Multimed Tools Appl (2018) 77:25223–25251
https://doi.org/10.1007/s11042-018-5782-2

Image encryption based on modified Henon map using hybrid chaotic shift transform

S. J. Sheela[1] · **K. V. Suresh**[1] · **Deepaknath Tandur**[2]

Received: 7 April 2017 / Revised: 15 December 2017 / Accepted: 9 February 2018 /
Published online: 21 March 2018

Abstract In this paper, a new two dimensional modified Henon map (2D-MHM) which is derived from Henon map is proposed. Its chaotic performance is analyzed through bifurcation diagram, Lyapunov exponent spectrum and Lyapunov dimension. The map has broad chaotic regime over an extensive range of system parameters, maximum Lyapunov exponent and better chaotic performance when compared to existing chaotic maps. Further, a novel image cryptosystem is proposed based on 2D-MHM and sine map. The algorithm employs confusion and diffusion operations in consecutive manner which is different from traditional chaos based cryptosystems. Hybrid chaotic shift transform (HCST) is introduced to perform confusion operation which is controlled by 2D-MHM. The principle of diffusion is achieved by using chaotic matrix generated from sine map and exclusive or (XOR) operation. Extensive simulation results and performance analysis demonstrate that the proposed image cryptosystem is able to resist various cryptanalytic attacks. Furthermore, the comparison results reveal that the algorithm outperforms traditional and existing encryption schemes. The proposed algorithm is also applicable for speech signals and data encryption of other multimedia.

Keywords Chaos · Confusion · Diffusion · 2D-modified Henon map · Hybrid chaotic shift transform

✉ S. J. Sheela
sheeladinu@sit.ac.in

K. V. Suresh
sureshkvsit@sit.ac.in

Deepaknath Tandur
deepaknath.tandur@in.abb.com

[1] Siddaganga Institute of Technology, Tumakuru, Karnataka 572103, India

[2] Corporate Research India, ABB, Bengaluru, Karnataka 560048, India

1 Introduction

Secured storage and transmission of the digital image is one of the prime concerns in multimedia communication. Cryptography, steganography and watermarking are the three ways to protect digital data from unauthorized access and illegal usage. Among these, cryptography plays a significant role in providing highly secured transmission over insecure channel. The cryptographic algorithms are classified into stream ciphers and block ciphers. In stream ciphers the digital data is encrypted bit by bit using a secret key generator while in block ciphers blocks of bits are encrypted. Most commonly used stream ciphers are linear feedback shift register (LFSR) based stream cipher and RC4. Block ciphers include the well known advanced encryption standard (AES), data encryption standard (DES), triple DES (TDES) [30, 31] etc. However, these conventional algorithms are not appropriate for image encryption due to some inherent characteristics of digital images such as high degree of redundancy among the pixels, bulk volume of data, replication of more pixels etc. Moreover, these ciphers require more amount of time, computational resources and high power for real time image encryption [46, 50]. In order to overcome these difficulties, numerous encryption algorithms based on optical transformation [11, 28], DNA computing [16, 34, 49], cellular automata [8], chaotic maps [5, 14, 18, 23–25, 40, 43, 49, 51] and others [21, 29] have been proposed. As many studies have revealed [10, 13, 48] that intrinsic properties of the chaotic maps are equivalent to the counterparts of cryptography. Hence, chaotic systems are the perfect candidate for cryptography which has been extensively used in image encryption.

Many researchers have identified the dynamic and disordered behavior in iterated functions which are chaotic maps. The idea of information encryption based on chaotic map was first proposed by Matthew [27]. In 1997, Fridrich [10] first proposed chaos based image encryption scheme which consists of two stages: confusion and diffusion. Confusion and diffusion stages are applied to scramble pixel positions randomly and to change the pixel values respectively. Most of the chaos based encryption schemes employ diffusion operation after shuffling the original image [14, 36, 47]. Moreover, some researchers have combined these two phases into one stage in order to get substantial improvement with respect to security [23, 38].

The chaotic maps which are used in image encryption schemes can be divided into two categories: one dimensional(1D) and higher dimensional chaotic map. Generally, 1D chaotic map is characterized by one variable and few system parameters. Some examples of 1D chaotic maps are logistic, sine, cubic map [6] etc. Some of them utilize various one dimensional chaotic maps in the development of security system because of their exceptional features, high speed encryption and simple structures. However, 1D chaotic maps result in single simple predictable chaotic orbits. As a result, the initial states and/or system parameters of the chaotic map can be obtained easily [17]. Hence, one dimensional chaotic maps cannot be used in the encryption of images because of small key space, stable windows, weak security and vulnerability to attacks [20, 22, 42]. In this regard, image encryption schemes based on coupled and modified 1D chaotic maps [4, 19, 42] which have more complex chaotic behavior than their original chaotic maps were proposed. The merit of these schemes are larger key space and good security results. On the other hand, security can be enhanced by increasing the dimension which in turn increases the nonlinearity. The higher dimensional (HD) chaotic maps are widely used in multimedia encryption owing to tough prediction of a time series and more numbers of positive Lyapunov exponents [43]. Furthermore, in HD chaotic system, the primitive operations of cryptography can be performed in multiple directions and helps to decorrelate the relation between the pixels quickly

[35]. However, higher dimensional chaotic systems have some drawbacks such as complex performance analysis and high implementation costs [45].

Modification of the existing chaotic maps thereby identifying and improving the chaotic region is one of the exciting fields in the dynamical systems theory. Hence, the modification of two dimensional (2D) Henon map, called 2D modified Henon map is introduced in this paper. The modification of Henon map is considered to increase the chaotic region thereby improving the range of system parameters. The chaotic behavior of the modified Henon map is analyzed and compared with original Henon map (HM) through bifurcation diagram and Lyapunov exponent. Further, the paper proposes a new image encryption scheme based on 2D-MHM and sine map (SM). This encryption scheme employs confusion and diffusion operations which is influenced by one after the other. The hybrid chaotic shift transform is proposed to scramble column and row pixel positions efficiently. And diffusion operation is controlled by chaotic matrix generated from the SM, previous encrypted pixel and current scrambled pixel. The encryption capability of the algorithm is assessed through security analysis for various synthetic images of different sizes.

Rest of the paper is organized in the following way. The novelty of the paper is listed in Section 2. Section 3 introduces the chaotic maps along with its dynamical behavior. HCST based image encryption algorithm is presented in Section 4. Results of security analysis are provided in Section 5. Final section concludes the paper.

2 Contribution of the paper

The novelty of this paper are as follows.

1. The Henon map is modified in order to increase the chaotic region which in turn improves the range of system parameters.
2. The chaotic behavior of the MHM is analyzed and compared with existing 2D maps.
3. The complex chaotic behavior of the MHM is explored and proposed a new image cryptosystem by utilizing MHM and SM.
4. The cryptographic primitive operations are followed strictly in consecutive manner with new techniques.

3 Chaotic maps

This section reviews existing chaotic maps such as HM and SM along with their dynamical behavior. Further, evaluation and comparison of dynamical behavior of MHM with HM is considered.

3.1 Henon map

French mathematician and astronomer Michel Henon in 1976 [15] proposed a two dimensional map called Henon map. Henon map is the simplest invertible map with quadratic nonlinearity in R^2 given by

$$\begin{aligned} x_{k+1} &= 1 - b_1 x_k^2 + b_2 y_k \\ y_{k+1} &= x_k \end{aligned} \tag{1}$$

Here (x_k, y_k) represents the two dimensional state of the system. The system parameters b_1 and b_2 yield the chaotic attractor for a range of values. In order to obtain fine

structure of the chaotic attractor, the system parameters should not be too large or too small. Attractor doesn't exist, if b_1 is too small or too large. The area of contraction will be excessive, if b_2 is too close to zero. On the other hand, the folding won't be strong enough if it is too large. The fine structure of the chaotic attractor can be obtained by selecting b_1 and b_2 as 1.4 and 0.3 respectively. Other chaotic attractors can be obtained by modifying these two parameters b_1 and b_2. The bounded solution can be obtained by selecting the proper nonlinear term and system parameters. Henon map has bounded solution for the parameter values $-1 < b_1 < 2$ and $|b_2| < 1$ and chaotic attractors can be obtained over some range of values. Henon map is simple to implement and easily accords itself to numerical explorations. But Henon map exhibits the chaotic behavior in the range of $b_1 \in [1.06, 1.4]$ which is shown in Fig. 1a. This drawback restricts its application in many security areas such as multiple real time image encryptions. In order to address this problem, Henon map is modified by replacing x_k^2 term by nonlinear term $cos(x_k)$ and $b_2 \neq 0$.

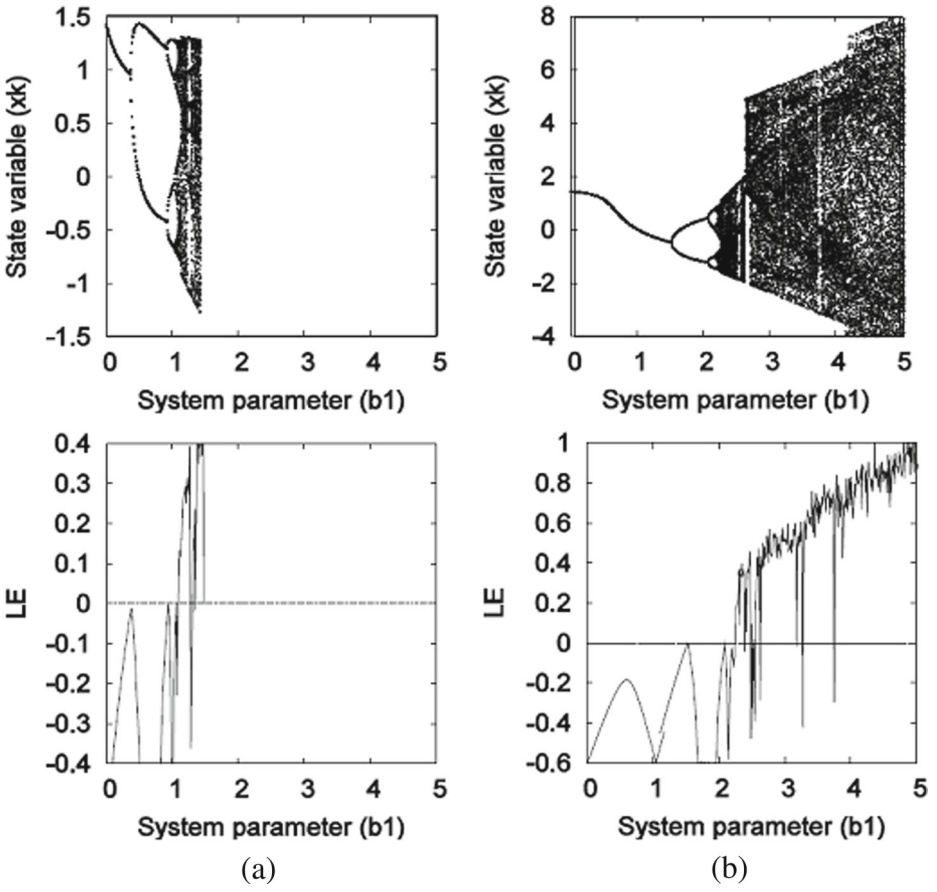

Fig. 1 **a** Bifurcation diagram and Lyapunov Exponent of the Henon map for the system parameter ($b_2 = 0.3$). **b** Bifurcation diagram and Lyapunov Exponent of the modified Henon map for the system parameter ($b_2 = 0.3$)

3.2 Modified Henon map

The modified Henon map is given by

$$H(x_k, y_k) = \begin{pmatrix} x_{k+1} \\ y_{k+1} \end{pmatrix} = \begin{pmatrix} 1 - b_1 cos(x_k) - b_2 y_k \\ -x_k \end{pmatrix} \quad (2)$$

For modified Henon map, the bounded solutions will be obtained for all values of b_1 and $|b_2| < 1$. A wide chaotic range can be obtained by selecting one of the system parameters $b_2 = 0.3$. The modified Henon map has broad array of chaotic regime over an extensive range of system parameters which is evidenced through bifurcation diagram and Lyapunov exponent shown in Fig. 1b.

