SECURE IMAGE CRYPTOSYSTEM BASED ON HENON MAP AND ADJUSTED SINE LOGISTIC MAP

HESHAM ALHUMYANI

Department of Computer Engineering, College of Computers and Information Technology, Taif University,

Al-Hawiya 21974, KSA

E-mail: h.alhumyani@tu.edu.sa

ABSTRACT

This paper presents a superior confusion-diffusion based color image cryptosystem that is based on employing both the 2D adjusted logistic sine mapping (2D ALSM) and the 2D Henon mapping (2D HM). The encryption phase of the proposed color image encryption scheme utilizes the 2D ALSM in the confusion stage to shuffle the plain color image for m-iterations. The 2D HM is employed in the diffusion stage to diffuse the resulted 2D ALSM based shuffled color image for n-iterations. The decryption phase of the proposed color image encryption scheme follows the same manner of the encryption phase but in a reverse order. The proposed 2D HM-ALSM color image encryption scheme is subjected to a series of security tests to study and investigate its security with respect to several attacks like entropy, histogram, correlation coefficient, differential, occlusion, and noise resistance attacks. The experimental outcomes for the proposed 2D HM-ALSM color image encryption scheme illustrate the superiority and efficiency of the proposed 2D HM-LSM image encryption scheme against different attacks.

Keywords: *Henon map, Adjusted Logistic-Sine map, Confusion, Diffusion, Image encryption.*

1. INTRODUCTION

Recently, networking and communication technologies have been rapidly developed and become more user-friendly. Technologies such as social network websites and the advancement of smart phones promote and facilitate the sharing of a huge number of digital images between different virtual communities. As matter of fact, there is an urgent need to protect and secure user's private communications from any tampering or unauthorized access and preserve the original data against different attacks. Conventional encryption methods utilized for text like AES, DES, RC5, RC6...etc. [1-3] do not work properly when dealing with images. This is due to the fact that image data contain high levels of correlations and more redundancy which in turn affects the performance in terms of more power to be consumed and more time complexity for processing. To countermeasure these issues, two classes of image encryption have arisen; image data hiding and chaotic image encryption. Image data hiding is defined as the process of embedding and concealing secret data into images where human vision cannot observe and detect [4-8]. However, chaotic image encryption applies non-linear theories using confusion and diffusion according to Shannon [9] that produces random behavior. One of the main advantages of using chaotic based encryption is their sensitivity to the initial conditions and parameters. Chaotic dynamic systems are classified into two main classes: discrete and continuous systems [10-13]. In discrete chaotic systems, chaotic behavior can be obtained in spatial domain by utilizing different chaotic functions applied in an iterative manner. However, continuous systems are employed using differential equations. The chaotic map is defined to be a discrete function which is very sensitive to initial conditions. Chaotic maps can be classified according to its dimension as: a one dimension (1D) like Logistic map, Tent map, and Bernoulli map; a two dimensional (2D) like Baker map, Arnold cat map, Standard map, and Henon map); and a three dimensional (3D) like Logistic map, Tent map, and Bernoulli map [14-17]. Moreover, chaotic based encryption can be applied in both time and frequency domains. Time domain based-encryption schemes employ encryption directly on the image pixel values. Also, selective encryption can be utilized in time domain for achieving efficient time complexity to meet real time applications [18]. On the other hand, image encryption may be employed using different frequency transforms [19-21]. In frequency transform based-encryption, image pixel values are transformed from time domain into frequency domain using different types of transforms like - Fractional Fourier Transform Domain (FrFT) [19], Discrete Cosine Transform (DCT) [20], and Discrete Wavelet Transform (DWT) [21]. This is done to overcome the issue of statistical characteristics that arises when applying spatial domain-based encryption as well as transform correlated information into different domains which result in additional random behavior and more security. Therefore, chaotic based encryption has been widely used recently in image cryptosystems [22-26].

In [27], a double chaotic image cryptosystem based on tent and logistics maps has been proposed. First, they applied the tent chaotic mapping into the RGB components of the original image. Second, for dual cryptography, they used an additional random image and applied the logistic mapping into its RGB components. Finally, XORing operation is performed between the resulted two images to produce the final cipherimage. In [28], a hybrid cryptosystem based on 1D chaotic map has been proposed. This 1D chaotic map produces a uniform distributed Lyapunov exponent (LE) and ensures preserving the phase space of the original map. They used plainimage pixel values for encryption where the first half of the image pixel values are used to encrypt the second half and vice-versa. In [29], a lightweight digital image cryptosystem that uses chaotic system for wireless network applications has been presented. First, the DCT is utilized to transform image pixels to the frequency domain for the purpose of speeding up the encryption process and remove the statistical similarity between pixels. Second, a 2D Logistics map is used for random confusion of the image pixels along with key generating. Third, for further security, a 2D Henon map is used for diffusing image pixels. Finally, the 2D Logistic map is used again for image substitution.

In [30], an image cryptosystem called 1D sine powered chaotic system is presented. This system depicts the same characteristics of sine map but with two control parameters which results in more chaotic behavior with complex predictability. A secret key is used as an input for the proposed map as an initial value to produce four chaotic-based sequences. The generated sequences are employed for confusion-diffusion at row and column levels. In [31], an optimized 5D image encryption scheme is proposed to solve the hyper-parameter tuning issue for generating secret keys. First, the 5D chaotic map is built using 4D chaotic map with five parameters as the initial state. Second, non-dominated sorting genetic algorithm utilizes a heuristic local search for initial parameters tuning of the 5D chaotic map. Third, the dual-tree complex wavelet transform (DTCWT) is exploited to breakdown the plainimage into several sub-bands. Then, the generated secret key resulted by the optimized 5D map is diffused with the obtained sub-bands. To get the cipherimage, the inverse DTCWT is performed. Finally, since the proposed technique is inefficient in terms of time complexity with large images, parallelism implementation is applied to speed up the execution time of the system.

