Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **6**, November **2018**

Image Encryption Scheme Based on 4D4W Hyperchaotic System

Faiz Ul Islam and Guangjie Liu

School of Automation
Nanjing University of Science and Technology
Nanjing 210094, China
uet_faiz@yahoo.com; gjieliu@gmail.com

Xiangyuan Li

Wuhan Ship Communication Research Institute,
Wuhan, China
375816454@qq.com

Received January, 2018; Revised June, 2018

Abstract. *Data confidentiality is the basically important concern for everyone in the digital era. In this paper, an image encryption scheme is proposed based on the recently discovered 4D4W hyperchaotic system. Initially, the hyperchaotic system is used to generate the S-Boxes and permutation index matrices. In the first stage of image encryption, the column permutation and self-column-forward XOR are executed successively for the setting times. During the second stage, the row permutation and self-row-forward XOR are executed successively for the setting times. Pixel-by-pixel substitutions are implemented during the third stage. The proposed method is simple and easy to be implemented. Several security analyses are performed to quantify the security level and efficiency of the proposed method including key space, key sensitivity, plaintext sensitivity, histogram, information entropy, adjacent pixels correlation. The results show that the proposed scheme has a remarkable strength to resist brute-force attacks, statistical attacks, and differential attacks.*

Keywords: Image Encryption; 4D4W Hyperchaotic System; S-Box; Permutation Index Matrix

1. **Introduction.** It is the most important issue to protect the confidentiality of information in the digital world. To fulfill the security requirements, the cryptosystems based on AES, DES, and IDEA etc. are widely used. Due to the high redundancy instinct, encrypted textual information exposure and requirement of fast encryption for high-volume multimedia data, the traditional cryptosystems are commonly considered inappropriate for image encryption. Chaos-based cryptosystems have attracted plenty of attentions and play an imperative role in modern cryptography especially in image encryption due to the good analogous requirements for an ideal cryptosystem such as sensitive dependence on initial conditions and parameters, unpredictability, ergodicity, mixing property etc. for secure cryptosystems[1, 2].

Chaotic systems are divided into two main categories according to its dimension. The 1D chaotic system refers to the chaotic map with the unique variable, few parameters and easily predicted trajectories. Meanwhile, its initial conditions and system parameters are easy to be estimated[3]. These limitations are also the main reasons to prove the weakness and vulnerability of those cryptosystems based on 1D chaotic systems. For example, it was revealed that several image encryption based on 1D chaotic maps are not secure enough[4, 5]. A color image encryption method[6] based on Logistic map was analyzed and proved to be insecure[7, 8]. On the other hand, Multi-dimensional chaotic maps have more than one variables such as Lorenz system[9], Chen system[10], Qi system[11] and L$\ddot{u}$ system[12]. Multi-dimensional chaotic maps are considered to have more complex chaotic structure than that of 1D chaotic systems. The additional qualities depict that multi-dimensional chaotic system and especially hyperchaotic systems are the best options to be used for image encryption.

Fridrich[13] firstly presented the idea to make the image encryption based on chaotic maps. Consequently, many image encryption work based on chaos were reported [14, 15, 16, 17, 18, 19]. However, due to weak encryption mechanism, they left some flaws such as uneven distribution of sequences, computational time, complexity, small keys space, immunity against statistical and differential attacks. In recent years, many image encryption schemes based on chaotic maps are further studied. In [20], DNA sequence addition separation was used to scramble pixel values and the logistic maps were used for make encryption. In [21], the image encryption method was proposed based on generalized Arnold map and generalized Bernoulli shift map. In [22], the chaos-based bit-level permutation was proposed to enhance security. In [23], the image encryption method is proposed based on self-correlation function driven by some chaotic system. In [24], the authors designed the permutation-substitution network based on the coupled map lattice. Furthermore, a new permutation-diffusion scheme based on cat map for block image encryption was proposed to resist the chosen plain-text attack [25]. In [26], a dynamical state variable selection mechanism was introduced to make the encryption. In [27], an algorithm was proposed to make the pixel positions changing in both the column and row direction using chaotic magic transform based on 2D-SLMM. In [28],various schemes for image encryption were discussed in detail.

In recent years, hyperchaotic systems have been deeply investigated in many fields such as nonlinear circuits[29], lasers[30], cryptography[31, 32, 33] and secure communications[34]. As we know, a hyperchaotic system shows eminent behaviors with a high degree of sensitivity to initial conditions, randomness, strong spatiotemporal complexity and mixture due to owning more than one positive Lyapunov exponent.

In this paper, a 4D4W hyperchaotic system is used to design image encryption scheme. The hyperchaotic system is firstly used to generate the S-Boxes and permutation index matrices. Then the image encryption is implemented by the permutation and substitution using the permutation index matrices and S-Box respectively during the three stages successively. The encryption scheme sufficiently utilizes the superiority of the nonlinearity of the hyperchaotic system and exhibits remarkable cryptographical strength against several typical attacks.

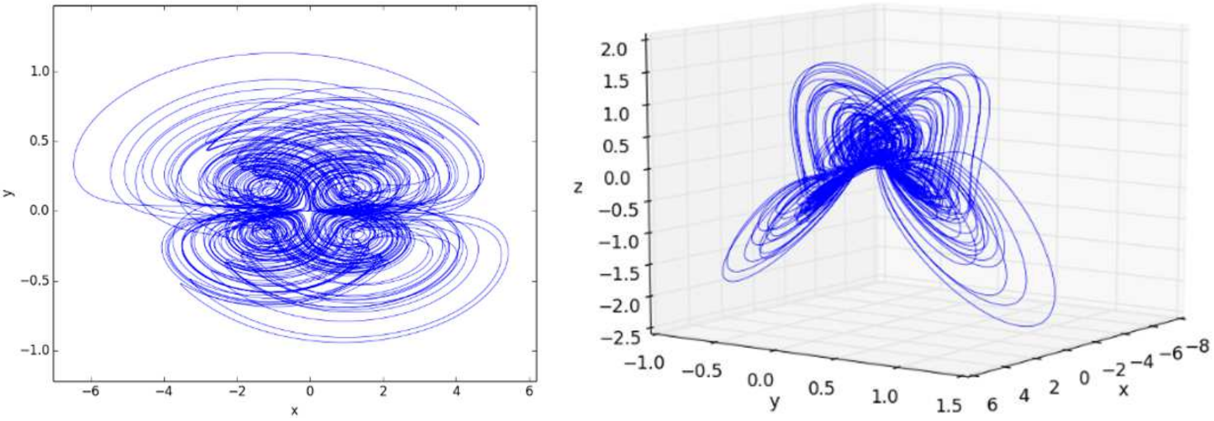
The rest of the paper is organized as follows. In Section 2, the model of a 4D4W hyperchaotic system is established. Section 3, introduces the method to generate S-Boxes and the permutation index matrices. In Section 4, the proposed image encryption algorithm is discussed in detail and the security analysis is investigated in Section 5. Finally, Section 6 concludes the paper and prospects future work.