3.3 Performance analysis and comparison

In this subsection, the chaotic performance of MHM is evaluated using bifurcation diagram, correlation test, Lyapunov exponent and dimension and it is compared with Henon map.

3.3.1 Bifurcation diagram and largest Lyapunov exponent

The investigation and comparison of the dynamical behavior of the system with parameter variation of original Henon map as well as modified Henon map is considered in this subsection. In order to use the chaotic map in a specific application, it is necessary to know the chaotic region which needs the investigation of the dynamic behavior. Discrete map changes suddenly from fixed and periodic points to chaotic behavior in many ways. This is evidenced through bifurcation diagram and largest Lyapunov exponent which helps to find chaotic region which in turn determines the fixed and periodic points. The bifurcation diagram plots output sequences of a chaotic map along with the change in system parameter(s) whereas Lyapunov exponent characterizes and quantifies the sustained chaotic behavior. The bifurcation diagram and Lyapunov exponent of original Henon map plotted by varying system parameter in the interval $0 \leq b_1 \leq 5$ with state variable (x_k) for the case $b_2 = 0.3$ is shown in Fig. 1a. For modified Henon map, these diagrams are drawn over the same range which is depicted in Fig. 1b. The different regions in the bifurcation diagram of MHM and Henon map are listed in Table 1. From the bifurcation diagram, it is clear that Henon map is chaotic for the range of $b_1 \in [1.06, 1.22] \cup [1.27, 1.29] \cup [1.31, 1.4]$ whereas modified Henon map is chaotic for the range of $b_1 \in [2.19, 2.5] \cup [> 2.54]$ in the interval $0 \leq b_1 \leq 5$. Thus, the simulation results show an improvement in the chaotic range ratio of 7% to 56% in this interval. Further, the 2D logistic map [41] has its chaotic behavior when the system parameter $r \in [1.11, 1.15] \cup [1.18, 1.19]$. The results of comparison of MHM with 2D

Table 1 Different regions in the bifurcation diagram of the map

	Henon map		Modified Henon map	
Nature of the dynamic behavior	b_1	b_2	b_1	b_2
Fixed point	$0 \leq b_1 \leq 0.35$	0.3	$0 \leq b_1 \leq 1.5$	0.3
Period-doubling cascade	$0.35 < b_1 \leq 1.06$	0.3	$1.5 < b_1 \leq 2.19$	0.3
Chaotic Attractor	$1.06 < b_1 \leq 1.22$	0.3	$2.19 < b_1 \leq 2.5$	0.3
Fixed point	$1.22 < b_1 \leq 1.27$	0.3	$2.5 < b_1 \leq 2.54$	0.3
Chaotic Range	$1.27 < b_1 \leq 1.4$	0.3	$b_1 > 2.54$	0.3

Table 2 Complexity analysis of chaotic maps

Parameters	Henon map $(b_1, b_2) = (1.4, 0.3)$	Modified Henon map $(b_1, b_2) = (3.85, 0.3)$
Lyapunov Exponent	LE_1=0.42312, LE_2=-1.6271	LE_1=0.69214, LE_2=-1.8961
Lyapunov Dimension	1.26	1.365
Correlation between C_1, C_2	0.0910	0.0011
Correlation between C_3, C_4	0.1223	0.0606

logistic map show an improvement in the chaotic range of 1.6% to 56% in this interval. Hence, the modified Henon map has wide application in multiple image encryptions which has broad array of chaotic range when compared to existing 2D maps.

3.3.2 Correlation test

The correlation test is used to evaluate the distance between two chaotic sequences which are generated from the chaotic map with slightly different system parameters/initial conditions. It can be defined as

$$C = \frac{E[(X - \mu_X)(Y - \mu_Y)]}{\sigma_X \sigma_Y} \tag{3}$$

where μ_X, μ_Y and σ_X, σ_Y are the mean and standard deviation of the chaotic sequences X and Y respectively. The chaotic sequences are completely different if the correlation value is close to zero. If the correlation value is close to one, then the two sequences are close to each other [17]. C_1, C_2 and C_3, C_4 are the chaotic output sequences generated by applying a slight change to their initial condition and system parameter respectively. The correlation values of these sequences for MHM and HM are listed in Table 2. From the table, it is clear that the chaotic sequences generated from MHM have lesser absolute correlation value when compared to HM. Thus, MHM is highly sensitive to their initial conditions and system parameters. Further, correlation plot of output sequences generated from the MHM with a slight change in initial condition and system parameter is shown in Fig. 2. It can be observed from the plot that a slight change in initial conditions or system parameters of MHM yields

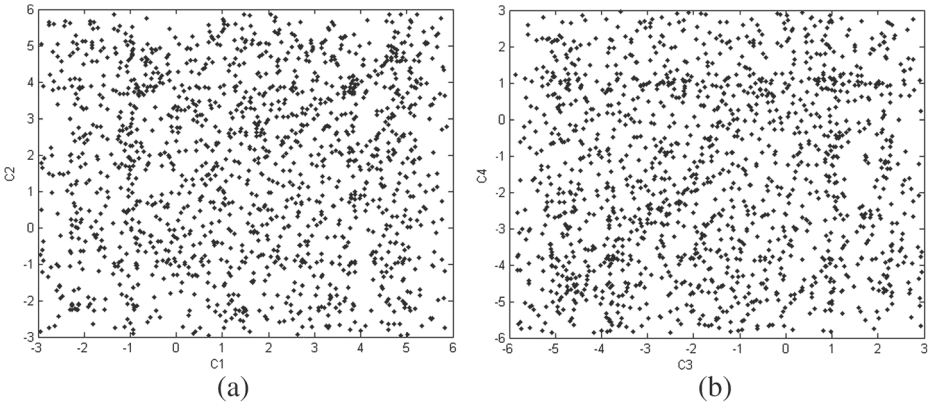

Fig. 2 Correlation plot of output sequences generated from the MHM with a slight change in **a** initial condition. **b** system parameter

dynamically scattered output sequences over the entire data range and no correlation with each other.

3.3.3 Lyapunov exponent and Lyapunov dimension

Lyapunov exponent (LE) and Lyapunov dimension (LD) are well known indicators to measure chaotic behavior of the dynamical systems quantitatively. LE measures the degree of divergence between two close trajectories. A positive Lyapunov exponent indicates that the trajectories separate exponentially with each iteration and completely different over the time. Thus, the map is said to be chaotic if one of the Lyapunov exponents is positive and magnitude of negative LE should be greater than one [1]. On the other hand, LD is one of the basic properties of the dynamical system which reflect its complexity [12]. The Lyapunov exponent and Lyapunov dimension of MHM and Henon map are listed in Table 2. From the table, it is clear that the modified Henon map is more dynamic as it has greater Lyapunov exponent when compared to HM.

3.4 Sine map

The Sine map is derived from the sine function which is defined as [6]

$$z_{n+1} = rsin\,(\pi z_n) \tag{4}$$

The SM exhibits chaotic behavior when $r \in [0.87, 1]$. The sensitive dependence to initial condition/system parameter and bifurcation diagram of the sine map is shown in Fig. 3a and b respectively. From the plot, it is clear that slight change in initial condition/system parameter results in entirely different chaotic sequence. The bifurcation diagram of sine map resembles that of logistic map although they have different mathematical expressions.

4 HCST based image encryption and decryption algorithm

In this section, the encryption algorithm based on HCST is presented. A typical chaos based image cryptosystem consists of two iterative phases namely confusion and diffusion which

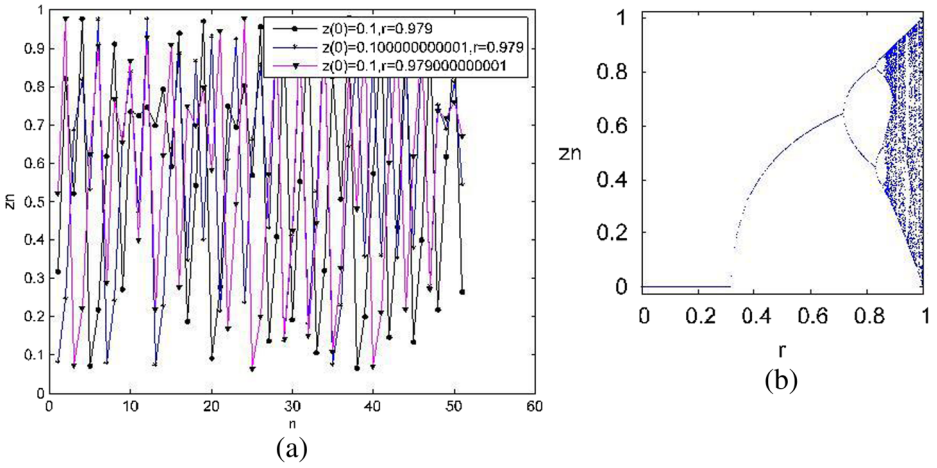

Fig. 3 Sine map's **a** Chaotic behavior. **b** Bifurcation diagram

are processed independently. Generally, 2D and 1D chaotic maps are employed to perform these primitive operations of cryptography [5]. Hence, 2D-MHM and one dimensional SM are used in this algorithm. These two chaotic maps generate the secret key for the proposed algorithm. The secret key contains the information of initial conditions and control parameters of these maps. Hence, the key set used for encryption/decryption is

$$Keyset = [x_0, y_0, b_1, b_2, z_0, r] \tag{5}$$

Usage of two chaotic maps increases the key space and security performance of the algorithm. Confusion and diffusion are applied to shuffle the pixel positions randomly and to change the value of the pixels respectively. In order to obtain satisfactory level of security, confusion and diffusion operations are repeated for several times. The complete architecture of the encryption scheme is shown in Fig. 4. It consists of mainly three algorithmic steps: generation of chaotic sequences, confusion and diffusion operations. The algorithm employs HCST to achieve column position shuffling and row position shuffling of each pixel. It includes two stages: (i) getting the column shift and row shift matrix from the positions of the sorted chaotic sequence. (ii) shifting the column and row pixels based on the column and row shift matrix respectively. The HCST is controlled by the chaotic sequences generated from 2D-MHM. The hybrid chaotic shift transformed image undergoes one more