In [32], a cross chaotic image encryption system based on 2D sine-cosine chaotic map is presented. The secret key is formulated through combining all initial and control parameters together. Then, using 2D sine-cosine chaotic map, two pseudorandom sequences are produced as a function of the obtained secret keys to perform confusion and diffusion respectively on the plainimage. The authors of [33], proposed a lightweight image cryptosystem suitable for real-time applications based on Bulban chaotic map. To increase the sensitivity of the secret key, the mean of all initial parameter values are added to each initial value independently and divided by 2. Also, confusion and diffusion operations are applied on row and column level for an efficient processing performance. In the confusion phase, two sequences are generated using Bülban map to perform circular shift right operation according to the corresponded value of the sequence where one sequence is to identify the number of shifts for rows and the other sequence is assigned to deal with columns. In the diffusion phase, two random rows are generated and placed at the top and the bottom of the shuffled matrix. Finally, four sequences are generated using Bülban map to perform a bitwise-XORing operation and then produce the final cipherimage.

Henon chaotic map is introduced by [34] as simplification model of Lorenz model [35], which represents 2D dynamic system with quadratic non-linear characteristics and has been practically utilized recently in the literature [36-38]. Another class of hybrid chaotic mapping called Logistic Adjusted Sine Map is proposed by [39] to utilize characteristics of both sine map and logistic map to provide more chaotic random behavior as well as additional security. In this paper, we present a hybrid confusion-diffusion image cryptosystem based on using the 2D Henon mapping (2D HM) and the 2D adjusted logistic sine mapping (2D ALSM). We aim to apply both encryption/decryption procedures in

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

order to investigate the performance of the proposed 2D HM-ALSM image encryption scheme with respect to different security metrics like statistical, sensitivity and differential tests.

The paper rest is sectioned as follows: Section 2 presents the employed tools in the proposed encryption scheme which involve the 2D HM and the 2D ALSM. Section 3 shows the encryption/decryption procedures of the proposed 2D HM-ALSM image encryption scheme. Section 4 explores and discusses the experimental results of the proposed 2D HM-ALSM image encryption scheme. Finally, Section 5 presents the conclusions of the paper.

2. PRELIMINARIES

In this section, we present and overview the employed tools in the proposed 2D HM-ALSM image encryption scheme. These tools include both the 2D ALSM and the 2D HM.

2.1 The 2D ALSM

The 2D ALSM is a hybrid nonlinear dynamic chaotic mapping approach that is composed of both logistic map [40] and sine map [41]. This hybrid 2D ALSM can overcome the drawbacks of using either logistic map or sine map independently due to their simple behavior, and small key space. Therefore, coupling both the logistic and the Sine maps result in a complex chaotic behavior. In this hybrid technique, the logistic map is employed first for confusion/diffusion and then the output is set to be the input for the sine map for adjustment. Then the plane is extended from one dimension into two dimensions. The mathematical formula of the 2D ALSM can be defined as [39]:

$$\begin{cases} A_{j+1} = \sin(\pi(4\lambda A_j(1-A_j) + (1-\lambda)\sin(\pi B_j))) \\ B_{j+1} = \sin(\pi(4\lambda A_j(1-B_j) + (1-\lambda)\sin(\pi A_{j+1}))) \end{cases} \quad (1)$$

where $\lambda \in [0,1]$ represents the control parameter.

2.2 The 2D HM

The 2D HM is one form of 2D dynamic chaotic system that exhibits a scrambling-based confusion behavior. It works through changing the image pixels positions. The 2D HM is mathematically defined as [42]:

$$\begin{cases} A_{k+1} = 1 - \alpha A_k^2 + B_k \\ B_{k+1} = \beta A_k \end{cases} \quad (2)$$

where α and β are the control parameters, A and B represent iteration values, and k manifest the iterations number

3. THE PROPOSED HM-ALSM IMAGE CRYPTOSYSTEM

In this section, the enciphering and the deciphering processes of the proposed 2D HM-ALSM are presented. As mentioned in section 2, both 2D HM and ALSM have been used to build the proposed HM-ALSM image cryptosystem.

3.1 Encryption Procedure

The enciphering algorithm of the proposed 2D HM-ALSM is depicted in Fig. 1. The procedure of the proposed cryptosystem is outlined as follows:

1. Read an input plainimage.
2. Split the plainimage into its RGB components.
3. Each of RGB color channels of the plainimage is taken respectively according to step 2.
4. Confusion operation is applied using the 2D ALSM on the plainimage for n-rounds.
5. The output scrambled image is used in diffusion operation using the 2D HM for m-rounds.
6. Repeat step 4 and 5 for each of RGB channels.
7. Finally, the cipherimage is produced by merging the RGB obtained cipher image channels and transmitted by communication channels.

3.2 Decryption Procedure

The deciphering procedure includes inverse operations of the ciphering algorithm. The procedure of the proposed 2D HM-ALSM image cryptosystem can be outlined as follows:

1. Receive the RGB color cipherimage.
2. Split the RGB color cipherimage into its RGB components.
3. Each of RGB color channel of the cipherimage is taken respectively according to step 2.
4. The diffusion operation is applied using the inverse of 2D HM for m-rounds.
5. The output of the inverse diffusion operation is subjected to a confusion using the inverse of 2D ALSM for n-rounds.
6. Repeat step 4 and 5 for each of the RGB color channels.
7. Finally, the plainimage is reconstructed by merging the RGB components.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

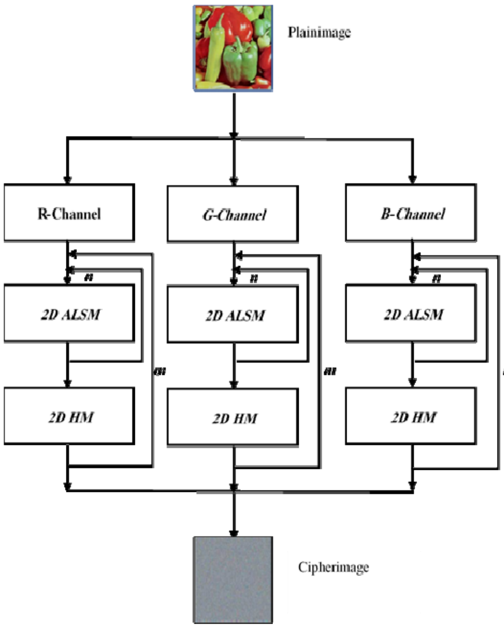


Fig. 1. Block diagram of the proposed 2D HM-ALSM image encryption scheme.