2. Brief introduction of a 4D4W Hyper-chaotic System.

In [35], a new four-wing hyperchaotic system was developed from a 4D memristive system with four Lyapunov exponents $LE1 = 0.0905$, $LE2 = 0.0147$, $LE3 = 0.0001$ and $LE4 = -1.9862$. The system exhibits line equilibrium with richer dynamical nature than most of the known memristive systems which make the system difficult to analyze than the classical dynamical systems. The system model is defined by Eq. (1),

$$\begin{cases} \dot{x} = ax + byz \\ \dot{y} = cy + dxz - kyW(u) \\ \dot{z} = ez + fxy + gxu \\ \dot{u} = -y \end{cases} \tag{1}$$

where $a, b, c, d, e, f, g, k, m, n$ are system parameters, $W(u) = m + 3nu^2$ and k, g, m, n $(\in R^+)$. When $a = 0.35, b = -10, c = -0.6, d = 0.3, e = -1.6, f = 2, g = 0.1, m = 0.1, n = 0.01$ and $k \in (0, 2.5)$, the system exhibits the sophisticated hyperchaotic nature. The 2D and 3D projection planes are shown in Fig.1 (a) and (b) respectively.



(A)

(B)

Figure 1. Four-wing Hyper-chaotic phase portraits of system (1) with parameters $a = 0.35, b = -10, c = -0.6, d = 0.3, e = -1.6, f = 2, g = 0.1, m = 0.1, n = 0.01$ and $k = 0.2$. (A) Projection on $x - y$ plane. (B) 3-D view in the $x - y - z$ space.

3. Generating S-Boxes and permutation index matrices.

3.1. S-Box Generation.

In this paper, we just discuss the image with an 8-bit gray pixel value. The case of 24-bit RGB image with each pixel containing three 8-bit color value can be extended easily. To fulfill the substitution operation in image encryption, we suggest generating 8×8 S-Boxes which can reversibly map an integer less than 256 to the other integer. The S-Boxes generation processes are as follows.

Step 1: Set the initial values (x_0, y_0, z_0, u_0) and the parameter k of System (1).

Step 2: Set the iteration step t_0 and iterate system for N times and get two sequences $\{x_i\}$ and $\{u_i\}$.

Step 3: Use the jump selection shown as Fig. 2 to merge $\{x_i\}$ and $\{u_i\}$ to $\{s_i\}$.

Step 4: Convert$\{s_i\}$ to the integer sequence $\{F_i\}$ by mod $([s_i \times 10^4], 256)$; Let $\{V_i\}_p$ be the new vector such that $\{V_i\}_p = \{F_{10000+p\times q}\}$ with $q = 0, 1, 2, 3, ...M$ (M >300) and $p = 1, 2, ..., L$.

Step 5: Select the first 256 distinct values from vector $\{V_i\}_p$ and rearrange them into 8×8 S-Boxes.

According to the description of the S-Box generation procedure, there are totally L S-Boxes generated once. In this paper, the initial condition is set as $(x_0, y_0, z_0, u_0) =$

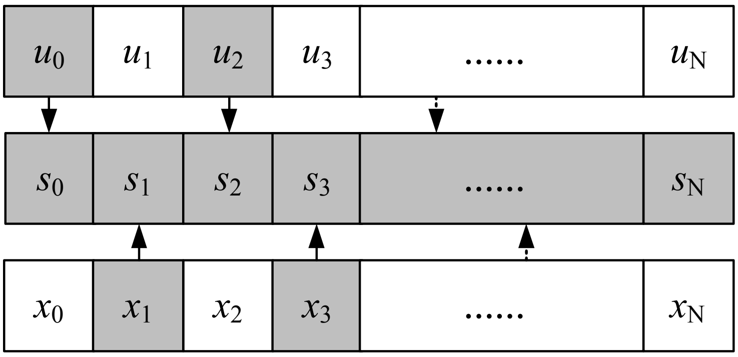


Figure 2. Illustration of Jump selection

(1, 1, 1, 1), the iteration parameters N is set to 1300000, the iteration step t_0 is set to 0.01. Let $L = 512$, there are totally 512 S-Boxes that are generated. We perform benchmarking according to five typical five criterion[33] such as strict avalanche criterion (SAC), nonlinearity, output bits independence criterion and differential uniformity.

From Fig. 3, it can be confirmed that the S-Boxes generated by the given method are all desirable. Hence, we set $p = 2$ to generate the S-Box for the following utilization.

3.2. Generating the permutation index matrix (PIM) for an $\mathbf{H \times W}$ image.

For an image with $H \times W$ pixels, the permutation of pixels is executed by the permutation index matrices PIM_c and PIM_r generated by the following steps.

Step 1-3: The same to the steps given in 3.1.

Step 4: Convert $\{s_i\}$ to the integer sequence $\{F_i\}$ by $mod([S_i \times 10^4], W)$; Let $\{V_i\}_p$ be the new vector such that $\{V_i\}_p = \{F_{10000+p\times q}\}$ with $q = 0, 1, 2, 3, ..., M$ (M>1.5W) and $p = 1, 2, ..., H$.

Step 5: Select the first W distinct values from $\{V_i\}_p$ for $p = 1, 2, ..., H$ and rearrange them row-by-row to form the $H \times W$ matrix PIM_c;

Step 6: Convert $\{s_i\}$ to the integer sequence $\{F_i\}$ by $mod([S_i \times 10^4], H)$; Let $\{V_i\}_p$ be the new vector such that $\{V_i\}_p = \{F_{10000+p\times q}\}$ with $q = 0, 1, 2, 3, ..., M$ (M>1.5H) and $p = 1, 2, ..., W$.