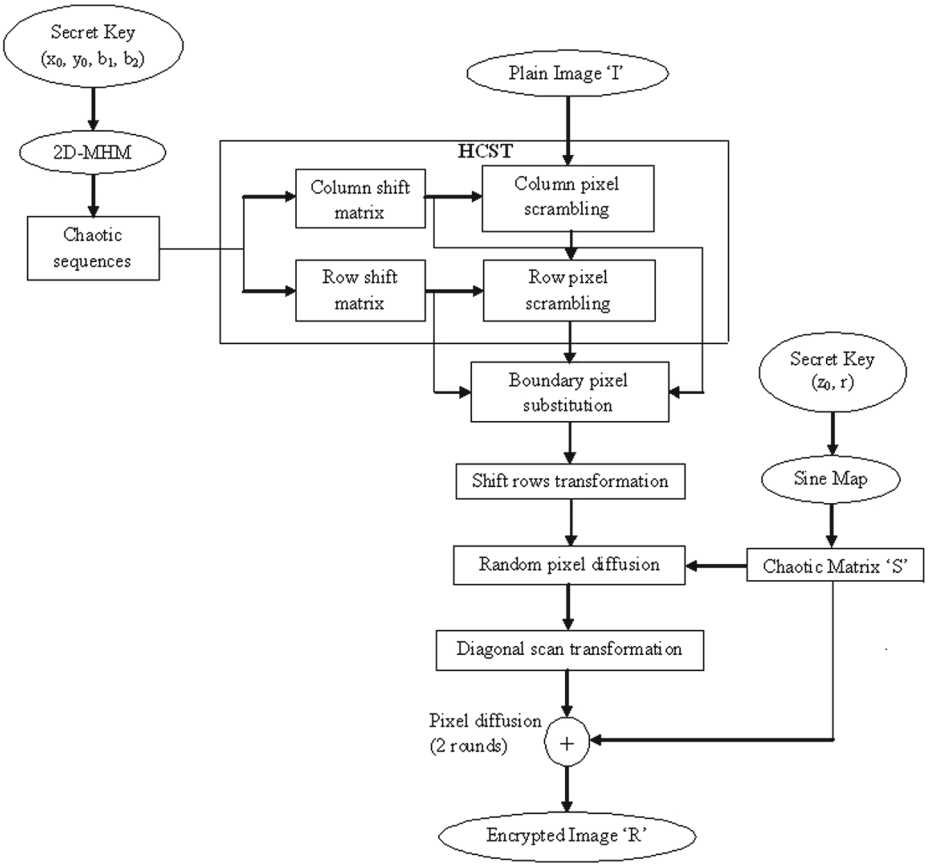

Fig. 4 HCST based encryption scheme flow diagram

level of confusion operation, called shift rows transformation. It operates one row at a time by shifting a byte to the left. The proposed algorithm employs the pixel diffusion process twice. In between two diffusion processes, the pixels are again scrambled randomly by using diagonal scanning mechanism. The scheme uses simple modulo and XOR operation to achieve diffusion process which in turn reduces the computational efforts. The diffusion operation is controlled by the chaotic matrix generated from the SM, previous encrypted pixel and current scrambled pixel. These confusion and diffusion procedures are applied in consecutive manner which is different from traditional chaos based encryption schemes.

4.1 Hybrid chaotic shift transform

In this section, hybrid chaotic shift transform is proposed to shuffle the pixel positions of the image thereby reducing the correlation between the pixels. The inherent features of the chaotic map such as random nature and sensitivity to initial conditions/system parameters make them a good candidate to perform confusion operation. In [23], chaotic shift transform (CST) is proposed to shuffle the pixel positions and row and column substitutions are employed to change the image pixel values simultaneously. This algorithm employs HCST to scramble column and row pixels based on the column and row shift matrix. These matrices are positional matrix obtained by sorting the chaotic sequences which serves as step size of shift. The column pixel positions are shifted cyclically up/down according to the column shift matrix. Similarly, row pixels are shifted cyclically left/right based on the step size of the row shift matrix. These cyclic shifts also depend on the nature of the numerical value (even=down/right, odd=up/left) of the step size of the chaotic shift matrices.The HCST changes the position of the pixel but not the value of the pixels and enables scrambling of image pixel positions in both row and column directions.

4.1.1 Definition of HCST

Firstly, generate $M + N$ chaotic values $(x_1, x_2...x_N)$, $(y_1, y_2...y_M)$ from the MHM for the plain image of size MXN with M rows and N columns using (2). Sort the chaotic sequence x_k in descending order and get the column shift matrix from the positions of the sorted sequence which is given by B=$[b_1, b_2...b_N]$. Similarly, get the row shift matrix by sorting the chaotic sequence y_k in ascending order which is given by C=$[c_1, c_2...c_M]$, where b_i and c_i represents the step size of cyclic up/down shift in column i and cyclic right/left shift in row i respectively.

Let I be an original image and T be the corresponding shuffled image. Then hybrid chaotic shift transform is defined as

$$T_1 = F(I, B) \tag{6}$$

$$T = F(T_1, C) \tag{7}$$

where T_1 represents the column shifted matrix. The hybrid CST function F is described in Algorithm 1. Therefore, HCST shuffles the column and row pixel positions within the plain image with the step size b_i and c_i respectively by using only $M + N$ chaotic values. By applying HCST, each pixel in each column and row encounters at least a column position shuffling and row position shuffling. Further, it is not possible to predict the results of HCST without the knowledge of initial conditions and system parameters of MHM.

Algorithm 1 The hybrid chaotic shift transform algorithm

Input: The original Image I and chaotic series matrix B and C
Output: The column and row shuffled image T

Generate the column and row shift matrices by sorting x_k and y_k chaotic sequence
for $i = 1$ to N **do**
    if mod(b_i, 2) = 0 **then** Cyclic shift the pixels in column i of I to down with the step size of b_i;
    elseCyclic shift the pixels in column i of I to up with the step size of b_i;
    end if
end for
Denote the column shifted image as T_1.
for $i = 1$ to M **do**
    if mod(c_i, 2) = 0 **then** Cyclic shift the pixels in row i of $T_1$to right with the step size of c_i;
    elseCyclic shift the pixels in row i of T_1 to left with the step size of c_i;
    end if
end for
Denote the row shifted image as T.

4.2 Boundary pixels substitution and shift rows transformation

In the shuffled image T, the boundary pixels of the first and last row values are replaced by the positions of the sorted chaotic sequence. This operation results in a matrix P. Further, the scheme uses shift rows transformation to complicate dependence of the statistics of ciphertext on the plaintext. The shift row transformation operates one row at a time by shifting the byte to the left. The number of shifts depends on the row number of the P which means that the row 0 doesn't encounter any shift at all and the last row is shifted by M-1 bytes.

4.3 First level of diffusion by XOR operation

The diffusion process is employed to illustrate the effect of change in one bit of the plaintext on each bit of the ciphertext thereby hiding the statistical structure of the plaintext [14]. In this scheme, different ways of diffusion process are applied at different stages. The chaotic matrix S generated from the sine map is used to change some of the pixel values. The elements of the chaotic matrix S' are converted to same representation format as that of pixel of the plain image using (8).

$$S = round((S'X10^8)modm) \tag{8}$$

where S' is the real chaotic matrix, S is the transformed chaotic matrix which is in integer form and m is 256 for gray scale image.

The pixel values are changed twice randomly by using XOR operation with the chaotic matrix using (9).

$$D(i,j) = \left\{ \begin{array}{rl} D_1(i,j) = L(i,j) \oplus S(i-1,N) & for \quad i=2 \quad to \quad M-1 \\ D_1(i,j) \oplus S(i,j+1) & and \quad j=2 \quad to \quad N-1 \end{array} \right\} \tag{9}$$

where L is the result of shift rows transformation, $\oplus$ denotes bitwise XOR operation and D is the result of diffusion operation.

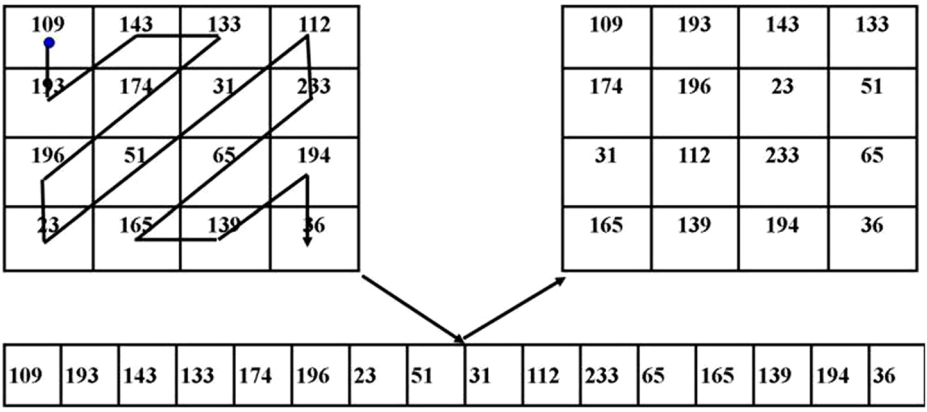

Fig. 5 Diagonal scanning mechanism

4.4 Diagonal scanning transformation

The pixel positions are randomly shuffled within the image by employing diagonal scanning mechanism. The scan starts from the left upper corner and ends in the right lower corner. Initially, the 2D image is converted into 1D array of size $D_{(1XMN)}$ by scanning the image diagonally. Then, it is converted into a two dimensional matrix O. The diagonal scanning mechanism is shown in Fig. 5. From the figure, it is clear that the pixel values are shuffled sufficiently.