4. EXPERIMENTAL TESTS AND DISCUSSIONS

This section is dedicated to examine and test the security the proposed 2D HM-ALSM image encryption scheme. This is done through conducting a set of security tests. In addition, the proposed 2D HM-ALSM image encryption scheme is compared to both 2D HM and 2D ALSM in terms of several security measurements including the most encryption metrics statistical, entropy and differential examination, visual notification, and noise tests. The test experiments are employed using three 512×512 color images as plainimages. These color plainimages include Lena, Peppers, and Baboon as depicted in Fig. 2.

a) Lena b) Peppers c) Baboon

Fig. 2. The utilized Test color images.

4.1 Visual Notification

The visually notified outcomes of encrypted color Lena, Peppers, and Baboon with the proposed 2D HM-ALSM image encryption scheme, 2D HM, and 2D ALSM image cryptosystems are shown in Fig. 3, Fig. 4, and Fig. 5 respectively. It is obvious that the resulted cipherimages are totally distinct from their respected plainimages. In addition, the visually notified encrypted color Lena, Peppers, and Baboon ensure the efficiency of the proposed 2D HM-ALSM image encryption scheme in concealing all the details of the corresponding original color images.

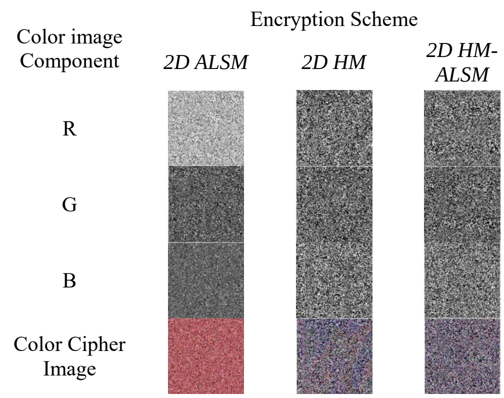


Fig. 3. The visual notified encryption outcomes using the proposed 2D HM-ALSM image encryption scheme for color Lena image.

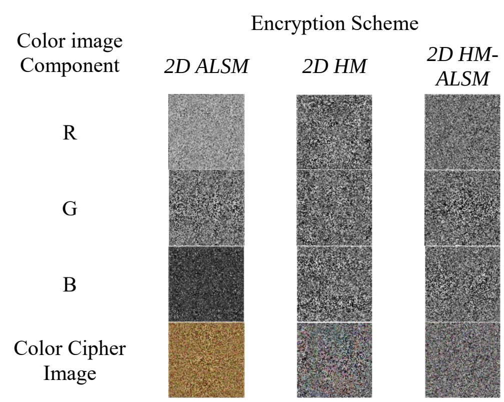


Fig. 4. The visual notified encryption outcomes using the proposed 2D HM-ALSM image encryption scheme for color Peppers image.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

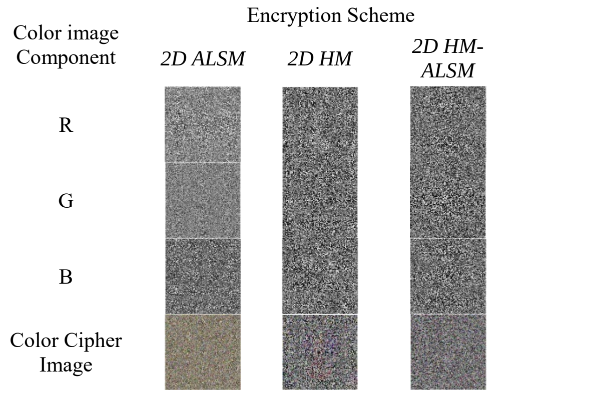


Fig. 5. The visual notified encryption outcomes using the proposed 2D HM-ALSM image encryption scheme for color Baboon image.

4.2 Histogram Testing

To achieve an efficient cipherimage, the cipherimage histogram must be uniformly distributed and completely different from its corresponding plainimage. The histograms of the tested color Lena, Peppers, and Baboon cipherimages are illustrated in Figs. 6-8. The histogram outcomes for the 2D ALSM encryption scheme indicate that the histogram results for both plainimages and their respected cipherimages are identical. This is due to the fact that the 2D ALSM is just perform scrambling and so does not change the histogram. However, the histogram outcomes of the proposed 2D HM-ALSM and 2D HM encryption schemes indicate that the histogram results for both plainimages and their respected cipherimages are completely different.

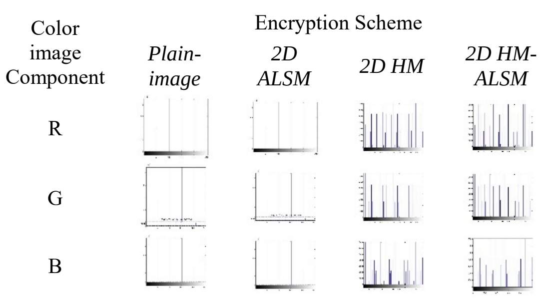


Fig. 6. Histogram outcomes of RGB plain/cipher images using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for color Lena image.

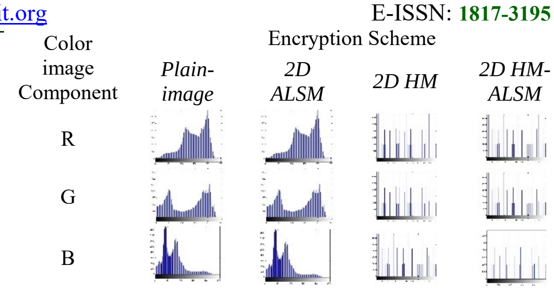


Fig. 7. Histogram outcomes of RGB plain/cipher images using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for color Peppers image.

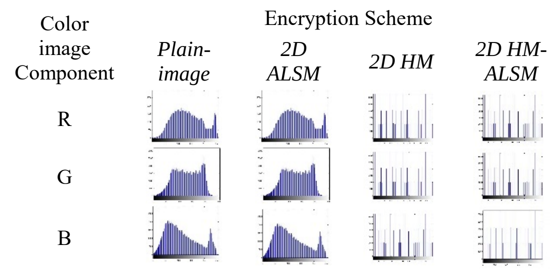


Fig. 8. Histogram outcomes of RGB plain/cipher images using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for color Baboon image.