Step 7: Select the first H distinct values from $\{V_i\}_p$ for $p = 1, 2, ..., W$ and rearrange them column-by-column to form the $H \times W$ matrix PIM_r.

4. Image Encryption and Decryption Scheme.

The entire image encryption process is illustrated as Fig. 4. The steps are listed as follows.

Step 1: Take the initial values (x_0, y_0, z_0, u_0) and the parameter k as the key for making image encryption, and make the iteration of 4D4W hyperchaotic system.

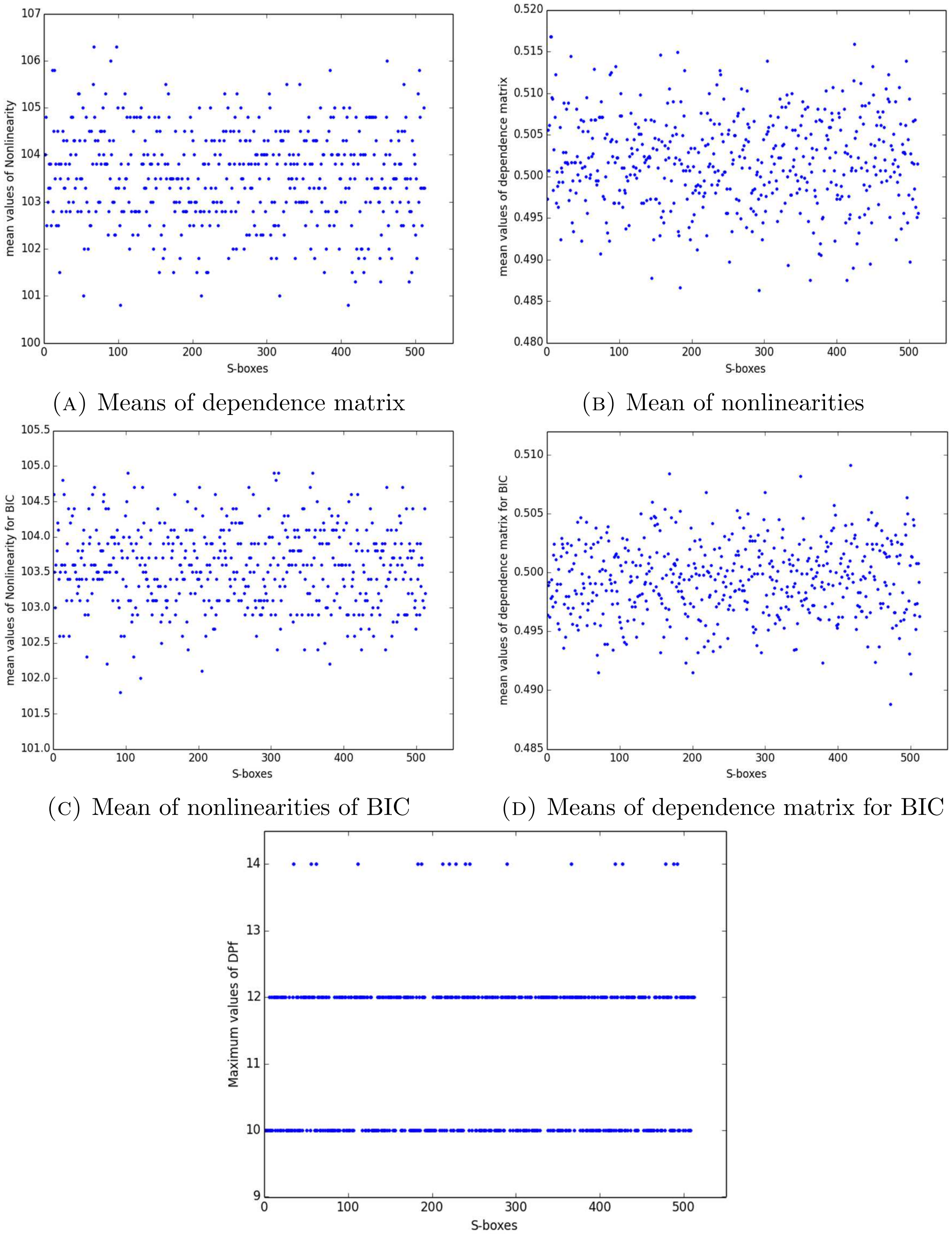
Step 2: Generate S-Box and PIM_s according to Section 3.1 and 3.2 respectively.

Step 3: Let $T(i, j) = I(i, j)$ for all pixels. Make column permutation (CP) with PIM_c following self-column-forward XOR (SCFXOR) according to Eq. (2) for $W/2$ times.

$$\begin{aligned} CP : T(i,j) \leftarrow T(i, PIM_c(i,j)).\ i = 1,2,...,H; j = 1,2,...,W \\ SCFXOR : T(i,j+1) \leftarrow T(i,j+1) \oplus T(i,j).\ i = 1,2,...,H; j = 1,2,...,W-1 \end{aligned} \tag{2}$$

We define the process as CP-SCFXOR. After Step 3, $I' = CP - SCFXOR^{w/2}(I, PIM_c)$

Step 4: Let $T(i, j) = I'(i, j)$ for all pixels. Make row permutation (RP) with PIM_r following self-row-forward XOR (SRFXOR) according to Eq. (3) for $H/2$ times.



(A) Means of dependence matrix

(B) Mean of nonlinearities

(C) Mean of nonlinearities of BIC

(D) Means of dependence matrix for BIC

(E) Maximum values of differential approximation probabilities

Figure 3. Standard cryptographic criterions of S-Boxes

$$\begin{aligned} RP &: T(i,j) \leftarrow T(PIM_r(i,j),j). \ \ i=1,2,...,H; j=1,2,...,W \\ SRFXOR &: T(i+1,j) \leftarrow T(i+1,j) \oplus T(i,j). \ \ i=1,2,...,H-1; j=1,2,...,W \end{aligned} \qquad (3)$$