4.5 Second level of diffusion by XOR operation

In this diffusion stage, the pixel values are changed by using bit XOR operation of each digit with the previous cipher digit, current scrambled pixel and chaotic matrix S generated from the sine map as defined in (10). This enhances the security of the cryptosystem to one more level. Further, it is not possible to get the current pixel value without knowing the previous pixel value and chaotic matrix. However, in the original image if a single digit gets corrupted due to noise results error in subsequent encrypted digits. Encrypted image R is obtained after applying two rounds of diffusion operation.

$$R_i = \left\{ \begin{array}{ll} O_i \oplus S_i & for \quad i = 1 \\ O_i \oplus O_{i-1} \oplus S_i & for \quad i \neq 1 \end{array} \right\} \tag{10}$$

4.6 Decryption algorithm

The decipher process is reverse that of encipher process. In order to design a secure cryptosystems, it is necessary to pay more attention to secret key. Hence, secret keys should be stored safely and transmitted to the receivers so that only authorized users can decipher the image correctly. The concrete decryption procedure is shown in Fig. 6. The decrypted images of various encrypted images are shown in Fig. 7. The figure shows that, the decrypted images are not unintelligible any longer.

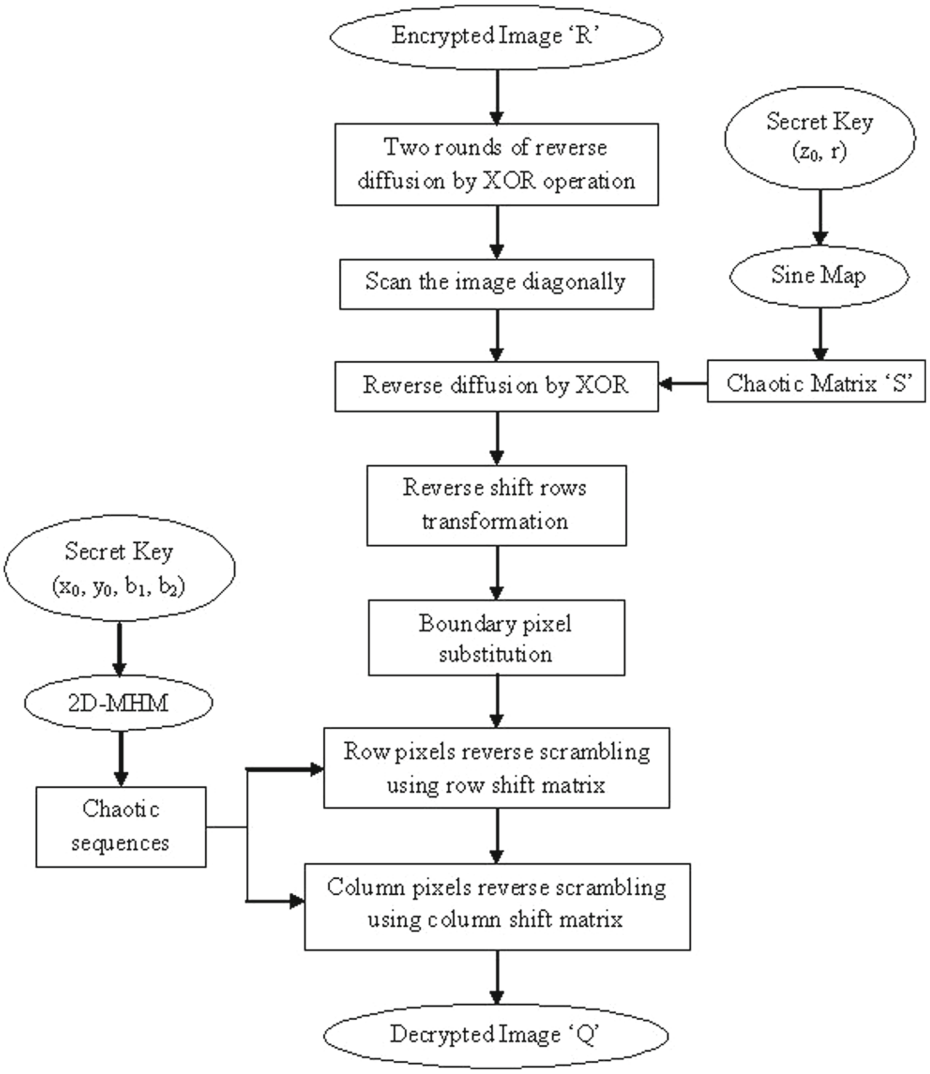

Fig. 6 Flowchart of the deciphering process

5 Security analysis

A good cryptosystem should satisfy mainly two objectives: (1) The cipher should offer resistance against all kinds of known attacks. (2) It should possess both confusion and diffusion property [32]. The confusion property corresponds to a tiny change in the key should produce entirely different ciphertext, whereas diffusion property refers to spreading the effect of slight change in the plaintext over the corresponding ciphertext. Further, a good cipher should be robust under noisy environment. Hence, in this section the performance and analysis of different types of attacks is presented with extensive simulation results and comparisons [3, 5, 9, 14, 16, 18, 23, 25, 26, 33, 40, 43, 46, 49–51]. Different

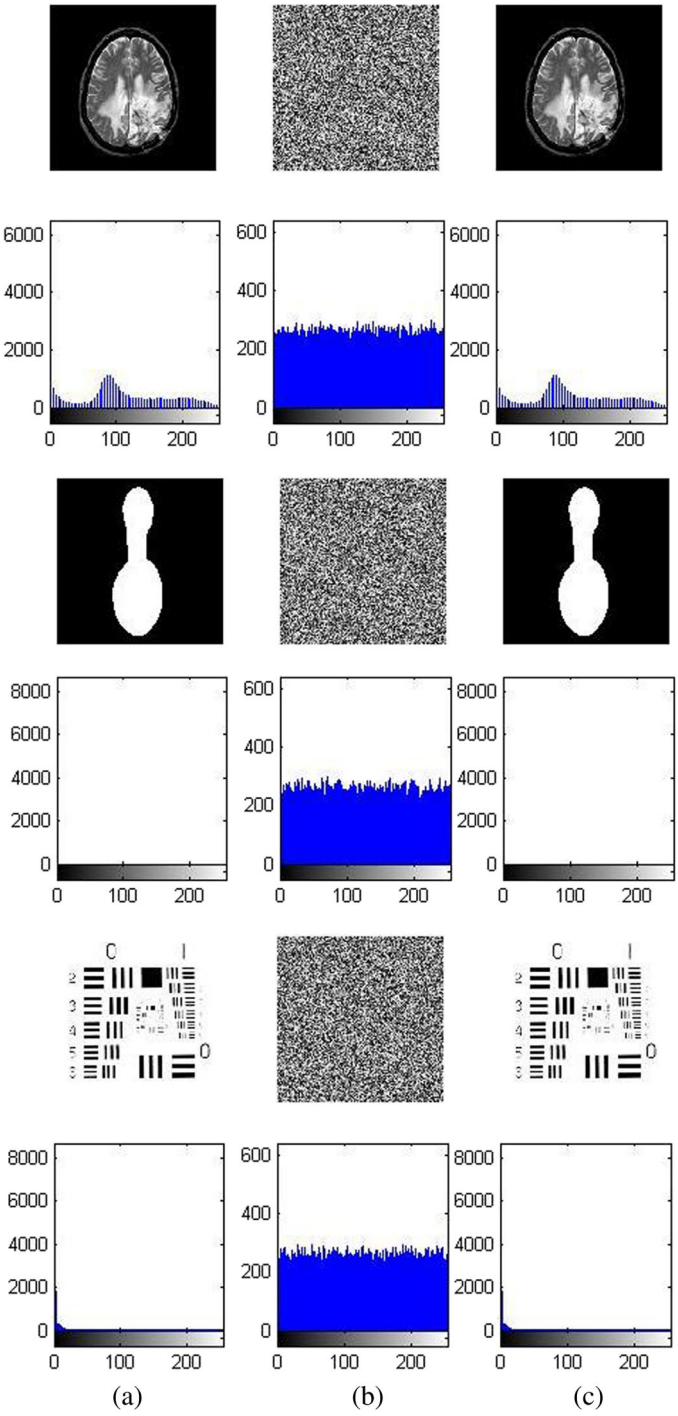

Fig. 7 Encryption and decryption results: **a** original images and its histograms. **b** encrypted images and its histograms. **c** decrypted images and its histograms

test images are taken from the USC-SIPI Miscellaneous image database for experimentation. The initial values of the key set used for encryption is x_0=0.1, y_0=0.675, b_1=5.85, b_2=0.3, z_0=0.5591, r=1. The algorithm is verified for various images of different sizes. The plain, ciphered and the corresponding decrypted images are shown in Fig. 7. From the figure, it is clear that the encrypted images are completely unrecognizable, unsystematic and not at all possible to get any information thereby achieving the confidentiality of the algorithm.

5.1 Confusion property and statistical attack analysis

It has been suggested that the algorithm can be cryptanaylzed effectively using statistical analysis [32]. Hence, the analysis has been performed to show resistance of the algorithm against statistical attacks. Some of the tests that demonstrate the confusion property include histogram analysis, correlation analysis and information entropy analysis.

5.1.1 Histogram analysis

The histogram analysis qualitatively evaluates any encryption algorithm. An image histogram shows the frequency distribution of each grayscale level which provides the statistical information of the image. Any encryption algorithm should have an ability to generate uniform and completely different histogram for any plain image [25, 46]. Figure 7 shows the histograms of several plain images and corresponding cipher images. It has been observed that statistical resemblance between the plain image and cipher image is very less as the pixels of ciphered image are distributed evenly. Hence, the algorithm resists against the statistical attacks and possesses good confusion property.

5.1.2 Correlation coefficient analysis

In this subsection, the correlations among adjacent pixels in various plain images and corresponding ciphered images in different directions have been analyzed. Because of high information redundancy in the plain image, the adjacent pixels have strong correlation with each other. However, it is expected to have weak correlation among adjacent pixels in ciphered image. The correlation distribution of the plain image and ciphered image in horizontal, vertical and diagonal directions is shown in Fig. 8. The correlation coefficients for various images in different directions are tabulated in Table 3. It has been observed that there is a high correlation among neighboring pixels in the plain image whereas low correlation in the ciphered image. This evidences the excellent confusion property of the algorithm. The comparison of correlation coefficient between plain and cipher images for the proposed scheme with other peer algorithms is shown in Fig. 9. The first 24 images are selected from Table 3 for comparison. It can be observed from the plot that the proposed scheme shows outstanding performance in almost all trials when compared to AES and RC4. Table 4 lists the correlation coefficient values of the plain image and its encrypted image for different encryption schemes for “Lena” image. From the table it is clear that, the algorithm outperforms other algorithms proposed in [9, 16, 18, 23, 26, 40, 43, 49, 50] in all the three directions and has least correlation coefficient than schemes proposed in [3, 5, 14, 25, 33, 46] in two directions. Thus, the algorithm reduces the correlation among the adjacent pixels efficiently thereby exhibiting the resistance against correlation based statistical attacks.