4.3 Information Entropy

The amount of information must not be affected by the encryption process. So, we utilize the information entropy metric to measure the amount of information in the encrypted image. The entropy metric is measured in bits and its optimal value is 8. The entropy metric can be mathematically expressed as [20]:

$$Ent(x) = \sum_{i=0}^{2^N-1} P(x_i)\log_2\frac{1}{P(x_i)} \tag{3}$$

where $Ent(x)$ defines the entropy value in bits. $P(x)$ is the probability of occurrence of X_i. Table 1 lists the entropy values for both RGB plainimages and their corresponding cipherimages using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for color Lena, Peppers, and Baboon images. The entropy outcomes shown in Table 1 ensure and confirm the

Table 1. Entropy outcomes of RGB plain/cipher images using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for color Lena, Peppers, and Baboon images.

Image	Encryption Scheme								
	2D ALSM			2D HM			2D HM-ALSM		
	R	G	B	R	G	B	R	G	B
Lena	7.3248	7.4908	6.9356	5.4382	5.1746	5.5317	7.8934	7.8091	7.8914
Peppers	7.1950	7.8031	7.1118	5.6804	5.6322	5.6360	7.8699	7.8452	7.8462
Baboon	7.5166	7.2977	7.6246	5.6881	5.6788	5.6880	7.8835	7.8671	7.8739

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

efficiency of the proposed 2D HM-ALSM encryption scheme whose entropy values are near to its optimal value of 8.

4.4 Differential Analysis

The differential analysis is employed using both number of pixel change rate (NPCR) and unified average changing intensity (UACI) metrics to estimate the impact of changing just only one pixel in two identical plainimages on their corresponding encrypted images.
The NPCR metric can be expressed as [43]:

$$NPCR_{R,G,B}(EI^1, EI^2) = \frac{\sum_{ij} SIM_{R,G,B}(A_i, B_j)}{N} \times 100\% \tag{4}$$

where N is total image pixels number and $SIM_{R,G,B}(A_i, B_j)$ is measured using Eq. 5 as:

$$SIM_{R,G,B}(EI^1, EI^2) = \begin{cases} 0, & EI^1_{R,G,B}(A_i, B_j) = EI^2_{R,G,B}(A_i, B_j) \\ 1, & EI^1_{R,G,B}(A_i, B_j) \neq EI^2_{R,G,B}(A_i, B_j) \end{cases} \tag{5}$$

where $EI^1_{R,G,B}(A_i, B_j)$ and $EI^2_{R,G,B}(A_i, B_j)$ are the RGB components of the two color encrypted images EI^1, EI^2.

The $UACI_{R,G,B}$ metric can be expressed as [43]:

$$UACI_{R,G,B}(EI^1, EI^2) = \frac{1}{N}\left[\sum_{ij} \frac{\left|EI^1_{R,G,B}(A_i, B_j) - EI^2_{R,G,B}(A_i, B_j)\right|}{255}\right] \times 100\% \tag{6}$$

Table 2 lists the NPCR and UACI outcomes using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for RGB color Lena, Peppers, and Baboon images. The NPCR and UACI outcomes reflect the high sensibility of the proposed 2D HM-ALSM encryption scheme regarding tiny modifications such as one-pixel change.

4.5 Ciphering Quality Assessment

One of the major image cryptosystem assessment tools is to investigate the quality of encryption in terms of different metrics like correlation coefficient (r_{xy}), histogram deviation (D_H), and irregular deviation (D_I). Therefore, correlation coefficient, histogram deviation, and irregular deviation tests are applied to evaluate the proposed 2D HM-ALSM encryption schemes for RGB color Lena, Peppers, and Baboon images. With respect to correlation coefficients, an efficient and secure encryption scheme must obtain a near zero correlation values. Regarding histogram deviation, an efficient and secure encryption scheme must obtain high values. With respect to irregular deviation, it must be low for an efficient image cryptosystem.

The mathematical formulations of r_{xy}, D_H, and D_I are shown as follows [44]:

$$r_{xy} = \frac{E\{(EI - E(EI)) \cdot (PI - E(PI))\}}{\sqrt{E\{(EI - E(EI))^2\}}\sqrt{E\{(PI - E(PI))^2\}}} \tag{7}$$

$$D_H = \frac{\left(\sum_{i=0}^{255} dif(i)\right)}{M \times N} \tag{8}$$

$$D_I = \frac{\left|\sum_{i=0}^{255} \left|hist(i) - AVG\right|\right|}{M \times N} \tag{9}$$

where *EI*, and *PI* are the encrypted image and plainimage. The *dif(i)* represents the absolute deviation between the plainimage and the encrypted images at intensity *i*. The *hist(i)* is the encrypted image histogram at intensity *i*. *AVG* is the histogram distribution of an ideal encrypted. *M, N* are the dimension of both the plainimage and the encrypted images. The obtained encryption quality results of the 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for RGB color Lena, Peppers, and Baboon images are presented in Table 3. The achieved results of the proposed 2D HM-ALSM encryption scheme validate the superiority of the proposed 2D HM-ALSM encryption scheme compared to both 2D ALSM and 2D HM.

4.6 Noise Immunity Analysis

The noise immunity analysis is employed to examine and investigate the resistance of the proposed 2D HM-ALSM image encryption scheme against different types of noise. The different types of used noises involve the additive white Gaussian noise (AWGN), Salt and peppers noise, and speckle noise. The noise immunity test is employed with the following scenario. The tested plainimage is firstly encrypted using the proposed 2D HM-ALSM image ciphering technique and the noise is added to the cipherimage. After that, the noisy cipherimage is decrypted, and the decrypted image is observed visually and mathematically analyzed with different measures like the PSNR, SSIM, and FSIM.

Journal of Theoretical and Applied Information Technology
31st August 2020. Vol.98. No 16

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2. The NPCR and UACI outcomes using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for RGB color Lena, Peppers, and Baboon images.

Image		Encryption Scheme								
		2D ALSM			2D HM			2D HM-ALSM		
		R	G	B	R	G	B	R	G	B
Lena	NPCR	100	99.9146	100	100	97.7859	100	100	100	100
	UACI	3.04×10^{-4}	1.91×10^{-4}	7.57×10^{-5}	-6.81×10^{-7}	-7.63×10^{-8}	-1.76×10^{-7}	-1.18×10^{-6}	-4.83×10^{-7}	-5.13×10^{-7}
Peppers	NPCR	100	99.9397	99.9710	99.6342	99.25	99.38	100	100	100
	UACI	1.74×10^{-4}	9.91×10^{-5}	3.49×10^{-5}	-7.39×10^{-7}	-6.57×10^{-7}	2.64×10^{-7}	-1.14×10^{-6}	-8.08×10^{-7}	-9.65×10^{-7}
Baboon	NPCR	100	100	100	99.6223	99.65	99.61	100	100	100
	UACI	1.23×10^{-4}	2.44×10^{-4}	2.36×10^{-4}	1.15×10^{-6}	1.14×10^{-6}	1.16×10^{-6}	-7.98×10^{-9}	-1.46×10^{-8}	7.27×10^{-7}

The PSNR is mathematically expressed as [20]:

$$PSNR(I,D) = 10\log_{10}\frac{(255)^2}{\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[PI(x_i,y_i) - DI(x_i,y_i)]^2} \quad (10)$$

where $PI(x_i,y_i)$ and $DI(x_i,y_i)$ are the original color image and the resulted deciphered image.

