology, the el-gamal algorithm and chaos theory," *IEEE Access*, vol. 8, pp. 155184–155209, 2020.

[6] U. Zia, M. McCartney, B. Scotney, J. Martinez, M. Abu-Tair, J. Memon, and A. Sajjad, "Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains," *International Journal of Information Security*, vol. 21, no. 4, pp. 917–935, 2022.

[7] Z. Tang, Y. Yang, S. Xu, C. Yu, X. Zhang, *et al.*, "Image encryption with double spiral scans and chaotic maps," *Security and Communication Networks*, vol. 2019, 2019.

[8] C. Fu, G.-y. Zhang, M. Zhu, Z. Chen, and W.-m. Lei, "A new chaos-based color image encryption scheme with an efficient substitution keystream generation strategy," *Security and Communication Networks*, vol. 2018, pp. 1–13, 2018.

[9] A. S. Hameed, "Speech compression and encryption based on discrete wavelet transform and chaotic signals," *Multimedia Tools and Applications*, vol. 80, no. 9, pp. 13663–13676, 2021.

[10] S. F. Yousif, A. J. Abboud, and R. S. Alhumaima, "A new image encryption based on bit replacing, chaos and dna coding techniques," *Multimedia Tools and Applications*, vol. 81, no. 19, pp. 27453–27493, 2022.

[11] H. N. Abdullah, S. F. Yousif, and A. A. Valenzuela, "Efficient steganography scheme for color images based on wavelets and chaotic maps," *Iraqi Journal of Information and Communication Technology*, vol. 2, no. 4, pp. 11–20, 2019.

[12] S. F. Yousif, "Speech encryption based on zaslavsky map," *J. Eng. Appl. Sci*, vol. 14, no. 17, pp. 6392–6399, 2019.

[13] S. F. Yousif, "Grayscale image confusion and diffusion based on multiple chaotic maps," in *2018 1st International scientific conference of engineering sciences-3rd scientific conference of engineering science (ISCES)*, pp. 114–119, IEEE, 2018.

[14] S. F. Yousif, "A new speech cryptosystem using dna encoding, genetic and rsa algorithms," *International*

Journal of Engineering & Technology, vol. 7, no. 4, pp. 4550–4557, 2018.

[15] A. S. Hameed, "High data rate of a novel modulation scheme based on orthogonal chaotic signals," *Telecommunications and Radio Engineering*, vol. 75, no. 18, 2016.

[16] R. M. Rad, A. Attar, and R. E. Atani, "A new fast and simple image encryption algorithm using scan patterns and xor," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 6, no. 5, pp. 275–290, 2013.

[17] X. Deng, C. Liao, C. Zhu, and Z. Chen, "A novel image encryption algorithm based on hyperchaotic system and shuffling scheme," in *2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing*, pp. 109–116, IEEE, 2013.

[18] Q. Zhang, L. Guo, and X. Wei, "A novel image fusion encryption algorithm based on dna sequence operation and hyper-chaotic system," *Optik-International Journal for Light and Electron Optics*, vol. 124, no. 18, pp. 3596–3600, 2013.

[19] B. Stoyanov, K. Kordov, *et al.*, "Novel image encryption scheme based on chebyshev polynomial and duffing map," *The Scientific World Journal*, vol. 2014, 2014.

[20] E. A. Naeem, M. M. Abd Elnaby, N. F. Soliman, A. M. Abbas, O. S. Faragallah, N. Semary, M. M. Hadhoud, S. A. Alshebeili, and F. E. Abd El-Samie, "Efficient implementation of chaotic image encryption in transform domains," *Journal of Systems and Software*, vol. 97, pp. 118–127, 2014.

[21] H. Niu, C. Zhou, B. Wang, X. Zheng, and S. Zhou, "Splicing model and hyper–chaotic system for image encryption," *Journal of Electrical Engineering*, vol. 67, no. 2, pp. 78–86, 2016.

[22] S. Somaraj and M. AliHussain, "An image encryption technique using scan based approach and image as key," in *Proceedings of the First International Conference on Computational Intelligence and Informatics: ICCII 2016*, pp. 645–653, Springer, 2017.

[23] X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu, "A novel image encryption scheme based on dna sequence operations and chaotic systems," *Neural Computing and Applications*, vol. 31, pp. 219–237, 2019.

[24] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, 2018.

[25] Nasrullah, J. Sang, M. A. Akbar, B. Cai, H. Xiang, and H. Hu, "Joint image compression and encryption using iwt with spiht, kd-tree and chaotic maps," *Applied Sciences*, vol. 8, no. 10, p. 1963, 2018.