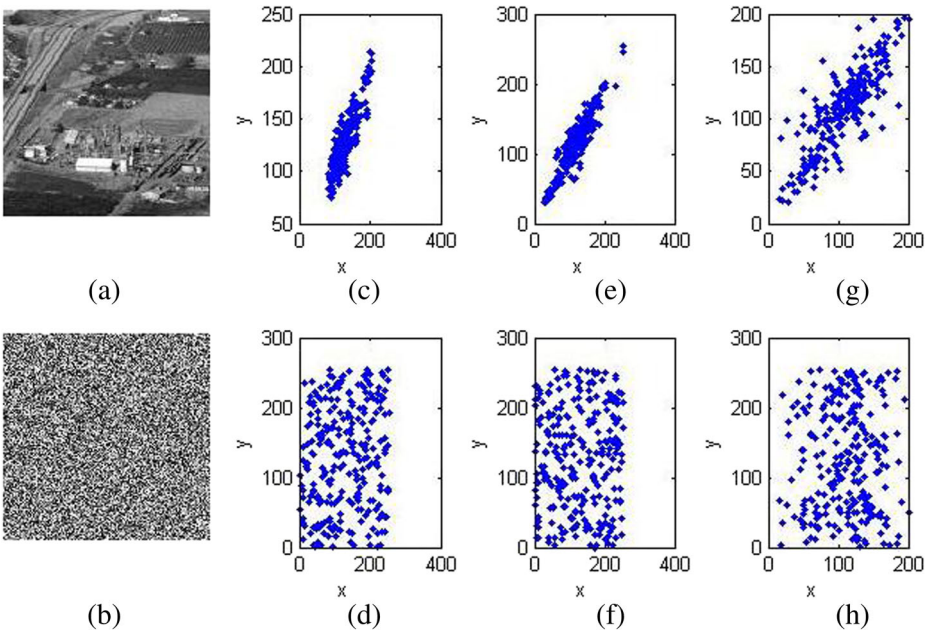

Fig. 8 Correlation of adjacent pixels before and after encryption in different directions **a** Plain image I. **b** Encrypted image R. **c** horizontal neighborhood pixels correlation of I. **d** horizontal neighborhood pixels correlation of R. **e** vertical neighborhood pixels correlation of I. **f** vertical neighborhood pixels correlation of R. **g** diagonal neighborhood pixels correlation of I. **h** diagonal neighborhood pixels correlation of R

5.1.3 Information entropy analysis

The strength of any encryption algorithm is measured quantatively in terms of information entropy which signifies the degree of randomness in the information content [43]. For the 8 bit message, suppose if there are 256 possible outcomes with equal probability then the ideal value of entropy should be equal to 8. The entropy value of the good encryption algorithm should be close to ideal one which means that leakage of information is negligible during encryption process. The information entropy of different ciphered images is given in Table 5. It can be observed from the table that the information entropy of ciphered image is much close to 8. This implies that the encryption algorithm results in random like ciphered images. Further, the comparison of this algorithm with other peer algorithms with respect to information entropy for Lena image is given in Table 4. The comparison results show that the algorithm outperforms the method proposed in [9, 14, 16, 18, 23, 26, 40, 43, 46, 49]. Thus, the algorithm offers resistance against entropy based attacks.

5.1.4 Maximum deviation (D)

The quality of encryption is measured in terms of maximum deviation which quantifies the deviation of encrypted image from the original plain image. The maximum deviation measures the encryption quality by considering a whole histogram distribution of original

Table 3 Correlation coefficient of different images

File name	Correlation coefficient					
	Horizontal		Vertical		Diagonal	
	Plain	Cipher	Plain	Cipher	Plain	Cipher
5.1.09	0.9020	0.0011	0.9390	0.0015	0.9037	−0.0056
5.1.10	0.9050	0.0094	0.8602	0.0018	0.8213	−0.0018
5.1.11	0.9571	0.00024553	0.9366	0.0032	0.8927	0.0020
5.1.12	0.9565	0.0027	0.9741	−0.0042	0.9389	0.00019336
5.1.13	0.8722	−0.0022	0.8667	0.0014	0.7562	0.0047
5.1.14	0.9466	0.0023	0.8984	−0.0027	0.8529	−0.0096
5.2.08	0.9371	0.00064542	0.8926	−0.00056350	0.8557	−0.00049560
5.2.09	0.9008	0.0027	0.8602	0.00059609	0.8031	0.0043
5.2.10	0.9404	0.0011	0.9275	−0.0011	0.8975	−0.000096446
7.1.01	0.9620	0.0020	0.9205	−0.0029	0.9074	−0.00047892
7.1.02	0.9463	0.0023	0.9459	−0.00033831	0.8962	0.00012025
7.1.03	0.9456	0.0020	0.9321	0.000044816	0.9017	0.000066546
7.1.04	0.9768	0.0002878	0.9675	−0.0013	0.9559	−0.00065317
7.1.05	0.9420	−0.0026	0.9120	−0.0022	0.8933	0.0023
7.1.06	0.9402	0.0017	0.9062	−0.0012	0.8861	−0.00018256
7.1.07	0.8862	−0.0037	0.8778	0.0021	0.8392	−0.0018
7.1.08	0.9577	0.0019	0.9292	0.0018	0.9219	0.0020
7.1.09	0.9657	−0.0021	0.9304	−0.00020231	0.9168	0.0011
7.1.10	0.9643	−0.0009117	0.9474	0.0018	0.9313	−0.00025816
boat.512	0.9381	−0.0008713	0.9713	−0.00083680	0.9222	−0.0043
elaine.512	0.9757	0.0011	0.9730	0.0049	0.9692	0.0015
gray21.512	0.9965	−0.00024549	0.9998	0.0039	0.9964	0.0028
numbers.512	0.7386	0.0033	0.7159	−0.00017056	0.6253	0.0016
ruler.512	0.4542	−0.0000069412	0.4648	−0.00040986	−0.0290	−0.00028806
Cameraman	0.9335	0.0031	0.9592	0.0078	0.9087	0.0020
Texture	0.9776	−0.000052765	0.9784	0.0054	0.9565	−0.0077
Medical	0.9761	0.00075150	0.9817	0.0029	0.9618	0.0022
Rice	0.9264	−0.0037	0.943	−0.0069	0.8978	0.0018

and encrypted image without taking care of each individual pixel value and deviation caused at every location of the original image [9, 52]. The higher value of D indicates more deviated ciphered image from the plain image. The maximum deviation of different ciphered images is tabulated in Table 6. From the obtained results, it is clear that the encrypted image is highly deviated with respect to its plain image. Hence, the quality of the algorithm is high when compared to RC5, AES and KAMKAR ciphers with CBC mode.

5.2 Diffusion property analysis

The ciphers ability of diffusing a change in one bit of plaintext over its entire cipher image is described by using diffusion property. The diffusion property is illustrated for “Elaine”

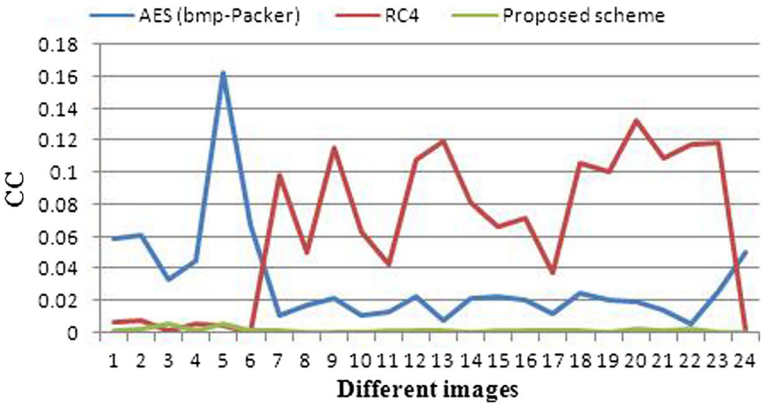

Fig. 9 Comparison of proposed algorithm with other peer algorithms with respect to correlation coefficient between original and encrypted image

Table 4 Comparison of proposed algorithm with existing algorithms for Lena image

Original image	Correlation coefficient			Entropy
	Horizontal 0.9258	Vertical 0.9593	Diagonal 0.9037	
Zhang et al. [50]	0.003206	−0.000289	0.001167	7.9993
Yuan et al. [46]	0.0019	0.0053	0.0042	7.9973
Huang et al. [18]	−0.0050	−0.0006	−0.0025	7.9967
Gururaj et al. [14]	−0.000319	0.001201	0.005271	7.9972
Chen et al. [5]	−0.00077491	0.0045	0.0061	7.999319
Liu et al. [23]	0.0030	−0.0024	−0.0034	7.9976
Machkour et al. [25]	−0.000169	0.001153	−0.000989	7.9993
Wang et al. [40]	−0.0331	0.0057	0.0169	7.9972
Zhang et al. [49]	0.0046	0.0040	0.0017	7.9978
Xu et al. [43]	−0.0230	0.0019	−0.0034	7.9974
Mandal et al. [26]	−0.0564	−0.0182	−0.0653	7.9666
Bakhache et al. [3]	0.000407	0.006686	0.006096	NA
Sheela et al. [33]	−0.0015	0.0036	0.0003054	7.9991
Faragallah et al. [9]	0.0035	0.0029	0.0025	7.926
Hu et al. [16]	−0.0077	0.0002	−0.0055	7.9975
Proposed method with HM	−0.0039	−0.0053	−0.0035	7.9991
Proposed method with MHM	−0.0020	0.00017585	0.00013470	7.9990

Table 5 Entropy values of different images

Image name	Cameraman	Peppers	Texture	Medical	Baboon	Einstein	House	Flowers
Entropy	7.9990	7.9992	7.6709	7.9991	7.9990	7.9990	7.9991	7.9991

Table 6 Comparison of maximum deviation of different images with other algorithms

Image name	Proposed method	RC5 [9]	AES [7]	KAMKAR [7]
Cameraman	64507	14817	NA	NA
Lena	42458	15694	27950.5	28670
Barbara	130713	17324	44652	44992.5

image which is shown in Fig. 10. From the figure, it is clear that a single pixel difference between I and I_1 diffuses to the entire cipher image which leads to significant difference between R and R_1.

5.2.1 Resisting differential attack analysis

One of the desirable properties of any encryption algorithm is to offer resistance against differential attack. The number of pixels change rate (NPCR) and unified average changing intensity (UACI) are used to measure ability of the algorithm to resist differential attack.