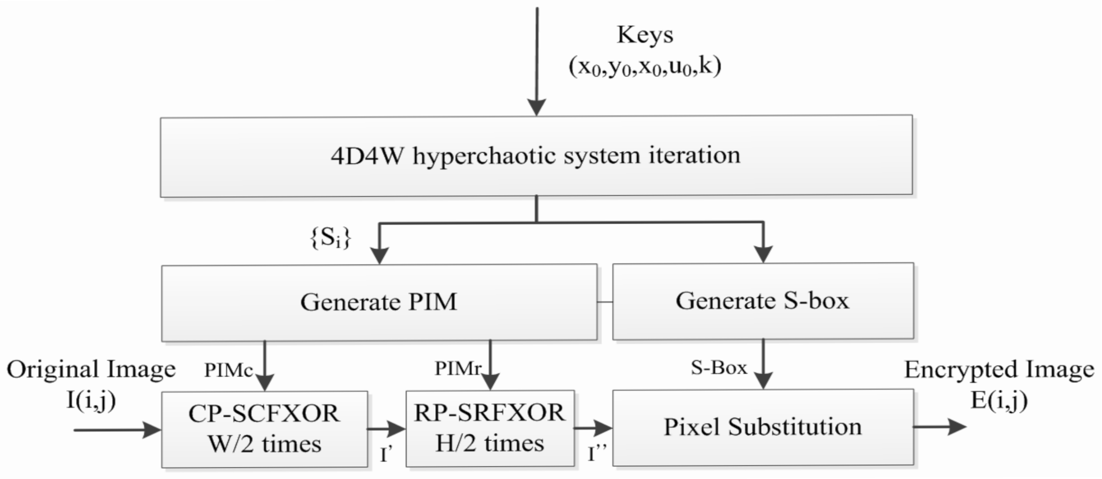


Figure 4. The image encryption process

We define the process as RP-SRFXOR. After Step 4, $I'' = RP{-}SRFXOR^{H/2}(I', PIM_r)$

Step 5: Make pixel value substitution using the function S defined by the S-Box according to Eq. (4).

$$E(i,j) = S(I''(i,j)) \tag{4}$$

According to the description of the encryption, the decryption is the reverse procedure of the above operations. For the encrypted image E, the decrypted image is obtained by $I''(i,j) = S^{-1}(E(i,j))$, $I' = SRFXOR - RP^{H/2}(I'', PIM_r^{-1})$ and $I = SCFXOR - CP^{W/2}(I', PIM_c^{-1})$ successively.

5. **Security analysis.** To evaluate the effectiveness of proposed scheme, several essential security factors are considered including key space, key sensitivity analysis, Plaintext sensitivity analysis, histogram analysis, information entropy analysis and correlation of adjacent pixels analysis.

5.1. **Key space analysis.** The key is the most important part for an attacker to break the cryptosystem easily through the brute-force attack. For secure encryption scheme, the key length should be sufficiently large to preclude eavesdropper by implementing brute-force attack. In this scheme, the initial conditions and system parameter for generation of the S-Box and the permutation index matrices can be considered as the key. The proposed algorithm comprises four initial conditions: x_0, y_0, z_0 and u_0 along with system parameter k as the key with the precision of ζ equal to 10^{14} . For any one of x_0, y_0, z_0, u_0 and k, we set the varying range be $[-0.01, 0.01]$, which mean the key space of each of x_0, y_0, z_0 and u_0 and k is 10^{12}. Hence the key achieves the acceptable limit of 10^{60} which is greater than 2^{199}. According to the computation ability of current best computers, the key space is sufficiently large to strongly resist the brute-force attack.

5.2. **Key sensitivity analysis.** Key sensitivity can be described in two aspects: **Case A.** When a tiny change in the secret key can produce a totally different cipher image from the same plain image. **Case B.** When a slightly changed key is not able to decrypt the cipher image to its original plain image. To justify both the cases, we make tiny changes at fourteenth decimal positions in the initial condition and get totally different results from original encryption scheme. For the first case, we change the initial condition value x_0 from 1 to $1 + 10^{-14}$ for generation of S-Box and z_0 from 1 to $1 + 10^{-14}$ for PIM, while all the other initial conditions, system parameters are kept unchanged. Fig. 5 shows the results under **Case A**. The different pixels between original ciphered image and ciphered image with keys changed slightly have the quote as high as 99.60%, which exhibits no any resemblance between the two ciphered images.