The structural similarity (SSIM) metric is employed to estimate the percentage of similarity among the original color image and the resulted deciphered image to evaluate efficiency of the proposed 2D HM-ALSM image encryption scheme against different types of noise. The SSIM values are expressed in the interval range from 0 to 1, such that 1 indicates two fully similar images. The SSIM can be defines as [45]:

$$SSIM_{R/G/B}(x,y|s) = \frac{(2\bar{z}_x\bar{z}_y + A_1)(2\sigma_{z_x z_y} + A_2)}{(\bar{z}_x^2 + \bar{z}_y^2 + A_1)(\sigma_{z_x}^2 + \sigma_{z_y}^2 + A_2)} \quad (11)$$

where $\bar{z}_x$, $\bar{z}_y$ represent the average value of the regions z_x and z_y. A_1, A_2 define small fixed values. $\sigma_{z_x z_y}$ defines the covariance among the two regions and $\sigma_{z_x}^2$ defines z_x variance.

The feature similarity index metric (FSIM) metric is employed to estimate the percentage of local similarity among the original color image and the resulted deciphered image to evaluate efficiency of the proposed 2D HM-ALSM image encryption scheme against different types of noise. The FSIM values are expressed in the interval range from 0 to 1, such that 1 indicates two fully similar images. The FSIM can be defines as [45]:

$$FSIM_{R/G/B} = \frac{\sum_{x\in\eta} T_L(x) \cdot PR(x)}{\sum_{x\in\eta} PR(x)} \quad (12)$$

where $T_L(x)$ represents the estimated similarity among the original color image and the resulted deciphered image, η defines the spatial domain of the image, and the $PR(x)$ represents the estimated value of the phase congruency.

The results of the noise resistance evaluation for decrypted color Lena, Peppers, and Baboon images with AWGN, Salt and Peppers noise, and speckle noise at different variances ranged from 0.05 to 0.20 with step of 0.05 are given in Table 4 and Figs. 9-11. The noise immunity results as shown in Table 4 and Figs. 9-11 confirmed the efficiency and the ability of the proposed 2D HM-ALSM image cryptosystem in withstanding the AWGN using variable variances.

Regarding SSIM and FSIM, it is required to achieve high values of SSIM and FSIM to confirm efficient noise resistance. The SSIM and FSIM among the original color image and the resulted deciphered image are estimated to evaluate efficiency of the proposed 2D HM-ALSM image encryption scheme against different types of noise. The estimated SSIM and FSIM values of the proposed 2D HM-ALSM image encryption scheme against different types of noise are given in in Tables 5-6.

For different types of noises, it is observed that the obtained SSIM and FSIM values decreased as the variance increased. However, the obtained SSIM and FSIM values are adequate and reasonable with distinct noise variances. Thence, the SSIM and

Table 3. The encryption quality results of RGB plain/cipher images using 2D ALSM, 2D HM and the proposed 2D HM-ALSM encryption schemes for color Lena, Peppers, and Baboon images.

Image	Metrics	Encryption Scheme								
		2D ALSM			2D HM			2D HM-ALSM		
		R	G	B	R	G	B	R	G	B
Lena	r_{xy}	0.0021	-4.3×10^{-4}	0.0010	- 0.0024	- 0.0071	0.0038	0.0042	0.0034	0.0027
	D_H	1.3101	1.4412	1.5000	1.9026	1.7278	1.9518	1.8961	1.9029	1.9628
	D_I	0.7325	0.6881	0.9985	1.9844	1.9844	1.9844	1.9844	1.9844	1.9844
Peppers	r_{xy}	-2.83×10^{-4}	0.0016	0.0041	- 0.0483	0.0141	0.0323	- 0.0025	- 0.0040	- 0.0035
	D_H	1.5	1.4587	1.4656	1.4814	1.4190	1.4691	0.7085	0.6709	0.7540
	D_I	0.9080	0.3457	0.9466	1.9844	1.9844	1.9844	1.9844	1.9844	1.9844
Baboon	r_{xy}	-9.51×10^{-4}	0.0017	8.58×10^{-4}	0.0236	- 0.0127	0.0291	0.0018	- 0.0029	- 0.0026
	D_H	1.4997	1.4999	1.4997	1.4627	1.4813	1.4562	0.3294	0.4331	0.3657
	D_I	0.6737	0.8191	0.5930	1.9844	1.9844	1.9844	1.9844	1.9844	1.9844

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

FSIM results assure the superiority of the 2D HM-ALSM image cryptosystem in the presence of AWGN, Salt & peppers noise, and Speckle noise.

Table 4. PSNR values of the deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image cryptosystem in the presence of AWGN, Salt & peppers noise, Speckle noise for color Lena, Peppers, and Baboon images.