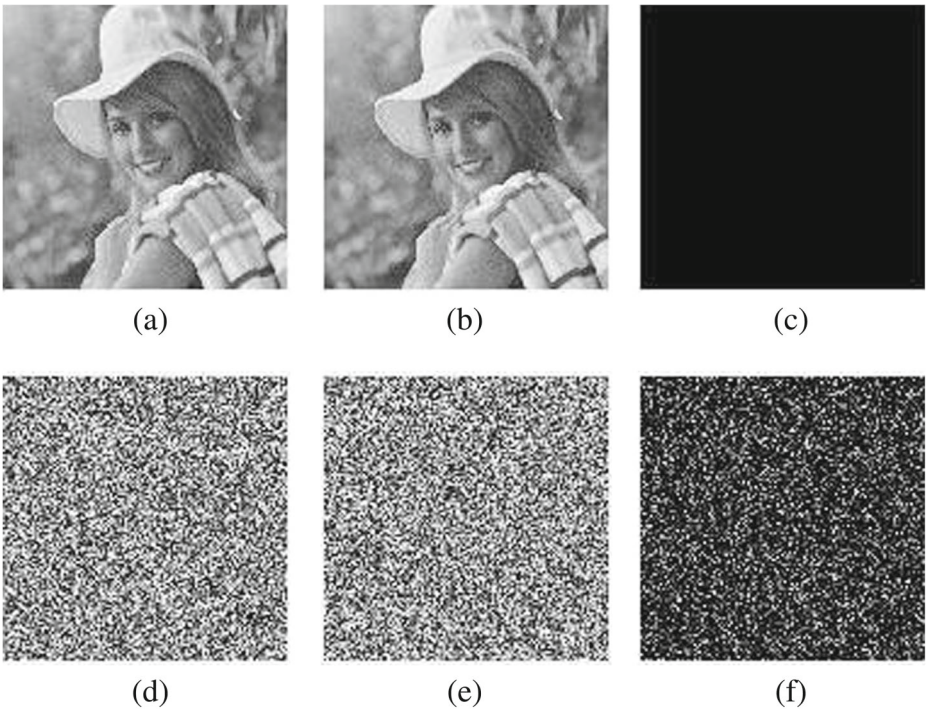

Fig. 10 Diffusion property results: **a** original image I. **b** modified image I_1 by single pixel. **c** difference image between (**a**) and (**b**). **d** ciphertext image of I. **e** ciphertext image of (**b**). **f** difference image between (**d**) and (**e**)

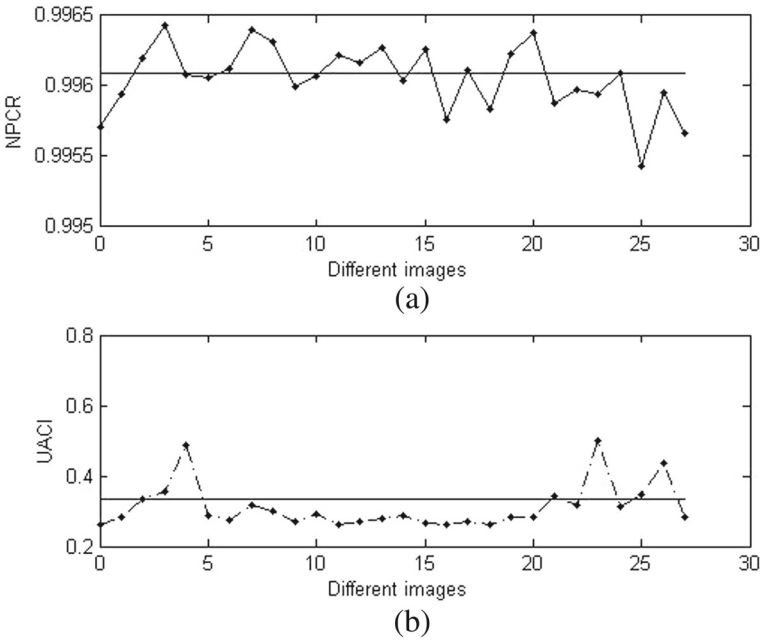

Fig. 11 **a** NPCR for the images given in Table 3. **b** UACI for the images given in Table 3

NPCR measures percentage of number of different pixels between two images and UACI measures the average change in intensity between original image and cipher image. The NPCR and UACI between plain image I and ciphered image R [3, 18, 26] are calculated using (11). The expected scores of NPCR and UACI are 99.609% and 33.464% respectively [51]. Figure 11 shows NPCR and UACI values for the images given in Table 3. It can be observed from the plot that the values are close to theoretical values. The average scores of NPCR and UACI are 99.6055% and 31.1675% respectively. Further, the NPCR and UACI values of this algorithm are compared with the existing algorithms for "Lena" image which are given in Table 7. From the table, it is clear that the proposed scheme is comparable

Table 7 Comparison of NPCR and UACI with other algorithms

Original image "Lena"	NPCR	UACI
Huang et al. [18]	99.54	28.27
Mandal et al. [26]	99.8246	28.3321
Bakhache et al. [3]	99.6277	32.5958
Faragallah et al. [9]	78.4	31.2
RC4	99.6414	28.6485
AES [Reported in Ref. [3]]	99.6185	32.9523
Proposed algorithm with HM	99.5834	28.5247
Proposed algorithm with MHM	99.5865	28.6372

Table 8 UIQ and SSIM for different images

Image name	UIQ	SSIM
Boat	0.8714	0.0103
Texture	0.5462	0.0073
Medical	0.2915	0.0012
Rice	0.8849	0.0098
Tulips	0.8409	0.0111

with the schemes proposed in [3, 9, 18, 26]. Thus, the algorithm resists against differential attacks effectively.

$$NPCR(I,R) = \frac{\sum_{i,j} G(i,j)}{MXN} X100\%$$
$$\text{where } G(i,j) = \begin{cases} 1, & \text{if} \quad I(i,j) \neq R(i,j) \\ 0, & \text{else} \end{cases}$$
$$UACI(I,R) = \frac{1}{MXN} \sum_{i,j} \frac{|I(i,j) - R(i,j)|}{255} X100\% \tag{11}$$

where M is width of the image and N is height of the image, $I(i,j)$ and $R(i,j)$ are original and encrypted image respectively.

5.3 Universal image quality index (UIQ) and structural similarity index measure (SSIM)

UIQ and SSIM are the two parameters used to measure structural similarity between two images whose value varies from -1 to 1 [37, 39]. The greater similarity between the images will be achieved when the value is closer to one. The values of UIQ and SSIM for different images are given in Table 8. It can be observed from the table that, there is no similarity between images as the values are not close to one.

5.4 Peak signal to noise ratio (PSNR) analysis

PSNR evaluates the encryption algorithm objectively by considering the original image and encrypted image as a signal and noise respectively [14]. The low value of the PSNR indicates the greater difference between the original and ciphered image. The PSNR values of different images are listed in Table 9. From the table results, it is clear that the encryption quality is good as the PSNR value of each image is very low ($< 10dB$). Further, it is very

Table 9 PSNR values of different images

Image name	PSNR (dB)
Cameraman	8.3497
Lena	9.2335
Pepper	9.0076
Baboon	9.7271
House	8.6695
Tree	8.1992

Table 10 Key space of different image encryption schemes

Image encryption schemes	Key space
Zhou et al. [51]	10^{68}
Huang et al. [18]	10^{48}
Chen et al. [5]	10^{60}
Mandal et al.[26]	$1.77X10^{77}$
Bakhache et al. [3]	$1.46X10^{48}$
Xue et al. [44]	10^{60}
Hu et al. [16]	10^{75}
AES [31]	$1.1579X10^{77}$
RC4 [31]	$7.2058X10^{16}$
Proposed algorithm	10^{84}

difficult to retrieve the original image from the encrypted image as the PSNR values are lower.

5.5 Resisting brute force attack analysis

The capability of resisting brute force attack is characterized by the size of the key space. The key space of image encryption algorithm should be larger than 2^{100} to resist against brute force attack [2, 31]. The modified Henon map employed for encryption exhibits broad chaotic regime which is highly sensitive to initial conditions and system parameters. The key set used for encryption contains six parameters $[x_0, y_0, b_1, b_2, z_0, r]$. The key space is 10^{84} if the length of each parameter and initial value is of 10^{14} decimals. Table 10 shows the comparison of the key space of this algorithm with other algorithms. From the results it can be found that the secret key space of this algorithm is much larger than cipher standards such as AES, DES and other schemes proposed in [5, 16, 18, 44, 51]. Thus, the algorithm has large key space to resist brute force attack.

5.6 Secret key sensitivity analysis

Any encryption algorithm should be highly sensitive to its secure key changes in addition to sufficient large key space in order to resist brute force attack. A good cryptosystem exhibits the high sensitivity to secret key if it satisfies following two conditions [31].

1. The cryptosystem should produce completely different encrypted image when slightly different secret keys are used to encrypt the image.
2. The cryptosystem should be unable to decrypt ciphertext even for the slight difference in the encryption and decryption keys.

The effect of key sensitivity on encryption process is verified by encrypting the images by using original key and slightly altered keys which are obtained by applying a tiny change on each subkey with the variation of 10^{-10}. Figure 12b–c shows the cipher image for different images obtained by using the original key and slightly modified keys. Although they look similar, they are completely different from each other. This is evident by observing the difference images shown in Fig. 12d. From the figure, it is clear that a slight change in the key will result in completely different ciphered image. Hence, the algorithm gratifies the sensitivity property required by the secure encryption scheme. Further, it is not

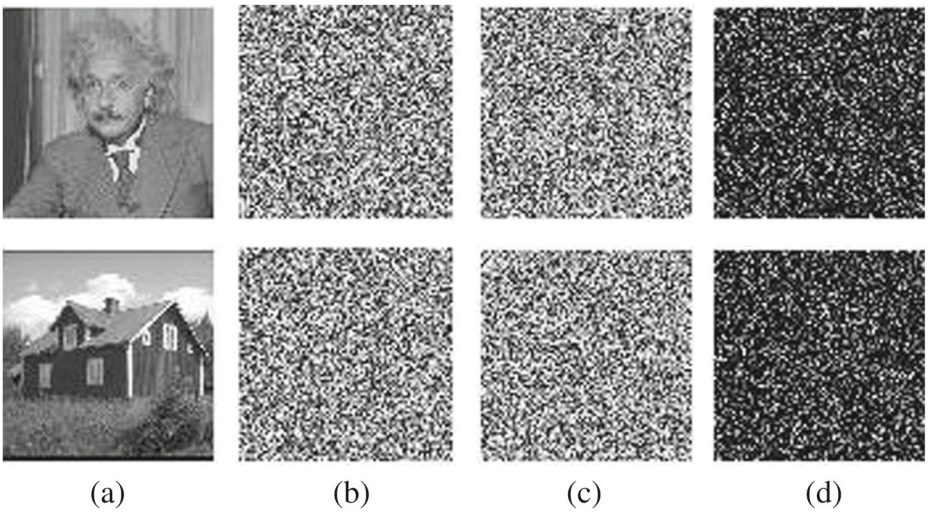

Fig. 12 Key sensitivity test for encryption process **a** original images. **b** ciphered image for the correct key. **c** ciphered images for the slightly altered keys. **d** difference image between (**b**) and (**c**)

possible to distinguish the difference between the images by visual inspection completely. Therefore, NPCR and UACI values are calculated to measure the difference between the images quantitatively which are tabulated in Table 11. From the results, it is clear that in an average 99.533% pixels are different with an average changing intensity of about 32.784%. Hence, the algorithm offers more security with high sensitivity to secret key. Furthermore, the effect of key sensitivity on correlation coefficient and PSNR is considered. Table 11 lists the PSNR and correlation coefficient values between the images encrypted using original key and slightly altered keys. Low correlation coefficient, PSNR, NPCR and UACI values indicate that the algorithm satisfies first condition of key sensitivity analysis.

