computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

AN EFFICIENT CONFUSION-DIFFUSION STRUCTURE FOR IMAGE ENCRYPTION USING PLAIN IMAGE RELATED HENON MAP

Mohammed Hussein Ahmed [1], Ahmed Kareem Shibeeb [2], Fadhil Hanoon Abbood [1]

[1] Department of Computer Science, College of Education, Al-Mustansiriyah University, Baghdad, Iraq, mohammedalbawi@uomustansiriyah.edu.iq, alsaadi.graphic@gmail.com
[2] Department of Computer Systems, Technical Institute – Suwaira, Middle Technical University Baghdad, Iraq, ahmed.kareem@mtu.edu.iq

Paper history:
Received 04 May 2020
Received in revised form 24 June 2020
Accepted 08 July 2020
Available online 27 September 2020

Keywords:
Henon map;
Image cryptosystem;
Gray difference degree (GVD);
Encryption quality.

Abstract: Chaos-based image encryption has great significance as a branch of image security. So, a series of chaos-based cryptosystems protecting digital images are proposed in recent years. But, most of them have been broken as a result of poor encryption structure. This research paper suggests an effective image encryption structure to resist possible attacks. The proposed method employs plain image related Henon map (PIHM) for shuffling and diffusion processes in a connected way which is different from conventional chaotic based image encryption systems, since the initial conditions of diffusion process are established based on the initial conditions of shuffling process. The principle of confusion is achieved by shuffling the pixels over all the rows and columns. And the diffusion is ensured by using XOR operation of current shuffled pixel value with the previous value, and random pixel produced from PIHM map. The results of simulation and security analysis indicate that the proposed scheme has desirable encryption effects and is robust against different common attacks.

1. INTRODUCTION

In the present age of the fast development of information transmission and multimedia technology, the privacy protection of the digital data in cyberspace must be emphasized. The traditional cryptography approaches like Data Encryption Standard (DES) [1], Advanced Encryption Standard (AES)[2], Rivest-Shamir-Adleman (RSA)[3], etc. are playing a significant role in textual data security, but they are unacceptable for image encryption, image data security due to some inherent properties of digital multimedia such as high degree of redundancy, bulk content capacity, pixels correlation, and execution time constraints. In order to address these issues and problems, various modifications have been suggested to make the traditional encryption algorithms more suitable for image security [4]–[6].

Due to the features of dynamic instability, unpredictability, and ergodicity that can be applied in the cryptography applications, the chaotic system has been used in a wide variety of image cryptosystems. In 1998, the American researcher Fridrich proposed chaos-based image encryption method for the first time [7]. Fridrich's Symmetric algorithm includes two stages: permutation process (i.e., shuffling the location of pixels) and diffusion process (i.e., changing the value of pixels). Despite the success of cryptanalyzing in 2010 [8], many cryptographers design their image encryption algorithms based on Fridrich's structure [9]–[12].

The basic shortcomings of Fridrich's structure are summarized as follows [8, 9]:

a) The pixels shuffling and diffusion are simple to cryptanalysis.
b) The shuffling and diffusion processes are independent of each other.
c) The encryption algorithm is not associated with the plaintext image.

To date, many image cryptosystems have been proposed to obtain a higher level of security by different chaotic map like one-dimensional logistic map [14], tent map [15], delayed coupled map [16], two-dimensional adjusted logistic map [17], three-

dimensional cat map [18], 4D logistic map [19] and 6D hyperchaotic system [20], etc. Generally, one-dimensional maps provide simple mathematical function, short key size, and insecure cryptosystem [14]. Hence, they are exposed to attack more than high dimensional chaotic maps [21]. In contrast, the high dimensional maps can withstand attack more than one-dimensional maps, but they require high-execution time in hardware and software implementation. Besides, the close connection between the encryption and decryption processes makes the algorithm strong against the attack of known-chosen plaintext [22].

Motivated by the above introduction and to address this shortcoming, a new image cryptosystem under an efficient connected structure of confusion-diffusion is suggested in this article. The proposed cryptosystem does not utilize a complex high dimensional chaotic system or hash algorithm, but it utilizes statistical property that is extracted from a plain image to enhance the chaotic behavior of modified two-dimensional Henon map [23] and immunity of the encryption algorithm against known-chosen plaintext cryptanalysis.

The remainder of this research paper is organized as follows: Section 2 presents the related works. In Section 3, the two-dimensional Henon map is explained. Section 4 shows the proposed image cryptosystem. Then, the performance of the proposed cryptosystem is evaluated and compared with existing systems in Section 5. Finally, Section 6 concludes this work and proposes future work.

2. RELATED WORKS

To take advantage of chaotic systems in a digital computer and improve the security of image cryptosystems, various methods have been proposed. Selecting a map type is not enough. Thus, some researchers try to avoid any possible attacks such as chosen and known-plaintext attacks, e.g., the authors in [24] presented a fast image cryptosystem based on a dimensional logistic map with optimized distribution and total original image characteristics to secure the color images. Despite the increase in the time of implementation when using hash algorithms, Change Dong [25] introduced a color image encryption scheme by using the hash value of the input image to generate the initial values of the coupled chaotic system for each encryption process. Xiangjun Wu et al. [26] combined the output hash function with a secret key and original image to update the system parameters and initial values of NCA map based CML, which is used with DNA coding for color image encryption. Also, a hash algorithm has been used by Ahmad Jawad et al. [27], in that research work, an enhanced image cryptosystem was introduced based on skew tent map and XOR operation. In [28], the authors used the hash value of the plain image to generate the cipher key. The cryptosystem utilizes PWLCM systems in three levels of permutation process and diffusion processes. Both pixel level and bit-level permutation are applied by Xiong et al. [29], who used a nine palace map for pixel permutation process and Cyclic Redundancy Check (CRC) technique to permute the binary vectors of R, G, B pixels. The output pixels are XORed to diffuse them. The authors in [30] proposed plain image sensitive cipher by applying the particle swarm optimization algorithm (PSO) to choose a lower correlated encrypted image as an output of the cryptosystem.