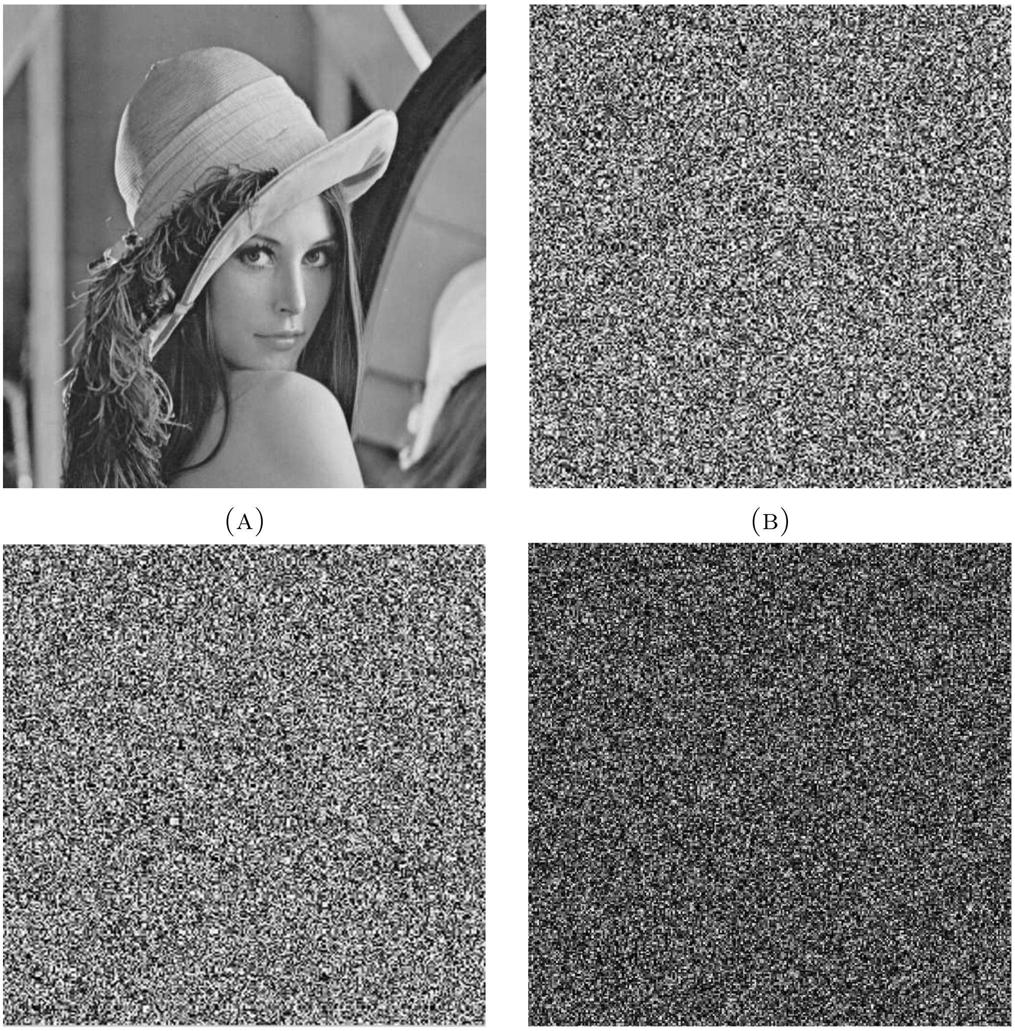

(A) (B) (C) (D)

Figure 5. Results for key sensitivity according to Case A. (A) plain image. (B) original ciphered image. (C) cipher image with keys changed slightly. (D) difference image of (B) and (C).

Fig. 6 shows the results of **Case B**. Fig. 6 (A) is decrypted by the original keys. Fig. 6 (B) is the decrypted result using the slightly changed keys, which is totally different from the plain image Lena. Both cases reflect extremely sensitive nature of the initial keys to proposed cryptosystem.

5.3. **Plaintext sensitivity analysis.** A good cryptosystem is sensitive to single pixel change in original image for resisting differential attacks. Number of pixel change rate (NPCR) and unified averaged changed intensity (UACI) are the two indices to measures the sensitivity to small change in a plain image[36]. NPCR and UACI for two encrypted images E_1 and E_2 with one pixel changed in a corresponding plain image can be defined as below.

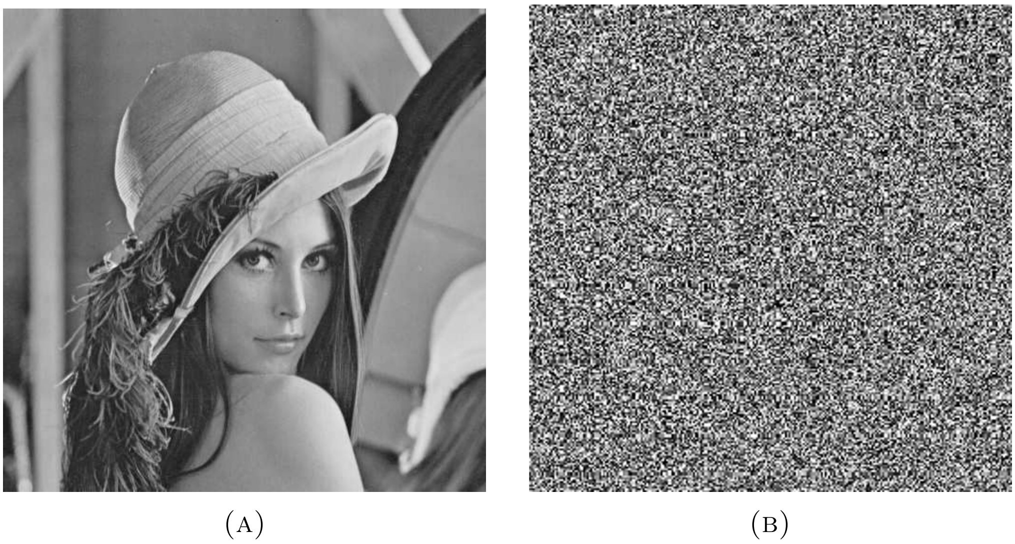


Figure 6. Results for key sensitivity according to **Case B**. (A) Deciphered image with original keys. (B) Deciphered image with slightly changed keys

$$NPCR(E_1, E_2) = \frac{1}{T}\sum\nolimits_{i,j} D(i,j) \times 100\% \tag{5}$$

$$D(i,j) = \begin{cases} 1, & if E_1(i,j) \neq E_2(i,j) \\ 0, & if E_1(i,j) = E_2(i,j) \end{cases} \tag{6}$$

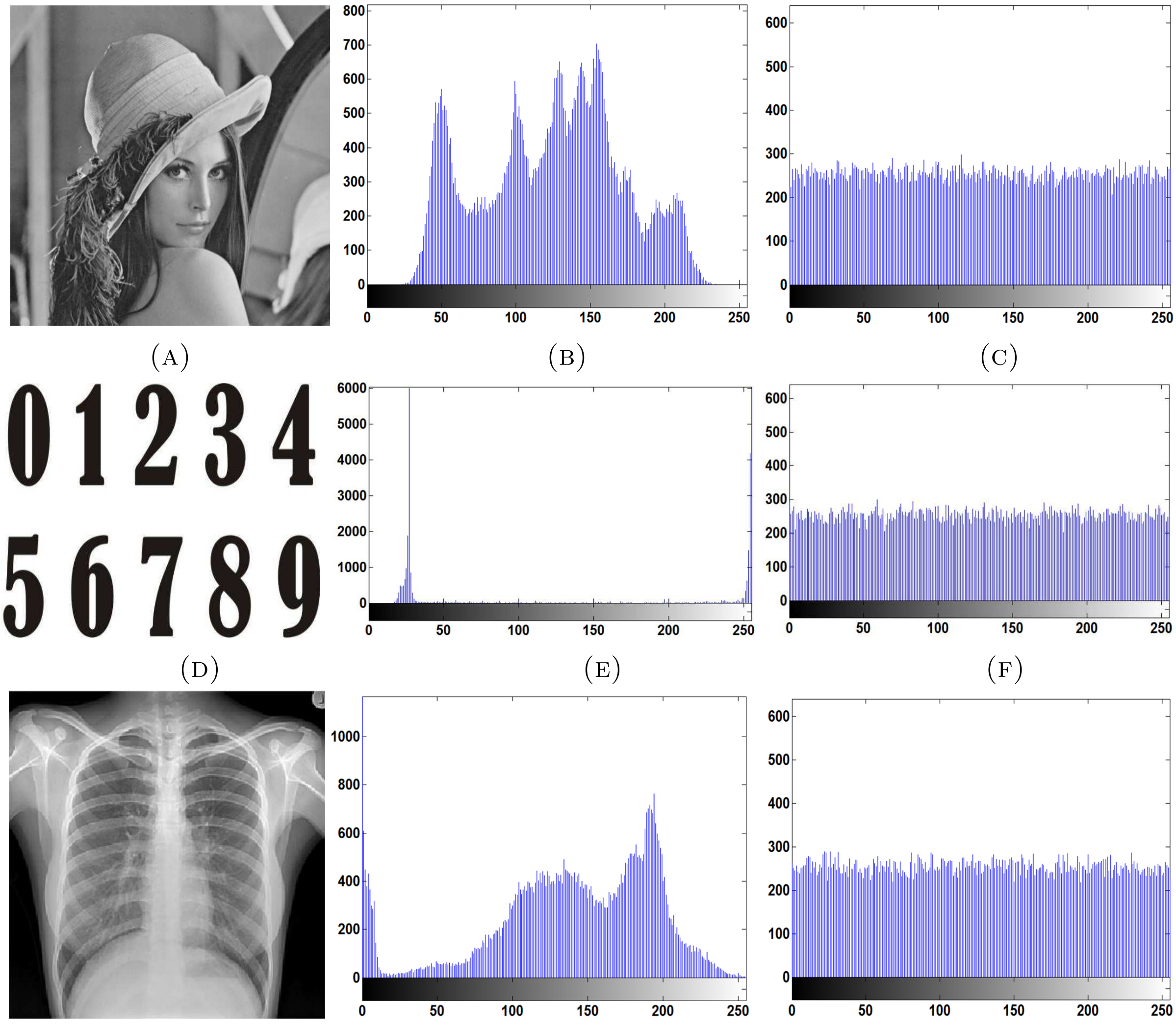
$$UACI(E_1, E_2) = \frac{1}{T}\sum\nolimits_{i,j} \frac{|E_1(i,j) - E_2(i,j)|}{255} \times 100\% \tag{7}$$