The key sensitivity test is also performed on decryption process in order to verify the second condition of the key sensitivity analysis. Figure 13c shows the decrypted image using correct key and the decrypted images along with its histogram for slightly altered keys are shown in Fig. 13d. The decrypted images for slightly altered keys are unrecognizable, noise like with uniform distribution. Thus, the correct decryption is not at all possible even for the

Table 11 Key sensitivity results for encryption process for Cameraman image

Parameter changed with the variation of 10^{-10}	NPCR (%)	UACI (%)	PSNR	Correlation between image encrypted with original key and slightly altered key
x_0	99.5010	32.4094	7.9117	0.0352
y_0	99.4843	32.4525	7.9001	0.0319
b_1	99.5178	32.5540	7.8852	0.0257
b_2	99.4827	32.4930	7.8828	0.0303
z_0	99.6033	32.5083	7.7376	−0.0036
r	99.6109	32.2914	7.7743	0.0057

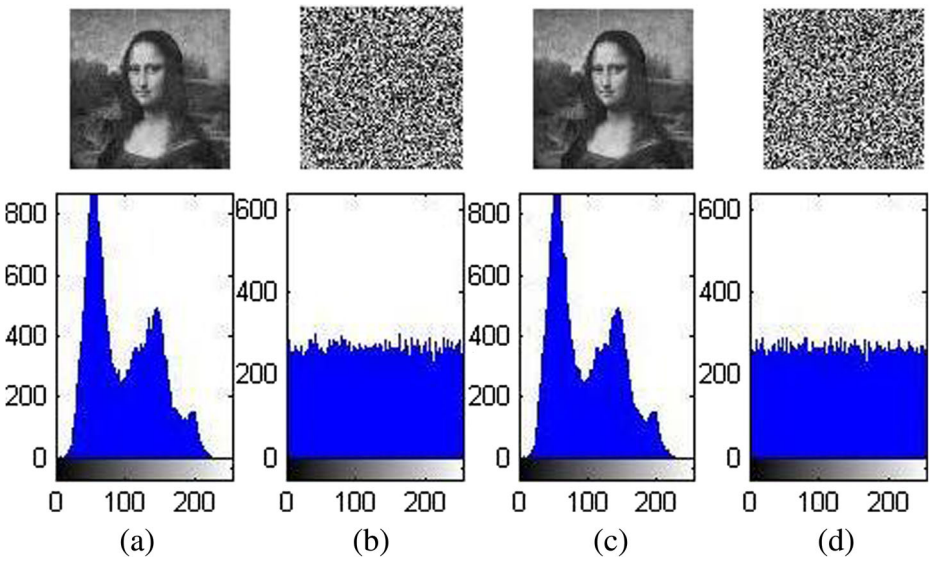

Fig. 13 Key sensitivity test for decryption process **a** original image and its histogram. **b** ciphered image and its histogram. **c** decrypted image using correct key set and its histogram. **d** decrypted image and its histogram by applying a tiny change (10^{-14}) in 'r'

slight change in the secret key thereby providing secured communication over noisy wireless channel. Further, the PSNR, NPCR and UACI values between correctly and incorrectly decrypted images are 8.8505, 98.0896% and 29.4623% respectively. The results reveal that slightly altered keys result in new decrypted image which is completely different from that

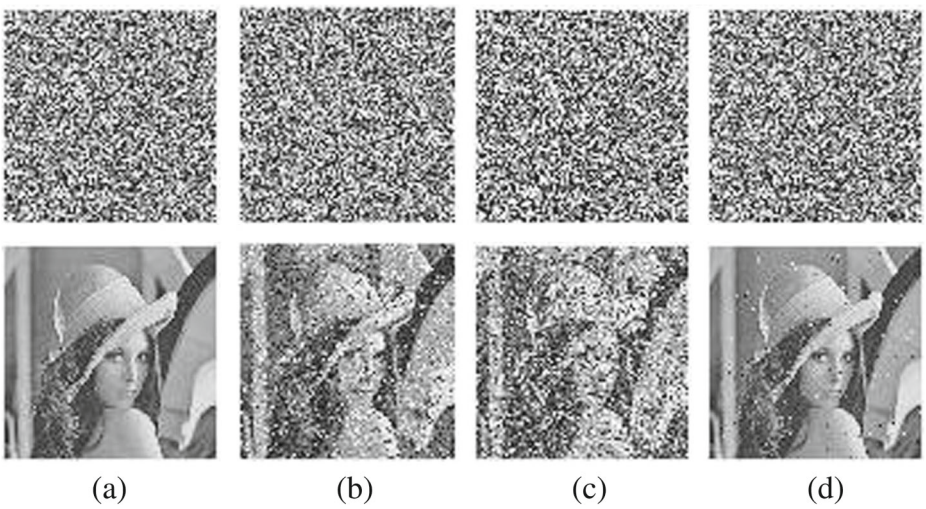

Fig. 14 Noise robustness analysis results. **a** ciphertext "R" and its corresponding decrypted image. **b** ciphertext with Gaussian noise of 0.01 variance and its decrypted image. **c** ciphertext Gaussian noise 0.05 variance and its decrypted image. **d** ciphertext with salt and pepper noise with probability of 0.02 and its decrypted image

Table 12 SSIM and PSNR between original "Lena" and decrypted image under salt and pepper noise attack

Parameter	Algorithm	Salt and pepper noise probability			
		0.005	0.05	0.1	0.5
PSNR(dB)	Proposed algorithm	31.9959	22.3720	19.3366	12.2869
	Hu et al. [16]	30.8394	21.4269	18.2828	11.3872
SSIM	Proposed algorithm	0.9365	0.5925	0.4099	0.0967

of original image. Thus, the algorithm gratifies the second condition of the key sensitivity analysis.

5.7 Noise robustness analysis

A good cryptosystem should be robust enough to resist different types of noise such as Gaussian noise, salt and pepper noise etc. to a certain extent [25, 51]. In the encryption process, the change in one pixel of the plaintext results in the change in entire ciphered image. However, in the decryption process, the change in one pixel of the ciphertext results in changing only few pixels of the recovered image. Thus, the algorithm is capable of decrypting the ciphered images in the presence of noise. Figure 14 shows the noise robustness analysis results for different types of noise with various levels. It can be observed from the figure that, it is possible to recover the original plaintext even in the presence of noise to some extent.

Further, the images are decrypted from the encrypted images which are contaminated by salt and pepper noise with probabilities of 0.005, 0.05, 0.1 and 0.5 to test the noise immunity of the proposed algorithm. PSNR and SSIM are the two metrics used to measure the visual quality between the original Lena and decrypted images that are obtained from the attacked encrypted images. The SSIM quantifies the visual difference between two images effectively than PSNR. Table 12 lists the SSIM values and comparisons with respect to PSNR between proposed method and existing algorithm [16]. The comparison results show that the proposed algorithm offers better robustness against salt and pepper noise attack when compared to other algorithm proposed in [16].

Table 13 Effective analysis of the proposed algorithm

	Proposed method with MHM		
	Permutated image	Diffused image (first level)	Diffused image (second level)
Avg correlation coefficient (Plain image = 0.9296)	0.092766	0.0037372	0.00077018
NPCR	99.3225	99.5972	99.5865
UACI	21.3445	28.6679	28.6372
SSIM	0.0225	0.0076	0.0106
UIQ	0.8815	0.8785	0.8781

5.8 Effectiveness analysis

The effectiveness of the proposed algorithm is validated at different stages. Generally, chaos based cryptosystem employs confusion stage at first to smash the strong correlation between the pixels [5]. The pixel correlation can be further degraded by using diffusion stage. This is evidenced through simulation results for the proposed algorithm at different stages as listed in Table 13. It has been observed that the average correlation coefficient and similarity between the images get reduced at each stage, owing to the interconnected structure of the cryptosystem. This algorithm uses confusion and diffusion operation at different stages which is influenced one after the other. Further, the proposed method has stable and acceptable security performance with respect to NPCR and UACI values.

5.9 Timing analysis

The time required to encrypt/decrypt the plaintext depends on various factors such as configuration of the system, programming language, operating system etc. The environment used for experimental findings is MATLAB 2009 on 1.88 GHz Intel CPU with 2.99 GB RAM in Windows XP Professional operating system. The average encryption and decryption time taken by the cryptosystem for the plain image of size 256x256 is 25.334485 s and 8.731854 s respectively. The proposed cryptosystem is slower when compared to existing algorithms [14, 23, 40, 50] However, the run time operation can be further improved with hardware as well as software optimization in order to meet the practical requirements. A suitable trade-off between the speed and the required security needs to be considered.

6 Conclusion

In this paper, a new 2D-MHM is introduced by using Henon map as seed map. The chaotic performance of the 2D-MHM is evaluated using bifurcation diagram, LEs and correlation test. The dynamical analysis and evaluation results show that, the 2D-MHM has wide chaotic regime for an extensive range of system parameters and more dynamic when compared to existing maps. Further, a novel image encryption scheme is proposed which demonstrates the performance of 2D-MHM in security applications. In contrast to the traditional chaos based cryptosystems, the proposed cryptosystem with successive confusion and diffusion procedures enhance the security level. HCST has been presented to scramble the position of image pixels which show good scrambling effect. The diffusion operation is controlled by XOR operation of previous encrypted pixel and current confused pixel along with the chaotic matrix. Extensive experimental findings show that the proposed algorithm can encrypt different types of images with a high security level and able to resist various kinds of attacks. Further, the proposed algorithm offers more security when compared to traditional encryption algorithms such as RC4, RC5 and AES with acceptable running time. Therefore, the proposed algorithm can be used in diverse applications for secure communication. Our future work is directed towards eliciting the robustness of the proposed algorithm against hypothetical differential attack. And it also includes the performance evaluation of proposed algorithm on hardware and software platforms under different network environment considerations and proposing the same for internet users.