[26] X. Huang and G. Ye, "An image encryption algorithm based on time-delay and random insertion," *Entropy*, vol. 20, no. 12, p. 974, 2018.

[27] C. Liu and Q. Ding, "A color image encryption scheme based on a novel 3d chaotic mapping," *Complexity*, vol. 2020, pp. 1–20, 2020.

[28] J. Ferdush, M. Begum, and M. S. Uddin, "Chaotic lightweight cryptosystem for image encryption," *Advances in Multimedia*, vol. 2021, pp. 1–16, 2021.

[29] T. S. Ali and R. Ali, "A novel color image encryption scheme based on a new dynamic compound chaotic map and s-box," *Multimedia Tools and Applications*, vol. 81, no. 15, pp. 20585–20609, 2022.

[30] X. Gao, M. Miao, and X. Chen, "Multi-image encryption algorithm for 2d and 3d images based on chaotic system," *Frontiers in Physics*, vol. 10, p. 901800, 2022.

[31] N. Chaudhary, T. B. Shahi, and A. Neupane, "Secure image encryption using chaotic, hybrid chaotic and block cipher approach," *Journal of Imaging*, vol. 8, no. 6, p. 167, 2022.

[32] Z. Cheng, W. Wang, Y. Dai, and L. Li, "A high-security privacy image encryption algorithm based on chaos and double encryption strategy," *Journal of Applied Mathematics*, vol. 2022, 2022.

[33] N. A. E.-S. Mohamed, A. Youssif, H. A.-G. El-Sayed, *et al.*, "Fast and robust image encryption scheme based on quantum logistic map and hyperchaotic system," *Complexity*, vol. 2022, 2022.

[34] M. Akraam, T. Rashid, S. Zafar, *et al.*, "A chaos-based image encryption scheme is proposed using multiple chaotic maps," *Mathematical Problems in Engineering*, vol. 2023, 2023.

[35] H. Gururaj, M. Almeshari, Y. Alzamil, V. Ravi, and K. Sudeesh, "Efficient scan and chaotic map encryption system for securing e-healthcare images," *Information*, vol. 14, no. 1, p. 47, 2023.

[36] A. A. Neamah, "An image encryption scheme based on a seven-dimensional hyperchaotic system and pascal's matrix," *Journal of King Saud University-Computer and Information Sciences*, vol. 35, no. 3, pp. 238–248, 2023.

[37] R. Candra, S. Madenda, S. A. Sudiro, and M. Subali, "The implementation of an efficient zigzag scan," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 9, no. 2, pp. 95–98, 2017.

[38] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[39] J. Lü and G. Chen, "A new chaotic attractor coined," *International Journal of Bifurcation and chaos*, vol. 12, no. 03, pp. 659–661, 2002.

[40] S. Pang and Y. Liu, "A new hyperchaotic system from the lü system and its control," *Journal of Computational and Applied Mathematics*, vol. 235, no. 8, pp. 2775–2789, 2011.

[41] Y. Chen, C. Tang, and Z. Yi, "A novel image encryption scheme based on pwlcm and standard map," *Complexity*, vol. 2020, pp. 1–23, 2020.

[42] Z. Li, C. Peng, W. Tan, and L. Li, "An effective chaos-based image encryption scheme using imitating jigsaw method," *Complexity*, vol. 2021, pp. 1–18, 2021.

[43] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, "Multiple grayscale image encryption using cross-coupled chaotic maps," *Journal of Information Security and Applications*, vol. 52, p. 102470, 2020.

[44] Q. Zhang, L. Guo, and X. Wei, "Image encryption using dna addition combining with chaotic maps," *Mathematical and Computer Modelling*, vol. 52, no. 11-12, pp. 2028–2035, 2010.

[45] A. S. Hameed, "Image encryption based on fractional order lorenz system and wavelet transform," *Diyala journal of engineering sciences*, pp. 81–91, 2017.

[46] J. N. Shehab, H. Y. Radhi, and R. A. Ibrahim, "Multimedia cryptography based on liu and chen systems," *Diyala Journal of Engineering Sciences*, pp. 24–35, 2016.

[47] J. Wu, X. Liao, and B. Yang, "Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation," *Signal Processing*, vol. 142, pp. 292–300, 2018.