Here, the symbol T denotes the total number of pixels in the original image. We analyzed the proposed encryption scheme against differential attacks in two different ways. We use Lena, Barbara, Cameraman, Text, X-ray, Peppers, and Einstein as the plain images. For each image, there are 1000 pixels are randomly selected from a different position. The encrypted image is obtained by encrypting the image with the selected pixel being modified by flipping its least important bit. For total 7000 encrypted images, the mean value of NPCR is equal to 99.91% which is very close to the ideal value 100% and the mean value of UACI is equal to the ideal value 33.33%.

5.4. **Histogram analysis.** A good cryptosystem should be able to make the histogram of cipher image as flat as possible otherwise, it will lead to the original image information leakage. The histogram of different images and their encrypted images are presented in Fig. 7. It is evident from the visual analysis that the amounts of each pixel value are almost equal for all the encrypted images. The proposed encryption scheme is able to make the fairly uniform histogram of every type of images and difficult for an attacker to vaticinate the plain image using statistical analysis.

5.5. **Information entropy analysis.** The similarity criteria to histogram analysis is the information entropy defined as Eq. (8).

$$H(s) = -\sum_{i=1}^{n} p(s_i) \log p(s_i) \tag{8}$$



(A) (B) (C)

(D) (E) (F)

(G) (H) (I)

Figure 7. Histogram analysis of different images: (A) plain image Lena. (B) histogram of image Lena. (C) histogram of lena ciphered image. (D) text image. (E) histogram of Text image. (F) histogram of text ciphered image. (G) X-ray image. (H) histogram of X-ray image. (I) histogram of ciphered X-ray image.

Here $p(s_i)$ represents the probability of message s_i and n is the total number of s_i. In an ideal situation, when the probabilities of all the gray values are equal then the information entropy is equal to 8. The entropies are computed for different plain images and their corresponding encrypted images listed in Table 1. Moreover, the results are extremely close to ideal value 8 and compared to some recent algorithm in Table 2. It is obvious from the discussion that the probability of information leakage is negligible and proposed encryption scheme is strong against entropy attacks.

5.6. **Adjacent pixels correlation analysis.** For image encryption, it is necessary to examine the relationship of adjacent pixels to resist the statistical attacks. Plain images have high data redundancy and exhibit a strong correlation in their neighboring pixels. Mathematically, The correlation coefficient $\triangle_{xy}$ for adjacent pixel pairs, x and y are defined by Eq. (9).

Table 1. Information entropies of original images and ciphered images

	Original image	Cipher image
Lena	7.4318	7.9975
Barbara	7.5838	7.9975
Cameraman	7.0097	7.9971
Text	2.9505	7.9966
X-ray	7.2584	7.9973
Peppers	6.9837	7.9973
Einstein	6.8746	7.9967