Moreover, modified classical cryptosystems and chaotic maps in the image encryption field were used in [31,32], pseudorandom sequences were generated in [31] based on improved Chebyshev map, logistic map, and sine map to avoid the problems of low dimensional maps through increasing the keyspace. Then, the variant Hill cipher was used to encrypt the image data pixel-by-pixel instead of the pairs of pixels which followed in the classical Hill cipher. The authors of [32] proposed a block image cryptosystem with 16 ×16 blocks, this scheme utilizes a chaotic cross-map to achieve diffusion property and to improve Playfair cipher in the confusion process.

Mondal et al. [33] introduced a faster pseudorandom generator based on skew tent map and cellular automata to secure the digital images, where the output of pseudorandom generator was used in the shuffling process and diffusion process. Hanchinamani and Kulakarni [34] adopted a two-dimensional Zaslavskii map for the shuffling process, combined with pseudo Hadmard transform, to provide avalanche effect. Then, forward and backward diffusion processes are achieved by multiple addition operations and XOR operation. Krishnamoorthi and Murali [35, 36] came up with and applied a selective image cryptosystems based on chaotic maps and orthogonal polynomials transform. They divided the image data into important and unimportant sections. the important section has been secured more than an unimportant section to decrease the complexity of the proposed cryptosystem. Also, the authors in [37] attempted to decrease the time complexity by applying one round diffusion operation. The suggested scheme used a large key space-based on the hyper-chaotic system. Butt et al. [38] introduced a low complex image cryptosystem via a combination of the shuffling process and diffusion process for the bit-planes of an input image. This method uses a hash function to generate a 128-bit keystream and performs modular addition operation to diffuse image blocks.

3. TWO-DIMENSIONAL HENON MAP (2DHM)

Henon map is a two-dimensional discrete-time dynamical system, which is described as follows:

$$\begin{aligned} X_{t+1} &= 1-\alpha * X_t + Y_t \\ Y_{t+1} &= \beta * X_t \end{aligned}, \quad (1)$$

where X_t and Y_t represent the iterated space variables and lie in the range[0,1], α and β are the parameters of the system. This system yields a complete chaotic attractor at $\alpha = 1.4$ and $\beta = 0.3$ as shown in Fig. 1.

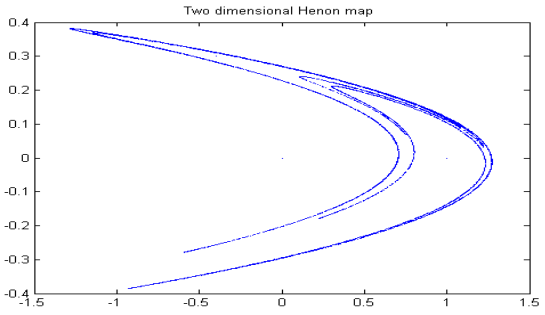

Figure 1 – Chaotic attractor of two-dimensional Henon map with $\alpha = 1.4$, $\beta = 0.3$, $X_0 = 0$ and $Y_0 = 0$

4. THE PROPOSED IMAGE CRYPTOSYSTEM

The proposed algorithm is composed of two associated parts: shuffling–diffusion structures both of them are dependent on the plain image related Henon map (PIHM) to obtain a satisfactory image cryptosystem. Fig. 2 presents a block diagram that illustrates the processes of the proposed image cryptosystem.

4.1 PLAIN IMAGE RELATED HENON MAP (PIHM)

In this process, we extract statistical property (A) from the original image as the following mathematical model:

$$A = \sqrt{\sum PI(i,j)^2 + r}, \quad (2)$$

where PI(i, j) is the gray value of the plaintext image and r is a random parameter. The value of r must be large than 0 to withstand a special image attack. The statistical property A will be multiplied with Henon map as presented in Equation (3) to enhance the immunity of the proposed scheme against known-chosen plaintext cryptanalysis, and to improve Henon map since the multiplication design and modular operator are used to enhance the chaotic dynamic of the Henon map without affecting the keyspace [23].

$$\begin{aligned} X_{t+1} &= Mod(((1-\alpha * X_t + Y_t) * A),1) \\ Y_{t+1} &= Mod(((\beta * X_t) * A),1) \end{aligned}. \quad (3)$$

The PIHM will be used in the shuffling process with initial conditions (X_{01}, Y_{01}) and control parameters (α_0, β_0). On the other hand, the initial conditions of the diffusion process are (X_{02}, Y_{02}) and the control parameters are (α_1, β_1).

4.2 SHUFFLING STAGE

In order to provide confusion property, the shuffling process permutes the positions of the pixels over all the rows and columns by using the produced sequence from PIHM map (X_t, Y_t).