TABLE X.
SPEED COMPARISON

Image	Size	Method	Encryption time
Cameraman	256×256	Ref. [24]	0.71
		Ref. [34]	3.319
		Proposed	0.154946
Cameraman	512×512	Ref. [16]	0.1120
		Proposed	0.527656
Lena	256×256	Ref. [24]	0.58
		Ref. [28]	2.227
		Ref. [34]	3.222
		Proposed	0.162288
Lena	512×512	Ref. [7]	2.792
		Ref. [16]	0.1022
		Ref. [25]	19.2
		Ref. [28]	9.5097
		Ref. [32]	0.336
		Ref. [47]	7.75
		Proposed	0.378125
Baboon	256×256	Ref. [24]	0.47
		Ref. [28]	2.2441
		Ref. [34]	3.259
		Ref. [36]	0.250984
		Proposed	0.131102
Baboon	512×512	Ref. [25]	18.7
		Ref. [28]	8.8939
		Ref. [36]	0.684918
		Proposed	0.384833
Barbara	512×512	Ref. [16]	0.1010
		Proposed	0.390394
Boat	256×256	Ref. [26]	0.137
		Ref. [36]	0.259434
		Proposed	0.149949
Boat	512×512	Ref. [33]	1.4375
		Ref. [36]	0.707523
		Proposed	0.339793
Peppers	256×256	Ref. [24]	0.66
		Ref. [34]	3.316
		Ref. [36]	0.253761
		Proposed	0.143553
Peppers	512×512	Ref. [16]	0.1051
		Ref. [25]	19.5
		Ref. [36]	0.688577
		Proposed	0.356593

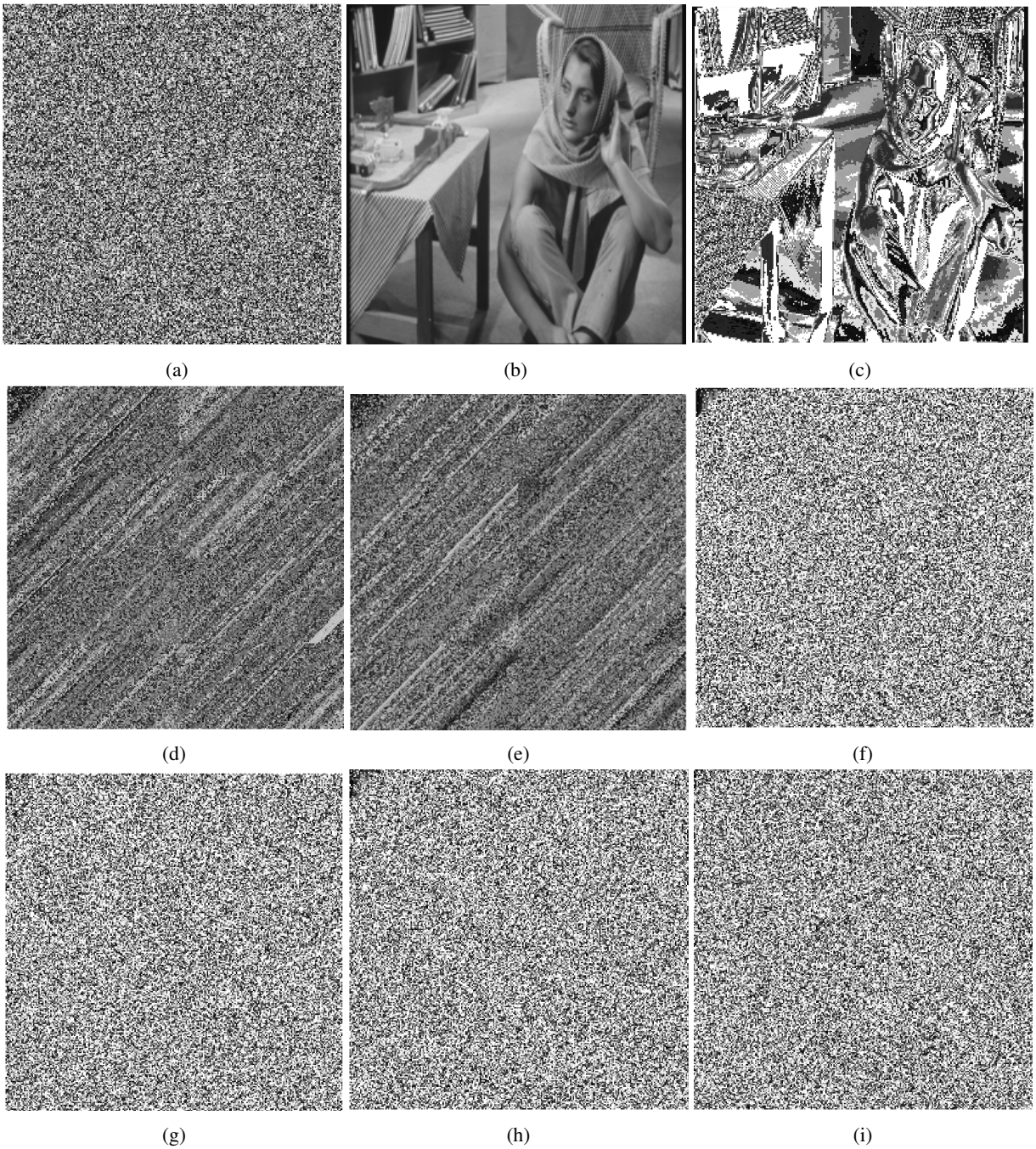
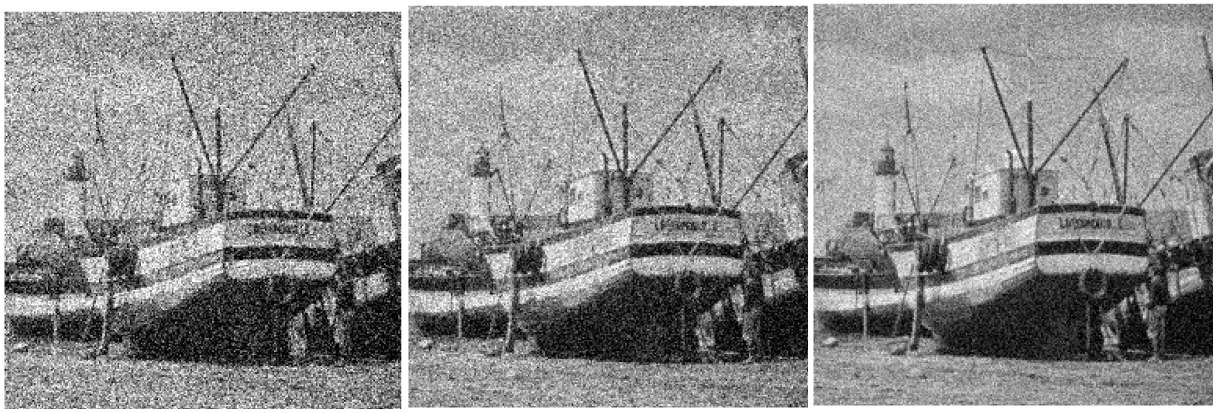