Table 2. Information Entropies generated by different encryption schemes

	Our algorithm	[21]	[22]	[23]
Lena	7.9975	7.9970	7.9880	7.9970

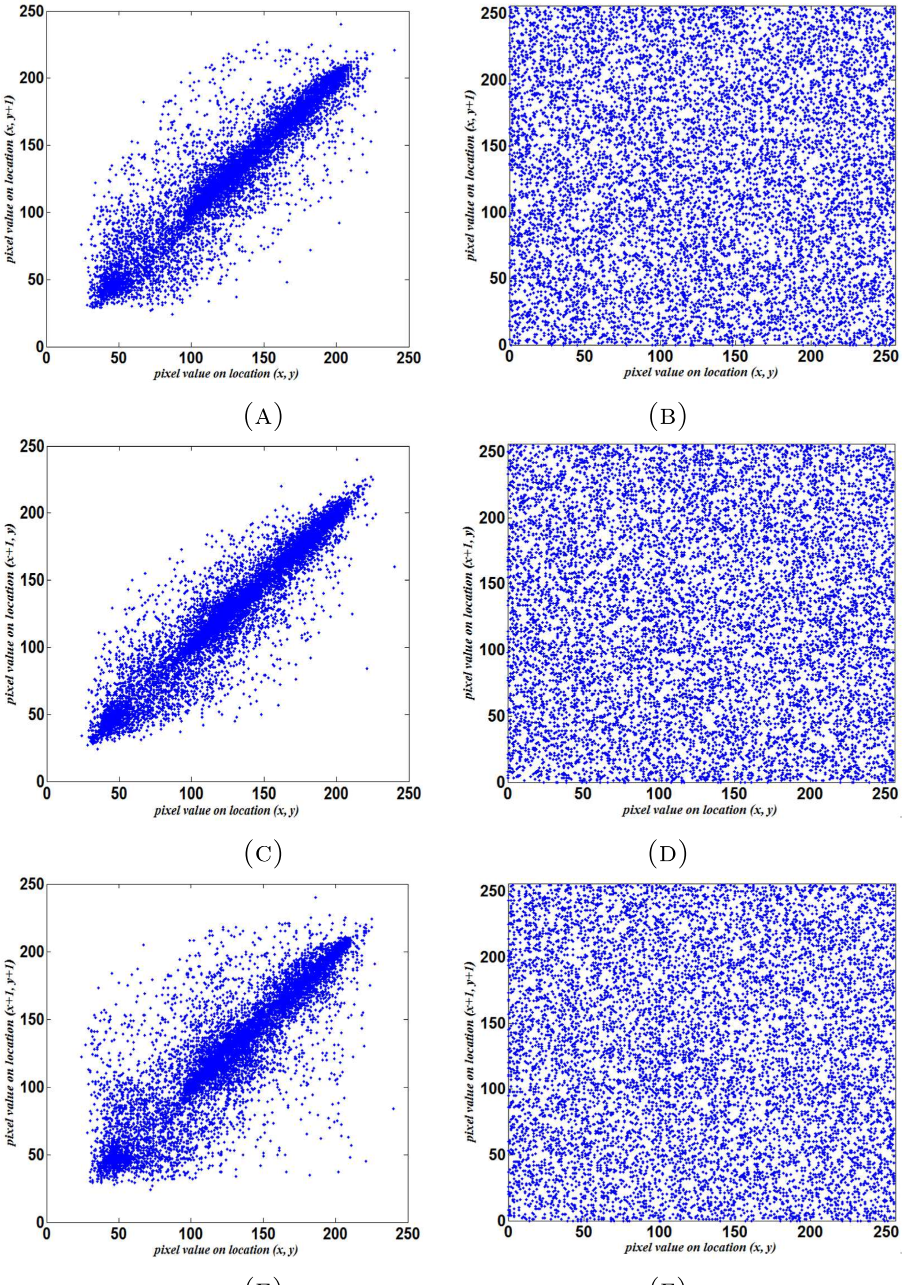
$$\triangle_{xy} = \frac{cov(x, y)}{\sqrt{D(X)D(y)}} \tag{9}$$

where $cov(x, y) = \frac{1}{K}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$, $D(x) = \frac{1}{K}\sum_{i=1}^{N}(x_i - E(x))^2$ and $D(x) = \frac{1}{K}\sum_{i=1}^{N}(y_i - E(y))^2$ with x_i, y_i being the neighboring pixel values and K being the number of total pixel pairs. Fig. 8 shows the corresponding horizontal, vertical and diagonal correlation of the image Lena and its encrypted version respectively.

The correlation of adjacent pixels for different plain images and their respective encrypted image are listed in Table 3, which indicates the encryption operation is very powerful to eliminate the adjacent pixels correlation. For comparison, Table 4 shows the remarkable superiority of the proposed scheme on adjacent pixels correlation compared with some existing schemes.

Table 3. The correlation of adjacent pixels in different images

	Original image			**Cipher image**		
Name	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9456	0.9727	0.9213	0.0002	-0.0025	-0.0040
Barbara	0.9456	0.9632	0.9254	0.0019	-0.0021	0.0022
Cameraman	0.9334	0.09592	0.9087	0.0026	0.0011	-0.0037
Text	0.9371	0.9833	0.9196	-0.0111	-0.0090	0.0015
X-ray	0.9890	0.9888	0.9819	-0.0070	0.0022	0.0036
Peppers	0.9810	0.9783	0.9630	-0.0017	0.0005	0.0053
House	0.9780	0.9652	0.9484	0.0074	0.0035	0.0018
Mandy	0.9656	0.9915	0.9607	-0.0038	0.0009	-0.0014



(A) (B)

(C) (D)

(E) (F)

Figure 8. Correlation plots of adjacent pixels in different directions. (A) horizontal correlation of Plain image. (B) horizontal correlation of encrypted image. (C) vertical correlation of Plain image. (D) vertical correlation of encrypted image. (E) diagonal correlation of Plain image . (F) diagonal correlation of encrypted image.

6. **Conclusions.** In this paper, a 4D4W hyperchaotic system with line equilibrium and richer dynamic behavior is employed to design an image encryption scheme. The proposed method is the combination of permutation and substitution of pixel positions and pixel values respectively. A decent permutation is induced by PIM based on hyperchaotic sequence. The permutation is followed by confusion (substitution) to fulfill the security requirements for robust encryption scheme. Furthermore, the detailed security analysis

Table 4. Correlation coefficient of encrypted Lena image with different encryption schemes

	Original image	Our algorithm	Ref.[20]	Ref.[27]	Ref.[28]
Horizontal	0.9456	0.0002	0.0036	0.0023	-0.0087
Vertical	0.9727	-0.0022	0.0023	-0.0086	-0.0279
Diagonal	0.9213	-0.0015	0.0039	0.0402	0.0246

are carried out such as key space analysis, key sensitivity analysis, NPCR and UACI analysis, histogram analysis, correlation of adjacent pixels analysis and information entropy analysis, which shows that the proposed image encryption scheme has the ability to resist the common attacks, including the brute-force attacks, statistical attacks, and differential attacks. Based on low computational complexity and satisfactory security measures, we conclude that the proposed image encryption scheme is applicable for practical digital encrypted image transmission using over public channels.

Acknowledgment. This work was supported by National Natural Science Foundation of China [Grant No. 61472188, 61602247, 61702235, U1636117], Natural Science Foundation of Jiangsu Province [Grant No. BK20150472, BK20160840], National Key Technology Research and Development Program of the Ministry of Science and Technology of China [Grant No. 2014BAH41B01], CCF-VENUSTECH Foundation [Grant No. 2016011], Fundamental Research Funds for the Central Universities [30920140121006, 30915012208].

REFERENCES

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

[2] G.Alvarez, and S. Li, Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos,* vol. 16, no.08, pp. 2129-2151, 2006.

[3] X. Wu, H. Hu, and B. Zhang, Parameter estimation only from the symbolic sequences generated by chaos system. *Journal of Chaos, Solitons & Fractals,* vol.22, no.2, pp. 359-366, 2004.