The phase of row shuffling is responsible for performing permutation operation on each row of the plain image PI(i, j) as shown in the following formula:

$$PI(i,j) = \begin{cases} K_1 + i & \text{IF } K_1 + i \le M \\ K_1 + i - M & \text{IF } K_1 + i > M \end{cases}, \quad (4)$$

where M represents the width of the original image $PI(i,j) = M \times N$ and K_1 is obtained using the following equation:

$$K_1 = Mod(Floor(X_t * 10^{15}),256) + z. \quad (5)$$

Here, Floor (.) is a mathematical function used for rounding of numerical data to the nearest integer number; X_t represents the generated sequence of PIHM map and z is a random number.

In contrast, the column shuffling phase uses X_t sequence to permute the columns pixels as follows:

$$PI(i,j) = \begin{cases} K_2 + j & \text{IF } K_2 + j \le N \\ K_2 + j - N & \text{IF } K_j + j > N \end{cases}, \quad (6)$$

where N denotes the height of the plain image and K_2 is calculated using the following equation:

$$K_2 = Mod(Floor(Y_t * 10^{15}),256) + z. \quad (7)$$

The security of the output image of the shuffling stage also depends on the iteration number. Thus, the proposed cryptosystem considered $itr_{shuffling}$ as a secret key.

4.3 DIFFUSION STAGE

The rows-columns pixels shuffling process in the previous subsection makes the cryptosystem pass

most security tests except the histogram test which can be achieved through the diffusion process.

The attack on the shuffling-diffusion structure is possible as the shuffling process is independent of the diffusion process and the plain image [22]. Therefore, the proposed scheme combines the shuffling process with the diffusion process as well as provides the connection between the original image and Henon map. The combination of shuffling-diffusion processes involves utilizing the values of the initial conditions of the shuffling stageX_{01} and Y_{01} to establish the initial conditions of the diffusion stageX_{02} and Y_{02} as follows:

$$X_{02} = \mathrm{Mod}\,(X_{02} + \frac{X_{01}}{f},1)$$
$$Y_{02} = \mathrm{Mod}\,(Y_{02} + \frac{Y_{01}}{g},1) \quad , \qquad (8)$$

where f and g are random prime numbers. Then, the proposed scheme iterates Equation (3) with a new version of initial conditions X_{02} and Y_{02} for $M \times N$ times to generate the random image $\mathrm{RI}(i,j)$. After that, the current pixel and previous pixel of the shuffled image and corresponding pixel of a random image are mixed by utilizing XOR operation as the following mathematical model:

$$EI(i,j) = \begin{cases} PI_i \oplus \mathrm{RI}_i & \mathrm{IF}\, i=1 \\ PI_i \oplus PI_{i-1} \oplus \mathrm{RI}_i & \mathrm{IF}\, i\neq 1 \end{cases} . \qquad (9)$$

Finally, the mixed image $\mathrm{EI}(i,j)$ is considered as an encrypted image and it is ready to be submitted to the recipient with the same secret keys. When a recipient receives the encrypted image, he will reverse the operations of the proposed image cryptosystem to decrypt the cipher image.

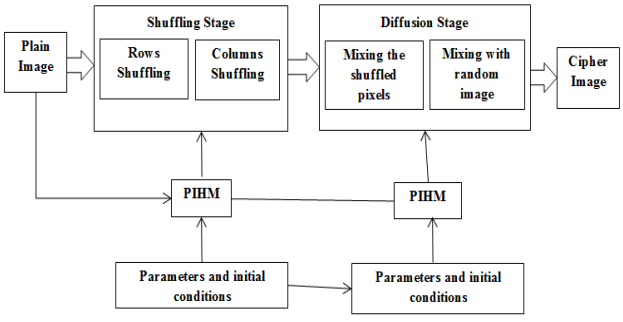

Figure 2 – Block diagram of the proposed image encryption scheme

5. PERFORMANCE AND SECURITY ANALYSIS

The performance of the proposed research work is tested and analyzed with two images from the last version of the USC-SIPI image database including "Mandrill", "Peppers", "Airplane", "Splash" and "House" and each of size 512× 512 as shown in Fig. 3. Also, the cryptosystem keys are $X_{01} = -0.793801, Y_{01} = 0.164091, X_{02} = 0.557744$, $Y_{02} = -0.344259$, $\alpha_0 = 1.4001$, $\beta_0 = 0.300027$, $\alpha_1 = 1.40098$, $\beta_1 = 0.300063$, $\mathrm{itr}_{\mathrm{shuffling}} = 1000$, $\mathrm{itr}_{\mathrm{diffusion}} = 300 + (3 \times M \times N)$, $r = 17$, $z = 100$, $f = 317$ and $g = 213$.

In order to verify the efficiency of the proposed image encryption scheme, we have evaluated it against different security criteria that involve the space of the secret key, sensitivity analysis, pixel distribution test, correlation analysis, information entropy, and the measure of encryption quality. Finally, the speed performance of the proposed cryptosystem is tested to determine the time taken by the encryption and decryption processes.