Image		Peak Signal to Noise Ratio (PSNR)											
		AWGN				Salt & peppers noise				Speckle noise			
		0.05	0.1	0.5	0.20	0.05	0.1	0.15	0.20	0.05	0.1	0.15	0.20
Lena	R	14.1419	11.7531	10.4783	9.7339	17.8774	14.8182	13.0272	11.7896	16.8056	14.2412	12.6967	11.5935
	G	13.9191	11.5664	10.3867	9.6422	18.0250	15.0545	13.2409	11.9815	20.5135	17.5975	15.9893	14.8222
	B	13.6410	11.3325	10.2135	9.5127	18.4339	15.4741	13.6807	12.4587	20.5419	17.5870	15.8627	14.6794
Peppers	R	13.6938	11.3973	10.2548	9.5418	18.3602	15.4115	13.6199	12.3704	17.4812	14.8371	13.3169	12.2340
	G	14.2696	11.8504	10.6008	9.7724	17.7009	14.6919	12.9321	11.6923	18.7524	16.1572	14.6772	13.6350
	B	14.2602	11.8183	10.5791	9.7669	17.8073	14.6873	12.9196	11.7433	23.1757	20.3173	18.6567	17.4603
Baboon	R	13.7753	11.4709	10.2935	9.5847	18.2978	15.2013	13.4853	12.2267	18.4225	15.6086	13.9932	12.8491
	G	13.6495	11.3388	10.2222	9.5370	18.4902	15.4801	13.7084	12.4234	18.4826	15.7336	14.1884	13.0898
	B	13.9899	11.6267	10.3917	9.6727	18.1092	15.0297	13.3146	12.0745	19.6423	16.8477	16.8477	14.0711

Table 5. SSIM values of the deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image encryption scheme in the presence of AWGN, Salt & peppers noise, Speckle noise for color Lena, Peppers, and Baboon images.

Image		SSIM											
		AWGN				Salt& peppers				Speckle			
		0.05	0.1	0.5	0.20	0.05	0.1	0.15	0.20	0.05	0.1	0.15	0.20
Lena	R	0.0030	0.0030	0.0029	0.0028	0.0031	0.0030	0.0030	0.0029	0.0030	0.0030	0.0029	0.0029
	G	0.3825	0.2794	0.2306	0.1945	0.6018	0.4495	0.3600	0.2984	0.7210	0.6202	0.5556	0.5105
	B	0.3275	0.2227	0.1791	0.1518	0.5708	0.4127	0.3183	0.2625	0.6810	0.5458	0.4619	0.4057
Peppers	R	0.0043	0.0043	0.0042	0.0042	0.0043	0.0043	0.0043	0.0043	0.0044	0.0043	0.0043	0.0042
	G	0.3605	0.2707	0.2269	0.1985	0.5361	0.3989	0.3271	0.2796	0.6598	0.5734	0.5234	0.4847
	B	0.3065	0.2158	0.1748	0.1459	0.5002	0.3495	0.2735	0.2288	0.7979	0.6957	0.6287	0.5780
Baboon	R	0.0022	0.0022	0.0021	0.0021	0.0022	0.0022	0.0022	0.0022	0.0022	0.0021	0.0021	0.0021
	G	0.5206	0.3925	0.3232	0.2830	0.7441	0.6054	0.5095	0.4349	0.7530	0.6433	0.5679	0.5112
	B	0.5565	0.4235	0.3498	0.3053	0.7490	0.6116	0.5199	0.4515	0.8154	0.7280	0.6645	0.6175

Table 6. FSIM values of the deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image encryption scheme in the presence of AWGN, Salt & peppers noise, Speckle noise for color Lena, Peppers, and Baboon images.

Image		FSIM											
		AWGN				Salt& peppers				Speckle			
		0.05	0.1	0.5	0.20	0.05	0.1	0.15	0.20	0.05	0.1	0.15	0.20
Lena	R	0.4329	0.4227	0.4180	0.4156	0.4447	0.4362	0.4298	0.4255	0.4393	0.4299	0.4244	0.4208
	G	0.7079	0.6284	0.5889	0.5586	0.8437	0.7546	0.6861	0.6441	0.8744	0.8231	0.7900	0.7616
	B	0.6494	0.5699	0.5287	0.5046	0.8222	0.7266	0.6585	0.6139	0.8538	0.7864	0.7367	0.7048
Peppers	R	0.5040	0.4960	0.4916	0.4889	0.5192	0.5086	0.5014	0.4978	0.5161	0.5078	0.5026	0.4992
	G	0.6828	0.6065	0.5648	0.5357	0.8162	0.7134	0.6493	0.6042	0.8435	0.7953	0.7631	0.7380
	B	0.6777	0.5963	0.5528	0.5236	0.8193	0.7105	0.6447	0.6004	0.9265	0.8847	0.8561	0.8298
Baboon	R	0.3254	0.3219	0.3211	0.3202	0.3322	0.3289	0.3266	0.3246	0.3304	0.3274	0.3255	0.3244
	G	0.7895	0.7311	0.6974	0.6773	0.9001	0.8377	0.7889	0.7578	0.8921	0.8458	0.8138	0.7895
	B	0.8131	0.7549	0.7164	0.6931	0.9000	0.8397	0.7959	0.7627	0.9193	0.8822	0.8582	0.8346