[4] D. Arroyo, R. Rhouma, G.Alvarez,, Li, S., and Fernandez, V. , On the security of a new image encryption scheme based on chaotic map lattices. *Journal of Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol.18, no.3, pp. 033112, 2008.

[5] A. Skrobek, , Cryptanalysis of chaotic stream cipher.*Journal of Physics Letters A,* vol.363, no.1, pp. 84-90, 2007.

[6] X. Wang, L. Teng, and X. Qin, A novel colour image encryption algorithm based on chaos. *Journal of Signal Processing,* vol.92, no.4, pp. 1101-1108, 2012.

[7] C. Li, L. Zhang, Y. Ou, R., Wong, K. W., and Shu, S, Breaking a novel colour image encryption algorithm based on chaos. *Journal of Nonlinear Dynamics*, vol.70, no.4, pp. 2383-2388, 2012.

[8] D. Arroyo, J. Diaz, and F.B. Rodriguez, Cryptanalysis of a one round chaos-based Substitution Permutation Network. *Journal of Signal Processing,* vol.93, no.5, pp. 1358-1364, 2013.

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

[10] G. Chen, and T. Ueta, Yet another chaotic attractor. International Journal of Bifurcation and Chaos, vol.9, no.07, pp. 1465-1466, 1999.

[11] G. Qi, G. Chen, , Du, S., Chen, Z., and Yuan, Z., Analysis of a new chaotic system. *Physica A: Statistical Mechanics and its Applications,* vol.352, no.2-4, pp. 295-308, 2005.

[12] J. L, and G. Chen, A new chaotic attractor coined. International Journal of Bifurcation and Chaos, vol.12, no.03, pp. 659-661, 2002.

[13] J. Fridrich, , Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos*, vol.8, no.06, pp. 1259-1284, 1998.

[14] L. Zhang, X. Liao, and X. Wang, An image encryption approach based on chaotic maps. Chaos, *Solitons & Fractals,* vol.24, no.3, pp. 759-765, 2005.

[15] H. Gao, Y. Zhang, Liang, S., and Li, D., A new chaotic algorithm for image encryption. *Chaos, Solitons & Fractals*, vol.29, no.2, pp. 393-399, 2006.

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

[17] S. Behnia, A. Akhshani,H. Mahmodi, and A. Akhavan, A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos, Solitons & Fractals*, vol.35, no.2, pp. 408-419, 2008.

[18] F. Sun, S. Liu, , Li, Z. and *Lü*, Z, A novel image encryption scheme based on spatial chaos map. *Chaos, Solitons & Fractals*, vol.38, no.3, pp. 631-640, 2008.

[19] Y. Wang, K. W. Wong, X. Liao, and G. Chen, A new chaos-based fast image encryption algorithm. *Applied soft computing*, vol.11, no.1, pp. 514-522, 2011.

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

[21] Ye, R., A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism. Optics Communications, vol.284, no.22, pp. 5290-5298, 2011.

[22] C. Fu, B. B. Lin, Y.S. Miao, X. Liu, and J. J. Chen, , A novel chaos-based bit-level permutation scheme for digital image encryption. *Optics Communications*, vol.284, no.23, pp. 5415-5423, 2011.

[23] Zhao, L., Adhikari, A., Xiao, D. and Sakurai, K., On the security analysis of an image scrambling encryption of pixel bit and its improved scheme based on self-correlation encryption. *Communications in Nonlinear Science and Numerical Simulation*, vol.17, no.8, pp. 3303-3327, 2012.

[24] Liu, Q., Li, P.Y., Zhang, M.C., Sui, Y.X. and Yang, H.J., A novel image encryption algorithm based on chaos maps with Markov properties. *Communications in Nonlinear Science and Numerical Simulation,* vol.20, no.2, pp. 506-515, 2015.

[25] Wang, X., L. Liu, and Y. Zhang, A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Optics and Lasers in Engineering*, vol.66, pp. 10-18, 2015.

[26] Chen, J.X., Zhu, Z.L., Fu, C., Yu, H. and Zhang, L.B., A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Communications in Nonlinear Science and Numerical Simulation, vol.20, no.3, pp. 846-860, 2015.

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

[28] Wang, B., Xie, Y., Zhou, C., Zhou, S. and Zheng, X., Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps. *Optik-International Journal for Light and Electron Optics*, vol.127, no.7, pp. 3541-3545, 2016.

[29] Cafagna, D. and G. Grassi, New 3D-scroll attractors in hyperchaotic Chua's circuits forming a ring. International Journal of Bifurcation and Chaos, vol.13, no.10, pp. 2889-2903, 2003.

[30] Vicente, R., Daudn, J., Colet, P. and Toral, R., . Analysis and characterization of the hyperchaos generated by a semiconductor laser subject to a delayed feedback loop. *IEEE Journal of Quantum Electronics*, vol.41, no.4, pp.541-548, 2005

[31] Gondal, M.A., A. Raheem, and I. Hussain, A Scheme for Obtaining Secure S-Boxes Based on Chaotic Bakers Map. *3D Research*, vol.5, no.3, pp. 1-8, 2014.

[32] Hussain, I., M.A. Gondal, and A. Hussain, Construction of Dynamical Non-linear Components Based on Lorenz System and Symmetric Group of Permutations. *3D Research*, vol.6, no.1, pp. 1-6, 2015.

[33] Liu, G., Yang, W., Liu, W. and Dai, Y., Designing S-boxes based on 3-D four-wing autonomous chaotic system. Nonlinear Dynamics, vol.82, no.4, pp. 1867-1877, 2015.

[34] V.S. Udaltsov,J.P. Goedgebuer, L. Larger, Cuenot, J.B., Levy, P. and Rhodes, W.T., Communicating with hyperchaos: the dynamics of a DNLF emitter and recovery of transmitted information. *Optics and Spectroscopy*, vol.95, no.1, pp. 114-118, 2003.

[35] J. Ma, Z. Chen, Wang, Z. and Zhang, Q., A four-wing hyper-chaotic attractor generated from a 4-D memristive system with a line equilibrium. *Nonlinear Dynamics,* vol.81, no.3, pp. 1275-1288, 2015.

[36] Y. Wu, J.P. Noonan, and S. Agaian, NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology, *Journal of Selected Areas in Telecommunications (JSAT)*, pp. 31-38, 2011