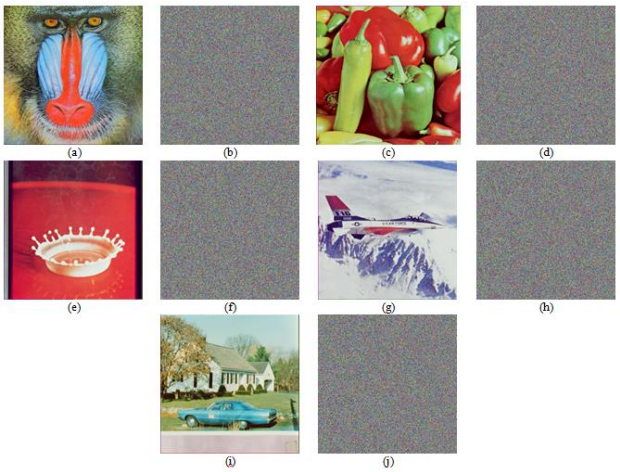

Figure 3 – Experimental outputs: Original image (a) "Mandrill", (c) "Peppers", (e) "Splash" (g) "F-16" and (i) "House" image; Cipher image (b) "Mandrill", (d) "Peppers", (f) "Splash" (h) "F-16" and (j) "House" image.

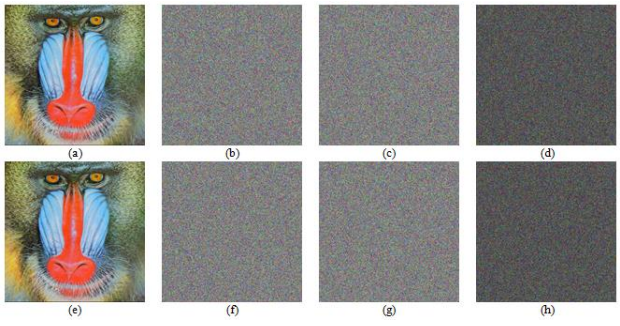

Figure 4 – Secret key sensitivity analysis: (a) Plain image; (b) Cipher image EI_1 with X_{01}; (c) Cipher image EI_2 with $X_{01} + 10^{-15}$; (d) Difference image $DiffI_1$ of EI_1 and EI_2; (e) Decrypted image DI_1 of EI_1 with X_{01}; (f) Decrypted image DI_2 of EI_1 with $X_{01} + 10^{-15}$; (g) Decrypted image DI_3 of EI_2 with X_{01}; (h) Difference image $DiffI_2$ of DI_2 and DI_3.

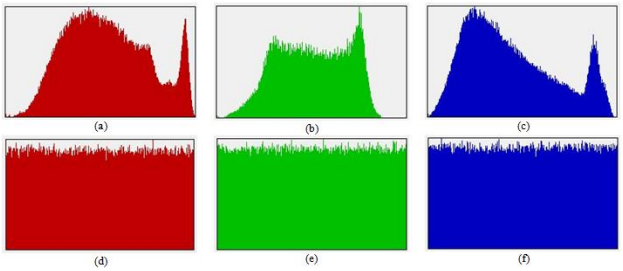

Figure 5 – Pixels distribution analysis of the plain image of "Mandrill" in (a) Red, (b) Green, (c) Blue channels; corresponding pixels distribution of the cipher image (d)–(f).

5.1 SECRET KEY SPACE ANALYSIS

The cryptosystem resistance against the brute force attack depends on the secret key size. Typically, the key size should be more than 2^{128} to thwart the brute force attack [25]. The proposed cryptosystem provides key size up to 2^{504}, where the initial values and system parameters of the enhanced Henon map provides 2^{222} for each map as described in Ref [23]. Besides, considering the moderate size for $itr_{shuffling}$ $itr_{diffusion}$, r, z, f, and g is 2^{60}. As demonstrated in Table 1, the proposed cryptosystem is able to withstand against brute force attacks.

Table 1. Secret keyspace of the proposed research work and comparable cryptosystems.

Proposed work	[14]	[24]	[26]	[29]
2^{504}	2^{190}	2^{128}	2^{203}	2^{166}

5.2 SENSITIVITY ANALYSIS

5.2.1 PLAIN IMAGE SENSITIVITY

Many cryptanalyzes try to modify the pixel value of the original image and compare the original and modified image with their corresponding encrypted images to find the relationship between them. This attack is called differential cryptanalysis, and it is evaluated by utilizing the number of pixel changing rate (NPCR) and unified average change intensity (UACI). They are calculated by using equations (10), (11), and (12).

$$EI(i,j) = \begin{cases} 0 & \text{IF } EI_1(i,j) = EI_2(i,j) \\ 1 & \text{IF } EI_1(i,j) \neq EI_2(i,j) \end{cases} \quad (10)$$

$$NPCR = \sum_{ij} \frac{V(i,j)}{M * N} * 100\% \quad (11)$$

$$UACI = \sum_{ij} \frac{|EI_1(i,j) - EI_1(i,j)|}{255 * M * N}, \quad (12)$$

where $EI_1(i,j)$ and $EI_2(i,j)$ are the cipher images that occurred before and after one-pixel modification; M and N are the width and height of the tested image, respectively. The optimal value of NPCR is about 99.61%, while UACI is about 33.46. Compared to the previous works, the suggested cryptosystem introduces high resistance against differential cryptanalysis as obtained in Table 2.

5.2.2 KEY SENSITIVITY

Similar to the plaintext image sensitivity, the key sensitivity criteria mean no plain data is retrieved from the encrypted image even if only a little dissimilarity is between the key of the encryption process and the decryption process. To achieve the secret key sensitivity characteristic, the image encryption scheme must meet the following conditions:

d) A tiny modification in the secret key leads to a completely different cipher image.
e) The cipher algorithm must be unable to discover any data from the cipher image even for the tiny difference in the decryption key.