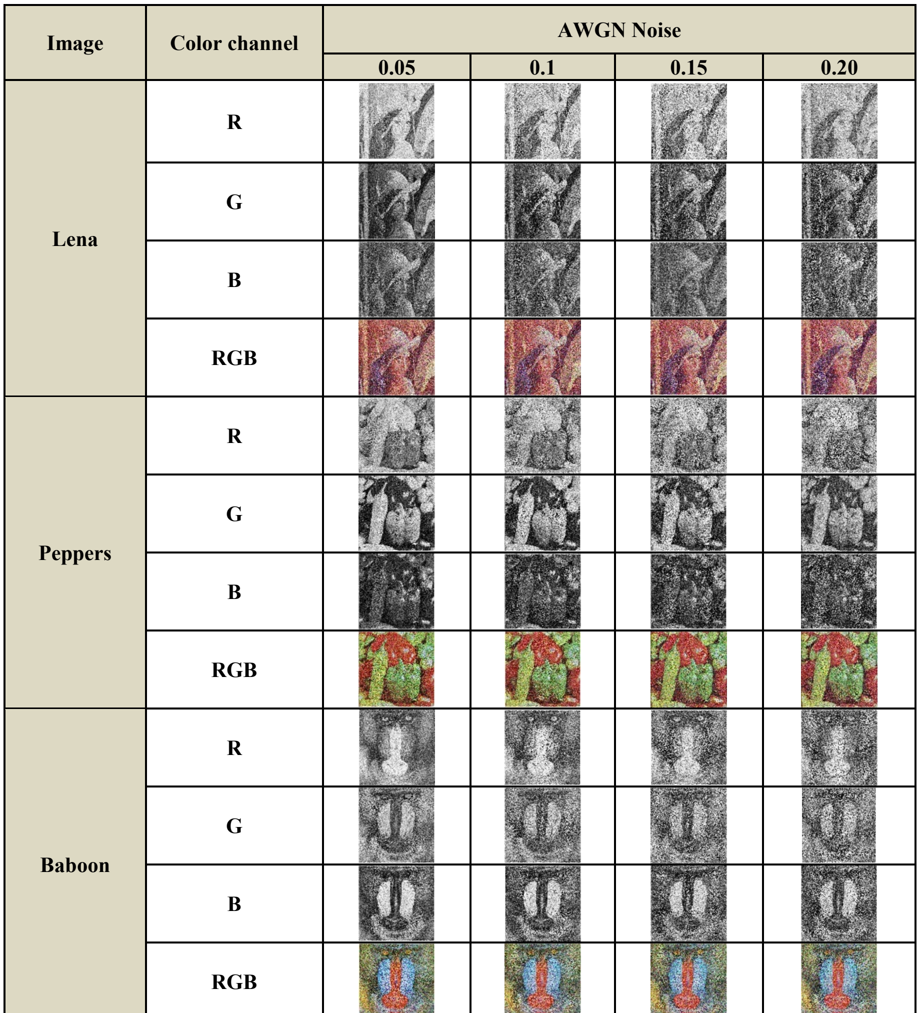


Fig. 9. The resulted deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image encryption scheme in the existence of AWGN noise for color Lena, Peppers, and Baboon images.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

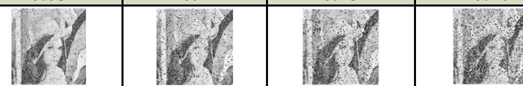
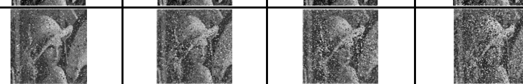
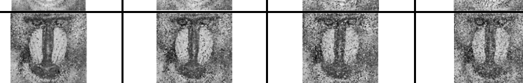
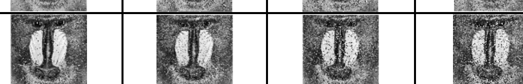
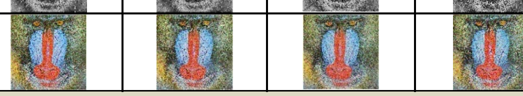
Image	Color channel	Salt & Peppers Noise			
		0.05	0.1	0.15	0.20
Lena	R				
	G				
	B				
	RGB				
Peppers	R				
	G				
	B				
	RGB				
Baboon	R				
	G				
	B				
	RGB				

Fig. 10. The resulted deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image encryption scheme in the existence of Salt & peppers noise for color Lena, Peppers, and Baboon images.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

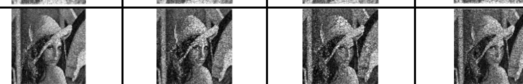
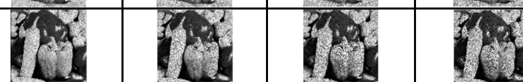
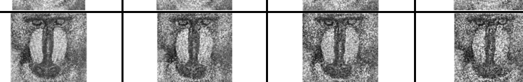
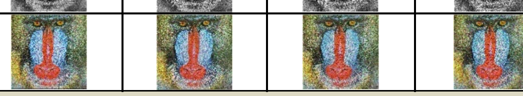
Image	Color channel	Speckle Noise 0.05 – 0.1 – 0.15 – 0.20
Lena	R	
	G	
	B	
	RGB	
Peppers	R	
	G	
	B	
	RGB	
Baboon	R	
	G	
	B	
	RGB	

Fig. 11. The resulted deciphered Red, Green and Blue components using the proposed 2D HM-ALSM image encryption scheme in the existence of Speckle noise for color Lena, Peppers, and Baboon images.

5. CONCLUSION

The paper presents an efficient confusion-diffusion image cryptosystem scheme based on 2D ALSM and 2D HM. In the proposed encryption system, confusion and diffusion operations have been utilized to provide more random behavior. This is realized through 2D ALSM for confusion stage and 2D HM for diffusion stage. These two employed mechanisms have ensured the capability of obtaining an efficient 2D HM-ALSM image encryption system. The proposed 2D HM-ALSM image encryption scheme is examined using multiple security metrics such as statistical, entropy, differential examination, visual notification, and noise resistance tests. Simulation results have validated the performance superiority of the proposed 2D HM-ALSM image encryption scheme.

REFERENCES:

[1] J. Daemen and V. Rijmen, "AES the advanced encryption standard," *The Design of Rijndael*, vol. 1, no. 1, pp. 1-238, 2002.

[2] RL. Rivest, "The RC5 encryption algorithm," in *International Workshop on Fast Software Encryption*, 1994, pp. 86-96.

[3] RL. Rivest, MJ. Robshaw, R. Sidney, YL. Yin, "The RC6 block cipher," in *First Advanced Encryption Standard (AES) Conference*, 1998.

[4] H. Yao, F. Mao, Z. Tang, and C. Qin, "High-fidelity dual-image reversible data hiding via prediction-error shift," *Signal Processing*, vol. 170, pp. 107447, 2020.

[5] L. Dong, J. Zhou, W. Sun, D. Yan and R. Wang, "First Steps Toward Concealing the Traces Left by Reversible Image Data Hiding," *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2020.

[6] A. Gutub and M. Al-Ghamdi, "Hiding shares by multimedia image steganography for optimized counting-based secret sharing," *Multimedia Tools and Applications,* vol. 79, no.13-14, pp. 1-35, 2020.

[7] Z. Tang, H. Nie, CM. Pun, H. Yao, C. Yu C, and X. Zhang, "Color Image Reversible Data Hiding With Double-Layer Embedding," *IEEE Access*, vol.8, pp. 6915-26, 2020.

[8] C. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, pp. 656-715, 1949.

[9] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International journal of bifurcation and chaos*, vol. 16, no. 8, pp. 2129-51, 2006.

[10] JM Amigo, L. Kocarev, and J. Szczepanski, "Theory and practice of chaotic cryptography," *Physics Letters A*, vol. 366, no. 3, pp. 211-6, 2007.

[11] MS. Baptista, "Cryptography with chaos," *Physics letters A*, vol. 240, no. 1-2, pp. 50-4, 1998.

[12] R. Matthews, "On the derivation of a “chaotic” encryption algorithm," *Cryptologia*, vol. 13, no.1, pp. 29-42, 1989.

[13] C. Pak, L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 138, pp. 129-37, 2017.

[14] C. Han, "An image encryption algorithm based on modified logistic chaotic map," *Optik*, vol. 181, pp. 779-85, 2019.