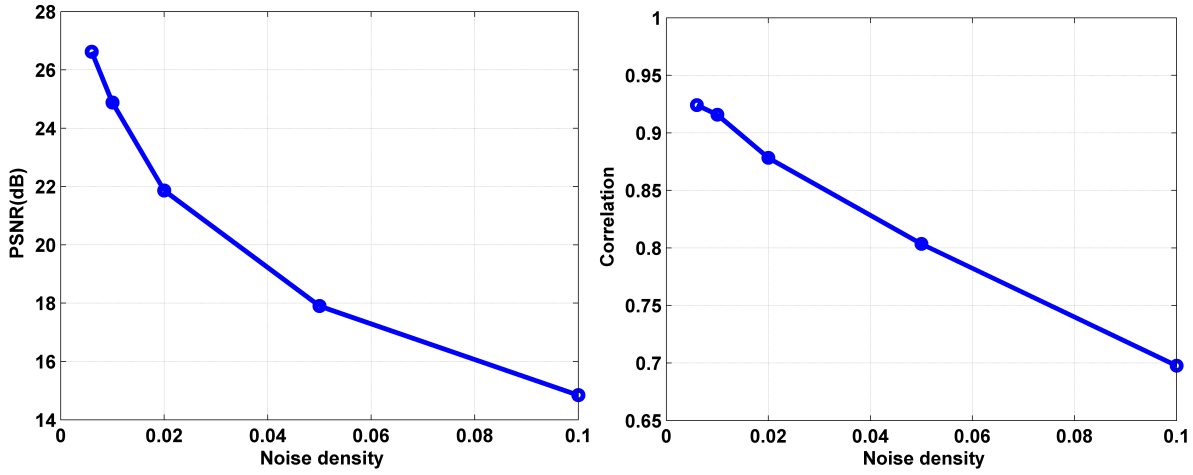
Fig. 7. Results of Key Sensitivity Test (a) Cipher Image (b) Decipher Image Using Correct Keys (c) Decipher Image Using Modified d of RSA (d) Decipher Image Using Modified x_0 of Duffing Map (e) Decipher Image Using Modified a of Duffing Map (f) Decipher Image Using Modified a of Lü System (g) Decipher Image Using Modified b of Lü System (h) Decipher Image Using Modified x_0 of Lü System (i) Decipher Image Using Modified z_0 of Lü System