Fig. 4 clearly shows the simulation outputs of key sensitivity measure in the proposed cryptosystem by altering secret key $X_{01}$to $X_{01} + 10^{-15}$, and keep others unaltered. Utilize $X_{01}$to encrypt Mandrill plain image in Fig. 4(a) and produce the output image EI_1 in Fig. 4(b). After that, encrypt the same Mandrill plain image PI in Fig. 4(a) by using $X_{01} + 10^{-15}$ to obtain a new output image EI_2 as shown in Fig. 4(c), and Fig. 4(d) illustrates the pixel-to-pixel difference image DiffI between EI_1 and EI_2. In a similar way, the sensitivity measure can be performed in the decryption process to obtain the decrypted image DI as shown in Fig. 4(e), Fig. 4(f), Fig. 4(g), and Fig. 4(h). Thus, the proposed image encryption method is extremely sensible to its secret key.

5.3 PIXELS DISTRIBUTION ANALYSIS

The distribution of pixels refers to the plot number of image pixels at each different intensity value for each of the images. The encrypted image of good cryptography must have sufficiently even distribution for image pixels to resist the histogram analysis. As illustrated in Fig. 5, the plot of pixels distribution of the cipher image is more even than the plain image for R, G, and B channels. Thus, the proposed image cryptosystem can make pixels distribution analysis difficult.

Table 2. Comparison of proposed NPCR and UACI values with existing values.

Images	Proposed Scheme		Other schemes		
	NPCR %	UACI	NPCR %	UACI	References
Mandrill	99.821	33.57	99.618	33.781	[27]
Peppers	99.722	33.373	99.167	33.667	[30]
Splash	99.684	33.142	99.619	33.462	[28]
F-16	99.851	33.107	99.629	33.54	[31]
House	99.691	33.369	98.905	33.567	[32]

5.4 ADJACENT PIXELS ANALYSIS

5.4.1 CORRELATION COEFFICIENT TEST

Due to the high relationship between the neighbor pixels of several plaintext images, the correlation coefficient test is utilized in the image encryption algorithms to evaluate the degree of pixel shuffling. We apply Equation (13), (14) and (15) for 1,500 pairs of neighboring pixels from the input and output images of the proposed cryptosystem and measure the correlation coefficient CC_{XY} at horizontal, vertical, and diagonal directions [39].

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{13}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \tag{14}$$

$$CC_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{15}$$

where x_i and y_i are two adjacent pixels, and N is the sequence length. The optimal value for CC_{XY} is close to zero. From the experimental results in Table 3, the ciphertext correlation value of the proposed work is close to zero in all directions, and it is lower than in other works. Also, scatter plots of correlation coefficients of Mandrill image in all directions are illustrated in Fig. 6. From the results of correlation analysis, the proposed image cryptosystem is very suitable for securing a highly correlated image.

5.4.2 GRAY DIFFERENCE DEGREE ANALYSIS

A gray difference degree (GDD) test is performed to examine the scrambling efficiency of the image encryption algorithm. To evaluate the GDD for M×N image, first, we have to calculate the gray difference (GD) for all pixels except the pixels of the edges with the following expression:

$$GD(x,y) = \frac{\sum\left[I(x,y) - I(\bar{x},\bar{y})\right]^2}{4}, \tag{16}$$

where $I(x,y)$ represents the gray value of image pixel, and $I(\bar{x},\bar{y})$ is a gray value of four neighborhood pixels at $(x+1,y)$, $(x-1,y)$, $(x,y+1)$ and $(x,y-1)$ positions. After that, the result of a gray difference degree can be computed by using equations (17) and (18).

$$E(GD(x,y)) = \frac{\sum_{x=2}^{M-1}\sum_{y=2}^{N-1} GD(X,Y)}{(M-2)(N-2)} \tag{17}$$

$$GDD = \frac{\left[\overline{O}(GD(X,Y)) - O(GD(X,Y))\right]}{\left[\overline{O}(GD(X,Y)) + O(GD(X,Y))\right]}, \tag{18}$$

where O and $\overline{O}$ refer to the average neighborhood gray difference of the plaintext images and the ciphertext images, respectively. A gray difference degree, which is close to one, means that it is very difficult for the cryptosystem to reveal information. As obtained from the comparison results in Table 4, the gray difference degree of the proposed algorithm is close to one which means that there is a negligible relationship among original and encrypted images.

5.5 INFORMATION ENTROPY

Entropy measure can be utilized to describe the randomness of pixels in the entire image. The uniformity of gray pixels distribution is reflected positively with image entropy getting increased as well. Mathematically, image entropy can be described as follows:

$$E(w) = \sum_{i=1}^{M} \mathrm{Pro}(w_i)\log_2 \mathrm{Pro}(w_i), \tag{19}$$

where Pro (w_i) refers to the probability of symbol w_i and M is the total number of w_i. For a good image encryption algorithm, the information entropy (E) value of the ciphertext image should be approximate to eight [40]. Table 5 shows the calculation of plaintext and ciphertext images. As it can be seen from the results, the image entropy of the proposed cryptosystem is very close to eight. Consequently, the proposed method is robust against the statistical attack.

Table 3. Comparison results of correlation coefficient test in various directions.