[15] ML. Sahari and I. Boukemara, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption," *Nonlinear Dynamics*, vol. 94, no. 1, pp. 723-44, 2018.

[16] R. Bansal, S. Gupta, and G. Sharma, "An innovative image encryption scheme based on chaotic map and Vigenère scheme," *Multimedia Tools and Applications*, vol. 76, no. 15, pp. 16529-62, 2017.

[17] J. Wang, LY. Zhang, J. Chen, G. Hua, Y. Zhang Y, and Y. Xiang Y, "Compressed sensing based selective encryption with data hiding capability," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 12, pp. 6560-71, 2019.

[18] N. Singh and A. Sinha, "Optical image encryption using fractional Fourier transform and chaos," *Optics and Lasers in Engineering*, vol. 46, no. 2, pp. 117-23, 2008.

[19] H. Alhumyani, "Efficient Image Cipher Based on Baker Map in the Discrete Cosine Transform," *Cybernetics and Information Technologies*, vol. 20, no. 1, pp. 68-81, 2020.

[20] X. Wu, D. Wang, J. Kurths, and H. Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system," *Information Sciences*, vol. 349, pp. 137-53, 2016.

[21] Q. Lu, C. Zhu, and X. Deng, "An efficient image encryption scheme based on the LSS chaotic map and single S-Box," *IEEE Access*, vol. 8, pp. 25664-78, 2020.

[22] M. Kumar, A. Saxena, and SS. Vuppala SS, "A Survey on Chaos Based Image Encryption Techniques," In *Multimedia Security Using Chaotic Maps: Principles and Methodologies*, pp. 1-26, 2020, Springer, Cham.

[23] KA. Patro, MP. Babu, KP. Kumar, and B. Acharya, "Dual-Layer DNA-Encoding–Decoding Operation Based Image Encryption Using One-Dimensional Chaotic Map," In Advances in Data and Information Sciences, pp. 67-80, 2020, Springer, Singapore.

[24] S. Xiao, Z. Yu, and Y. Deng, "Design and Analysis of a Novel Chaos-Based Image Encryption Algorithm via Switch Control Mechanism," *Security and Communication Networks,* vol. 2020, 2020.

[25] MB. Farah, R. Guesmi, A. Kachouri, and M. Samet M, "A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation," *Optics & Laser Technology*, vol. 121, pp. 105777, 2020.

[26] M. Kalra, S. Katyal, and R. Singh, "A Tent Map and Logistic Map Based Approach for Chaos-Based Image Encryption and Decryption," *Innovations in Computer Science and Engineering*, pp. 159-165, 2019, Singapore, Springer.

[27] M. Alawida, A. Samsudin, JS. Teh, and RS. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45-58, 2019.

[28] IT. Almalkawi, R. Halloush, A. Alsarhan, A. Al-Dubai, and JN. Al-karaki, "A lightweight and efficient digital image encryption using hybrid chaotic systems for wireless network applications," *Journal of Information Security and Applications*, vol. 49, pp. 102384, 2019.

[29] A. Mansouri and X. Wang, "A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme," *Information Sciences,* vol. 520, pp. 46-62, 2020.

[30] M. Kaur, D. Singh, K. Sun, and U. Rawat, "Color image encryption using non-dominated sorting genetic algorithm with local chaotic search based 5D chaotic map," *Future Generation Computer Systems,* vol. 107, pp. 333-50, 2020.

[31] B. Mondal, PK. Behera, and S. Gangopadhyay, "A secure image encryption scheme based on a novel 2D sine–cosine cross-chaotic (SC3) map," *Journal of Real-Time Image Processing*, pp. 1-8, 2020.

[32] MZ. Talhaoui, X. Wang, and MA. Midoun, "Fast image encryption algorithm with high security level using the Bülban chaotic map," *Journal of Real-Time Image Processing*, pp. 1-4, 2020.

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

[34] E. Lorenz, "Deterministic nonperiodic flow," *Journal of the atmospheric sciences,* vol. 20, no. 2, pp. 130-141, 1963.

[35] K. Zhou, M. Xu, J. Luo, H. Fan, and M. Li, "Cryptanalyzing an image encryption based on a modified Henon map using hybrid chaotic shift transform," *Digital Signal Processing,* vol. 93, pp. 115-27, 2019.

[36] LO. Tresor LO and M. Sumbwanyambe, "A Selective Image Encryption Scheme Based on 2D DWT, Henon Map and 4D Qi Hyper-Chaos," *IEEE Access*, vol. 7, pp. 103463-72, 2019.

[37] R. Anandkumar and R. Kalpana, "Designing a fast image encryption scheme using fractal function and 3D Henon Map," *Journal of Information Security and Applications*, vol. 49, pp. 102390, 2019.

[38] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Information Sciences*, vol. 339, pp. 237-53, 2016.

[39] RM. May, "Simple mathematical models with very complicated dynamics," *Nature,* vol. 261, no. 5560, 1976.

[40] Y. Zhou, L. Bao, and CP, Chen CP, "A new 1D chaotic system for image encryption," *Signal processing,* vol. 97, pp. 172-82, 2014.

[41] P. Ping P, Y. Mao, X. Lv, F. Xu, and G. Xu, "An image scrambling algorithm using discrete Henon map," *IEEE International Conference on Information and Automation*, Lijiang, China, 2015 Aug 8, pp. 429-432.

[42] P. Ramasamy, V. Ranganathan, S. Kadry, R. Damaševičius, and T. Blažauskas, "An image encryption scheme based on block scrambling, modified zigzag transformation and key generation using enhanced logistic—Tent map," *Entropy,* vol. 21, no. 7, pp. 656, 2019.

[43] A. Roy, AP. Misra, and S. Banerjee, "Chaos-based image encryption using vertical-cavity surface-emitting lasers," *Optik*, vol. 176, pp. 119-31 2019.

[44] OS. Faragallah, "Digital image encryption based on the RC5 block cipher algorithm," *Sensing and Imaging: An International Journal*, vol. 12, no. 3-4, pp. 73-94, 2011.

[45] E. Naeem, M. Elnaby, N. Soliman, A. Abbas, O. Faragallah, N. Semary, and F. El-Samie, "Efficient implementation of chaotic image encryption in transform domains," *Journal of Systems and Software*, vol. 79, pp. 118-127, 2014.