List of abbreviations 2D-MHM, Two dimensional modified Henon map; HCST, Hybrid chaotic shift transform; XOR, Exclusive or; LFSR, Linear feedback shift register; AES, Advanced encryption standard;

DES, Data encryption standard; T-DES, Triple DES; 1D, One dimensional; HD, Higher dimension; HM, Henon map; SM, Sine map; LE, Lyapunov exponent; LD, Lyapunov dimension; NPCR, Number of pixels change rate; UACI, Unified average changing intensity; UIQ, Unified image quality index; SSIM, Structural similarity index measure; PSNR, Peak signal to noise ratio

References

1. Alligood KT, Sauer TD, Yorke JA (1997) Chaos: an introduction to dynamic systems. Textbooks in Mathematical Sciences Springer, New York
2. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcat Chaos 16(8):2129–2151
3. Bakhache B, Ghazal JM, El Assad S (2014) Improvement of the security of zigbee by a new chaotic algorithm. IEEE Syst J 8(4):1024–1033
4. Boriga R, Dsclescu AC, Diaconu AV (2014) A new one-dimensional chaotic map and its use in a novel real-time image encryption scheme. Adv in Mult Article ID 409586
5. Chen JX, Zhu ZL, Fu C, Yu H, Zhang LB (2015) A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Commun Nonlinear Sci Numer Simul 20(3):846–860
6. El-Latif AAA, Li L, Zhang T et al (2012) Digital image encryption scheme based on multiple chaotic systems. Sens Imaging 13(2):67–88
7. Elkamchouchi HM, Makar MA (2005) Measuring encryption quality for bitmap images encrypted with rijndael and kamkar block ciphers [C]. In: 2005 National conference on IEEE radio science (NRSC), pp 277–284
8. Enayatifar R, Sadaei HJ, Abdullah AH, Lee M, Isnin If (2015) A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. Opt Laser Eng 71:33–41
9. Faragallah OS (2011) Digital image encryption based on the RC5 block cipher algorithm. Sens Imaging 12(3):73–94
10. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcation Chaos 8:1259–1284
11. Galizzi GE, Cuadrado-Laborde C (2015) Joint transform correlator optical encryption system: extensions of the recorded encrypted signal and its inverse Fourier transform. Opt Commun 353:76–82
12. Gallas JA (1993) Structure of the parameter space of the Henon map. Phys Rev Lett 70(18):2714
13. Habutsu T, Nishio Y, Sasase I, Mori S (1991) A secret key cryptosystem by iterating a chaotic map. In: Davies D (ed) Advances in cryptology - EUROCRYPT'91 lecture notes in computer science, vol 547. Springer, Berlin, pp 127–140
14. Hanchinamani G, Kulkarni L (2015) An efficient image encryption scheme based on a Peter De Jong chaotic map and a RC4 stream cipher. 3D Res 6(3):1–15
15. Henon M (1976) A two-dimensional mapping with a strange attractor. In: The theory of chaotic attractors. Springer, New York, pp 94–102
16. Hu T, Liu Y, Gong LH et al (2017) Chaotic image cryptosystem using DNA deletion and DNA insertion. Signal Process 134:234–243
17. Hua Z, Zhou Y, Chen CP (2013) A new series-wound framework for generating 1D chaotic maps [C]. In: 2013 International conference on IEEE digital signal processing and signal processing education meeting (DSP/SPE), pp 118–123
18. Huang CK, Liao CW, Hsu SL, Jeng YC (2013) Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. Telecommun Syst 52(2):1–9
19. Kanafchian M, Fathi-Vajargah B (2017) A novel image encryption scheme based on clifford attractor and noisy logistic map for secure transferring images in navy. Int J e-Navi Maritime Econ 6:53–63
20. Kocarev L (2001) Chaos-based cryptography: a brief overview. IEEE Circuits Syst Mag 1(3):6–21
21. Kokkonis G, Psannis KE, Roumeliotis M, Schonfeld D (2017) Real-time wireless multisensory smart surveillance with 3D-HEVC streams for internet-of-things (IoT). J Supercomput 73(3):1044–1062
22. Li C, Liu Y, Zhang LY, Chen MZ (2013) Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation. Int J Bifurcat Chaos 23(4):1350075
23. Liu W, Sun K, Zhu C (2016) A fast image encryption algorithm based on chaotic map. Opt Lasers Eng 84:26–36
24. Liu H, Kadir A, Sun X (2017) Chaos-based fast colour image encryption scheme with true random number keys from environmental noise. IET Image Process 11(5):324–332
25. Machkour M, Saaidi A, Benmaati ML (2015) A novel image encryption algorithm based on the two-dimensional logistic map and the latin square image cipher. 3D Res 6(4):36

26. Mandal MK, Banik GD, Chattopadhyay D, Nandi D (2012) An image encryption process based on chaotic logistic map. IETE Tech Rev 29(5):395–404
27. Matthews R (1989) On the derivation of a chaotic encryption algorithm. Cryptologia 13(1):29–42
28. Mehra I, Nishchal NK (2015) Optical asymmetric image encryption using gyrator wavelet transform. Opt Commun 354:344–352
29. Memos VA, Psannis KE, Ishibashi Y, Kim BG, Gupta BB (2017) An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework. Future Gener Comput Syst
30. Pareek NK (2012) Design and analysis of a novel digital image encryption scheme. Int J Netw Secur Appl 4(2):95–108
31. Schneier B (1996) Applied cryptography, protocols, algorithms and source code in C. Wiley, New York
32. Shannon CE (1949) Communication theory of secrecy systems. Bell Labs Techn J 28(4):656–715
33. Sheela SJ, Suresh KV, Tandur D (2016) Performance evaluation of modified Henon map in image encryption. In: Ray I, Gaur M, Conti M, Sanghi D, Kamakoti V (eds) Information systems security (ICISS) lecture notes in computer science, vol 10063. Springer, pp 225–240
34. Sheela SJ, Suresh KV, Tandur D (2017) A novel audio cryptosystem using chaotic maps and DNA encoding. J Comput Netw Comm, Article ID 2721910
35. Sun F, Liu S, Li Z, Lu Z (2008) A novel image encryption scheme based on spatial chaos map. Chaos, Solitons and Fractals 38(3):631–640
36. Tong XJ, Zhang M, Wang Z, Liu Y, Ma J (2015) An image encryption scheme based on a new hyper-chaotic finance system. Optik-Int J Light Electron Opt 126(20):2445–2452
37. Wang Z, Bovik AC (2002) A universal image quality index. IEEE Signal Process Lett 9(3):81–84
38. Wang XY, Wang Q (2014) A fast image encryption algorithm based on only blocks in cipher text. Chin Phys B 23(3):030503
39. Wang Z, Bovik AC, Sheikh HR, Simoncelli EP (2004) Image quality assessment: from error visibility to structural similarity. IEEE Trans Image Process 13(4):600–612
40. Wang X, Wang Q, Zhang Y (2015) A fast image algorithm based on rows and columns switch. Nonlinear Dyn 79(2):1141–1149
41. Wu Y, Yang G, Jin H, Noonan JP (2012) Image encryption using the two-dimensional logistic chaotic map. J Electron Imaging 21(1):013014-1
42. Xie J, Yang C, Xie Q, Tian L (2009) An encryption algorithm based on transformed logistic map [C]. In: 2009 International conference on IEEE networks security wireless communications and trusted computing (NSWCTC), pp 111–114
43. Xu L, Li Z, Li J, Hua W (2016) A novel bit-level image encryption algorithm based on chaotic maps. Opt Lasers Eng 78:17–25
44. Xue X, Zhang Q, Wei X et al (2010) A digital image encryption algorithm based on DNA sequence and multi-chaotic maps. Neural Netw World 20(3):285
45. Ye G (2010) Image scrambling encryption algorithm of pixel bit based on chaos map. Pattern Recogn Lett 31(5):347–354
46. Yuan HM, Liu Y, Gong LH, Wang J (2017) A new image cryptosystem based on 2D hyper-chaotic system. Multimed Tools Appl 76(6):8087–8108
47. Zhang XP, Zhao ZM (2014) Chaos-based image encryption with total shuffling and bidirectional diffusion. Nonlinear Dyn 75(1–2):319–330
48. Zhang LY, Hu X, Liu Y, Wong KW, Gan J (2014) A chaotic image encryption scheme owning temp-value feedback. Commun Nonlinear Sci Numer Simul 19(10):3653–3659
49. Zhang Q, Liu L, Wei XP (2014) Improved algorithm for image encryption based on DNA encoding and multi-chaotic maps. AEU Int J Electron Commun 68(3):186–192
50. Zhang X, Mao Y, Zhao Z (2014) An efficient chaotic image encryption based on alternate circular S-boxes. Nonlinear Dyn 78(1):359–369
51. Zhou Y, Bao L, Chen CP (2013) Image encryption using a new parametric switching chaotic system. Signal Process 93(11):3039–3052
52. Ziedan IE, Fouad MM, Salem DH (2003) Application of data encryption standard to bitmap and JPEG images [C]. In: 2003 National conference on IEEE radio science (NRSC), pp 16–1

S. J. Sheela received her B.E. degree in telecommunication engineering from Bangalore University and M.Tech from Visvesvaraya Technological University, India. Currently she is doing Ph.D in the field of chaos based cryptography at Siddaganga Institute of Technology, Tumakuru, India. Her research interests include nonlinear dynamics and chaos, cryptography and multimedia security.

K. V. Suresh received B.E. degree in electronics and communication engineering in the year 1990 and M.Tech in industrial electronics in the year 1993 both from the University of Mysore, India. From March 1990 to september 1991, he served as a faculty in the department of electronics and communication engineering, Kalpataru Institute of Technology, Tiptur, India. Since 1993, he is working as a faculty in the department of electronics and communication engineering, Siddaganga Institute of Technology, Tumkur, India. He completed Ph.D in the department of electrical engineering, Indian Institute of Technology, Madras in 2007. His research interests include signal processing and computer vision.

Dr. Deepaknath Tandur is working as a principal scientist in the software research group of ABB's India Corporate Research Center. Prior to this, he worked at the Measurement and Research Lab of Agilent Technologies, Belgium. His research interests are in the area of industrial wireless infrastructure networks, IoT solutions, and the various radio access techniques involved in industrial communication systems. He has written over 30 peer reviewed papers in the area of communication and he also holds 5 patent applications.

Deepak has received his PhD in Electrical Engineering from University of Leuven, Belgium; and a Masters in Embedded Systems Design from University of Lugano, Switzerland.