Schemes	Images	Original image			Cipher image		
		H	V	D	H	V	D
Ours	Mandrill	0.8917	0.8563	0.8751	0.0044	-0.0002	-0.0013
	Peppers	0.9862	0.9843	0.9764	**0.0011**	**-0.0018**	**0.0007**
	Splash	0.9927	0.9901	0.9855	0.0061	0.0058	0.0026
	F-16	0.9623	0.9507	0.9518	-0.0057	0.0009	-0.0015
	House	0.9519	0.963	0.9566	0.0022	0.0063	-0.0041
[29]	**Peppers**	0.9706	0.9727	0.9604	**0.0079**	**-0.0975**	**0.005**
[32]	**Peppers**	0.9472	0.955	0.8983	**0.0485**	**−0.0218**	**0.0058**
[33]	**Peppers**	0.9786	0.982	0.9694	**-0.0263**	**-0.0015**	**0.0126**

5.6 ENCRYPTION QUALITY

This measure gives the result of an average number of alterations for each gray level between the plaintext image and ciphertext image. It can be defined through the following equation [41]:

$$EQ = \sum_{g=0}^{2^8-1} \frac{(Hg(PI) - Hg(EI))^2}{2^8}, \qquad (20)$$

where Hg(PI) and Hg(EI) represent the number of occurrences for each gray level g in the original and cipher images, respectively. An image cryptosystem is ideal for work when the encryption quality is large. The present encryption qualities results are tabulated in Table 6 along with those reported in previous works. The encryption qualities results of the proposed cryptosystem are found to be perfect in comparison to the ones described in the previous works.

5.7 ABILITY TO RESIST CHOSEN AND KNOWN PLAINTEXT ATTACKS

The chosen and known-plaintext attacks are other widespread attacks in cryptanalysis science. To make the cryptosystem able to resist such attacks, there are two points to consider. Firstly, the cipher algorithm must be related to a plain image. The shuffling stage and diffusion stage should be closely related [22].

In the proposed cryptosystem, the encryption process depends on Plain image related Henon map (PIHM). Moreover, the relationship between the shuffling and diffusion stages is achieved by establishing the initial conditions of diffusion operation based on the initial conditions of shuffling operation, and also by mixing the pixels of the shuffled image before XORing them with the random pixels as described in equation (9). Thus, the proposed algorithm has an efficient confusion-diffusion structure. Besides, the cipher algorithm also has a connection with the input image.

Some cryptanalysts utilize special images for encryption, such as a black image with zero pixels to analyze the cryptosystem. To show the resistance of the proposed method against such a situation, the black image in Fig. 7(a) is encrypted by using the proposed cryptosystem, and the result is illustrated in Fig. 7(b). Then, the cipher black image may be used as a possible cipher key to implementing a known-plaintext attack on the cipher Mandrill image but it does not decrypt it as shown in Fig. 7(c) and Fig. 7(d). From equation (2), the statistical value of the black image is $A = \sqrt{r}$, and Mandrill image was encrypted with $A = \sqrt{\sum PI(i,j)^2 + r}$. Consequently, the proposed cryptosystem can produce entirely different output images even with the same keys, proving that the proposed method can resist the chosen and known-plaintext cryptanalysis.

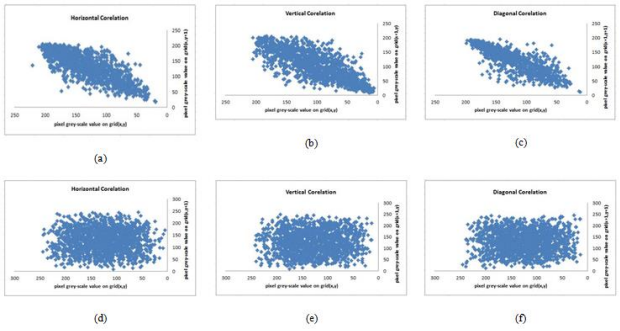

Figure 6 – Scatter plot of "Mandrill" image: (a) horizontally, (b) vertically, and (c) diagonally plot of a plain image; (d) horizontally, (e) vertically and (f) diagonally plot of cipher image.

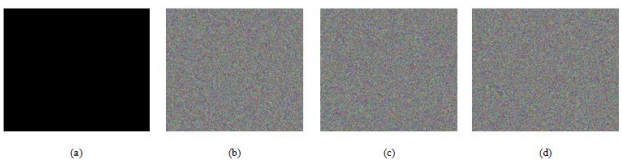

Figure 7 – The simulation results of chosen and known-plaintext attacks: (a) black image, (b) the cipher image of the black image, (c) the cipher image of "Mandrill" image, and (d) deciphered "Mandrill" image with a recovered key from the cipher black image.

Table 4. GDD measure results and comparison with other cryptosystems.

Images	Proposed cryptosystem	Other cryptosystems	
	GDD	GDD	References
Mandrill	0.9771	0.9038	[34]
Peppers	0.9885	0.9637	[34]
Splash	0.9866	0.9825	[36]
F-16	0.9785	0.955	[36]
House	0.9883	0.976	[35]

Table 5. Entropy analysis of the proposed cryptosystem and exist cryptosystems.

Image	Plain image	Proposed scheme	Other schemes	
	E	E	E	Refere-nces
Mandrill	7.7624	7.9998	7.9971	[34]
Peppers	7.6698	7.9998	7.9797	[30]
Splash	7.2428	7.9996	7.9817	[36]
F-16	6.6639	7.9997	7.9994	[33]
House	7.4858	7.9998	7.9972	[37]

Table 6. Encryption quality test results and comparison with other cryptosystems.