(a) (b) (c)

(d) (e)

Fig. 8. Deciphered Images Under Gaussian Noise Attack of Different Intensities (a) Noise Intensity is 0.1 (b) Noise Intensity is 0.05 (c) Noise Intensity is 0.02 (d) Noise Intensity is 0.01 (e) Noise Intensity is 0.006



(a) (b)

Fig. 9. Plot of (a) PSNR (b) Correlation Between the Original and Deciphered Images Under Various Levels of Gaussian Noise Density for Boat Image

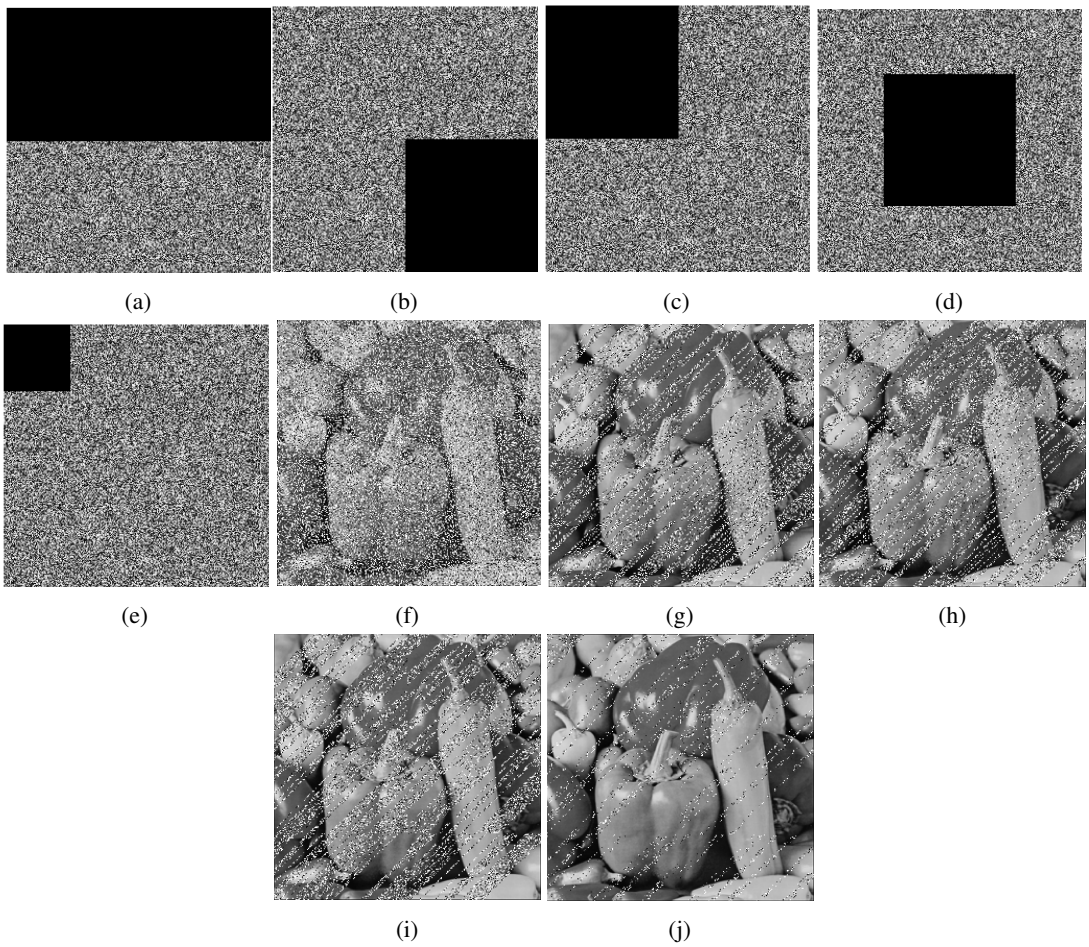


Fig. 10. Results of Cropping Attack on Peppers Ciphered and Deciphered Images (a) Cropping ½. (b) Cropping ¼ in the Bottom Right Corner. (c) Cropping ¼ in the Top Left Corner (d) Cropping ¼ in the Center Part. (e) Cropping 1/8 in the Top Left Corner of the Encrypted Image (f) Restored Image of (a) (g) Restored Image of (b) (h) Restored Image of (c) (i) Restored Image of (d) (j) Restored Image of (e)