Images	Proposed cryptosystem	Other cryptosystems	
	Encryption quality	Encryption quality	References
Mandrill	791.5278	774.0313	[33]
Peppers	805/1242	596.1719	[33]
Splash	625.671	209.32	[37]
F-16	783.1265	758.1640	[33]
House	674.8024	292.3333	[38]

Table 7. The results of encryption time analysis and comparison with other cryptosystems.

Image size	Proposed cryptosystems	[29]	[38]	[28]
512×512	0.907-1.315 s	20.916-21.286 s	3.77	1.623-1.989 s

5.8 COMPUTATIONAL TIME ANALYSIS

An important issue in multimedia security is the processing time. To evaluate the computational timing, the practical application of the proposed scheme is applied in C#.net 2013 programming language on Microsoft Windows 7with Intel Core i3-2328M CPU @ 2.20 GHz, 4.0 GB RAM and the images size of 512×512. The comparison of processing time in the second unit is reported in Table 7. That is to say, the proposed work is more rapid than most of the other cryptosystems and suitable for real-time applications.

6. CONCLUSIONS

In this research paper, an efficient image cryptosystem using plain image-based Henon map (PIHM) is presented. The proposed scheme combines confusion and diffusion processes to ensure higher protection and excellent resistance capability. The PIHM is applied to permute plain image using row-column pixel shuffling. Then, the pixels of the permuted image are mixed before mixing them with random pixels using XOR operation. From the results of performance analysis, it is found that the suggested cryptosystem has a perfect encryption quality, is highly sensible to the secret key and original image, and has even pixel distribution, big secret key space, and low autocorrelation. Moreover, the proposed cryptosystem is fast running and can effectively resist usual attacks such as the differential, known, and chosen-plaintext attacks. Due to the computing efficiency of the proposed cryptosystem, we intend to apply it for wireless communication systems in future work as well as consider a quality evaluation of the deciphered image at the recipient.

7. REFERENCES

[1] D. Coppersmith, "The Data Encryption Standard (DES) and its strength against attacks," *IBM Journal of Research and Development*, vol. 38, issue 3, pp. 243–250, 1994.

[2] D. E. Standard, "Federal information processing standards publication 46," National Bureau of Standards, US Department of Commerce, vol. 23, pp. 1–18, 1977.

[3] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Upper Saddle River, 2017.

[4] R.Shaktawat, R.S. Shaktawat, I. Suwalka, N. Lakshmi, "Implementation of block-based symmetric algorithms for real image encryption," in: A. Chaudhary, C. Choudhary, M. Gupta, C. Lal, T. Badal (Eds.), *Microservices in Big Data Analytics*, Springer, Singapore, 2020, pp. 127-140.

[5] G. Lokeshwari, S. Susarla, S. U. Kumar, "A modified technique for reliable image encryption method using Merkle-Hellman cryptosystem and RSA algorithm," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 18, issue 3, pp. 293–300, 2015.

[6] S. A. Abaas, A. K. Shibeeb, "A new approach for video encryption based on modified AES algorithm," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 17, issue 3, pp. 44–51, 2015.

[7] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, issue 6, pp. 1259–1284, 1998.

[8] E. Solak, C. Çokal, O. T. Yildiz, T. Biyikoğlu, "Cryptanalysis of Fridrich's chaotic image encryption," *International Journal of Bifurcation and Chaos*, vol. 20, issue 5, pp. 1405–1413, 2010.

[9] A. Kanso, M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, issue 7, pp. 2943–2959, 2012.

[10] J. Chen, Z. Zhu, C. Fu, H. Yu, Y. Zhang, "Reusing the permutation matrix dynamically for efficient image cryptographic algorithm," *Signal Processing*, vol. 111, pp. 294–307, 2015.

[11] Z. Gan, X. Chai, M. Zhang, Y. Lu, "A double color image encryption scheme based on three-dimensional brownian motion," *Multimedia Tools and Applications*, vol. 77, issue 21, pp. 27919–27953, 2018.

[12] W. Zhang, H. Yu, Z. Zhu, "An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion," *Signal Processing*, vol. 151, pp. 130–143, 2018.

[13] E. Y. Xie, C. Li, S. Yu, J. Lü, "On the cryptanalysis of Fridrich's chaotic image encryption scheme reference," *Signal Processing*, vol. 132, pp. 150-154, 2016.

[14] M. Arora, M. Khurana, "Secure image encryption technique based on Jigsaw transform and chaotic scrambling using digital image watermarking," *Optical and Quantum Electronics*, vol. 52, issue 2, article no. 59, 2020.

[15] C. Li, G. Luo, K. Qin, C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, issue 1, pp. 127–133, 2017.

[16] I. Hussain, M. A. Gondal, "An extended image encryption using chaotic coupled map and S-box transformation," *Nonlinear Dynamics*, vol. 76, issue 2, pp. 1355–1363, 2014.

[17] M. Sharma, "Image encryption based on a new 2D logistic adjusted logistic map," *Multimedia Tools and Applications*, vol. 79, issue 1–2, pp. 355–374, 2019.

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

[19] S. Stalin, P. Maheshwary, P. K. Shukla, M. Maheshwari, B. Gour, A. Khare, "Fast and Secure Medical Image Encryption Based on Non Linear 4D Logistic Map and DNA Sequences (NL4DLM_DNA)," *Journal of Medical Systems*, vol. 43, issue 8, article no. 267, 2019.

[20] S. A. Mehdi, Z. L. Ali, "Image encryption algorithm based on a novel six - dimensional hyper - chaotic system," *Al-Mustansiriyah Journal of Science*, vol. 31, issue 5, pp. 54-63, 2020.

[21] H. Wang, D. Xiao, X. Chen, H. Huang, "Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map," *Signal Processing*, vol. 144, pp. 444–452, 2018.

[22] W. Feng, Y.-G. He, H.-M. Li, C.-L. Li, "Cryptanalysis of the integrated chaotic systems based image encryption algorithm," *Optik*, vol. 186, pp. 449–457, 2019.

[23] M. O. Meranza-Castillón, M. A. Murillo-Escobar, R. M. López-Gutiérrez, and C. Cruz-Hernández, "Pseudorandom number generator based on enhanced Hénon map and its implementation," *International Journal of Electronics and Communications (AEÜ)*, vol. 107, pp. 239–251, 2019.

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

[25] C. Dong, "Color image encryption using one-time keys and coupled chaotic systems," *Signal Process. Image Communication*, vol. 29, issue 5, pp. 628–640, 2014.

[26] X. Wu, K. Wang, X. Wang, H. Kan, J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Processing*, vol. 148, pp. 272–287, 2018.

[27] J. Ahmad, M. A. Khan, F. Ahmed, J. S. Khan, "A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation," *Neural Computing and Applications*, vol. 30, issue 12, pp. 3847–3857, 2018.

[28] K. A. K. Patro, B. Acharya, "Secure multi – level permutation operation based multiple colour image encryption," *Journal of Information Security and Applications*, vol. 40, pp. 111–133, 2018.

[29] Z. Xiong, Y. Wu, C. Ye, X. Zhang, F. Xu, "Color image chaos encryption algorithm

combining CRC and nine palace map," *Multimedia Tools and Applications*, vol. 78, issue 22, pp. 31035-31055, 2019.
[30] M. Ahmad, M. Z. Alam, Z. Umayya, S. Khan, F. Ahmad, "An image encryption approach using particle swarm optimization and chaotic map," *International Journal of Information Technology*, vol. 10, issue 3, pp. 247–255, 2018.
[31] M. Essaid, I. Akharraz, A. Saaidi, A. Mouhib, "Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps," *Journal of Information Security and Applications*, vol. 47, pp. 173–187, 2019.
[32] E. A. Albahrani, A. A.Maryoosh, S. H. Lafta, "Block image encryption based on modified playfair and chaotic system," *Journal of Information Security and Applications*, vol. 51, pp. 102445, 2020.
[33] B. Mondal, S. Singh, P. Kumar, "A secure image encryption scheme based on cellular automata and chaotic skew tent map," *Journal of Information Security and Applications*, vol. 45, pp. 117–130, 2019.
[34] G. Hanchinamani, L. Kulakarni, "Image Encryption Based on 2-D Zaslavskii Chaotic Map and Pseudo Hadmard Transform," *International Journal of Hybrid Information Technology*, vol. 7, issue 4, pp. 185–200, 2014.
[35] R. Krishnamoorthi, P. Murali, "Chaos based image encryption with orthogonal polynomials model and bit shuffling," *Proceedings of the International Conference on Signal processing and Integrated Networks (SPIN)*, Noida, India, February 20-21, 2014, pp. 107–112.
[36] R. Krishnamoorthi, P. Murali, "A selective image encryption based on square-wave shuffling with orthogonal polynomials transformation suitable for mobile devices," *Multimedia Tools and Applications*, vol. 76, issue 1, pp. 1217–1246, 2017.
[37] B. Norouzi, S. Mirzakuchaki, S. M. Seyedzadeh, M. R. Mosavi, "A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process," *Multimedia Tools and Applications*, vol. 71, issue 3, pp. 1469–1497, 2014.
[38] K. K. Butt, G. Li, S. Khan, S. Manzoor, "Fast and Efficient Image Encryption Algorithm Based on Modular Addition and SPD," *Entropy*, vol. 22, issue 1, article no. 112, 2020.
[39] C. Pak, K. An, P. Jang, J. Kim, S. Kim, "A novel bit-level color image encryption using improved 1D chaotic map," *Multimedia Tools and Applications*, vol. 78, issue 22, pp. 31035-31055, 2019.
[40] X. Wang, S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Information Sciences*, vol. 507, pp. 16-36, 2020.
[41] H. M. Ghadirli, A. Nodehi, R. Enayatifar, "An overview of encryption algorithms in color images," *Signal Processing*, vol. 164, pp. 163-185, 2019.

***Mohammed Hussein Ahmed**, received computer Science degree and M.Sc. degree from Al-Mustansiriyah University, Baghdad, Iraq, in 2010 and 2016, respectively. He is currently an assistant lecturer at Al-Mustansiriyah University. His research interests include cryptology science, artificial intelligent systems and cryptanalysis of a classical cipher.*

***Ahmed Kareem Shibeeb**, received computer Science degree and M.Sc. degree from Al- Mustansiriyah University, Baghdad, Iraq, in 2013 and 2016, respectively. He is Currently an assistant lecturer at Middle Technical University. His research interests include multimedia security, chaos-based cryptography, and cryptanalysis of a classical cipher.*

***Fadhil Hanoon Abbood**, received computer Science degree from Al-Mustansiriyah University, Baghdad, Iraq, in 2007, and M.Sc. degree from Iraqi commission for computers and informatics, Baghdad, Iraq, in 2013. He is Currently a lecturer at Al-Mustansiriyah University. His research interests include software engineering and image security.*