DOI:10.24996/ijs.2018.59.4B.17

ISSN: 0067-2904

A new Color image Encryption based on multi Chaotic Maps

Ibtisam A.Taqi*, Sarab M. Hameed
Department of Computer Science, College of Science, University of Baghdad, Baghdad, Iraq

Abstract

This paper presents a new RGB image encryption scheme using multi chaotic maps. Encrypting an image is performed via chaotic maps to confirm the properties of secure cipher namely confusion and diffusion are satisfied. Also, the key sequence for encrypting an image is generated using a combination of 1D logistic and Sine chaotic maps. Experimental results and the compassion results indicate that the suggested scheme provides high security against several types of attack, large secret keyspace and highly sensitive.

Keywords: Chen-hyper chaotic system, image encryption, Logistic map, Sine map.

طريقة جديدة لتشفير الصور الملونة باستخدام خرائط فوضوية متعددة

ابتسام عبدالله تقي* ، سراب مجيد حميد
قسم علوم الحاسوب، كلية العلوم، جامعة بغداد، بغداد، العراق

الخلاصة

يقدم هذا البحث طريقة جديدًا لتشفير الصور الملونة RGB باستخدام خرائط فوضوية متعددة. يتم تنفيذ تشفير صورة من خلال خرائط فوضوية لتأكيد خصائص التشفير الآمن ، وهي مطابقة للارتباك والانتشار. أيضا ، يتم إنشاء تسلسل مفتاح لتشفير صورة باستخدام مجموعة من 1D اللوجستية وخرائط الفوضى Sine. تشير النتائج التجريبية إلى أن الطريقة المقترحة توفر أمانًا عاليًا ضد عدة أنواع من الهجوم ، وتوفرمساحة مفتاح سرية كبيرة وحساسة للغاية.

1. Introduction

With the fast development of network technology, the communications have been greatly changed. Transmission for multimedia content over Internet has become more and more frequently. However, the digital image security has a severe threat in the transmission due to the openness and sharing of networks. Therefore, people became further attention on security and confidentiality of multimedia information.

Among various protecting methods, image encryption technique is one of the most efficient and common methods for image information protection. Because of the particular storage format of an image, the traditional block cipher algorithms, such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES) are not particularly proper for encryption an image. Presently, numerous methods are proposed for image encryption that tries for reducing image content's redundancy using the chaos-based ciphers. The chaos system holds a number of characteristics including high sensitivity to initial conditions, determinacy, and ergodicity. Chaotic sequences produced by chaotic maps are often pseudo-random sequences, and their structures are very complex and challenging to be analyzed [1].

*Email: iat812000@yahoo.com

Several image encryption algorithms have been proposed using chaotic maps. Wu et al. [2] in 2012 proposed an image encryption method using two- dimensional logistic chaotic maps and permutation-substitution network structure. The result showed that the proposed method could produce a random cipher image and withstand several attacks including the statistical attacks and the differential attacks. Xiaoling Huang in 2012 [3] proposed an image encryption algorithm using Chebyshev chaotic to generate the keystream. Testing the performance of the proposed algorithm showed that the key space was large and its sensitivity to initial settings. Zhou et al. in 2015 [4] proposed an image encryption algorithm via skew tent map and line map for shuffling. The proposed algorithm was implemented in parallel to obtain high performance regarding speed. The results illustrated that the robustness of the proposed algorithm against chosen plaintext attack. Kumar et al. in 2015 [5] proposed a new algorithm that used a compound of chaotic maps with diffusion for image encryption. The results illustrated that the proposed algorithm was proper for image encryption with high security. Niyat et al. in 2015 [6] suggested an encryption algorithm for RGB image using DNA sequence operation and chaotic maps namely Chen hyper-chaotic system for image shuffling, 1D logistic and Sine maps for key generation. The results confirmed the capability of the algorithm to counter several attacks. Jha et al. in 2016 [7] introduced image encryption algorithm using double encryption, the first one with a 2D logistic map and the second one AES. The results of the algorithm showed it's could withstand differential attacks. Lingfeng Liu and Suoxia Miao in 2016 [8] proposed an image encryption algorithm via logistic chaotic map using a varying parameter that was used for shuffling an image. After that, a dynamical algorithm was employed for encrypting the image. The results clarified that the algorithm provided high security and competitive with several image encryption algorithms. Wang et al. in 2016 [9] proposed an encryption scheme for color image using 1D and 2D logistic map for generating a chaotic matrix. Then, the two chaotic maps are repeated one after the other for permuting the matrix. The experimental results proved the security and suitability of the scheme for image encryption. Rim Zahmoul and Mourad Zaied in 2016 [10] produced new chaotic maps based on beta function were created. The generation of different pseudo-random sequence was carried out to shuffle the position of the image pixels and to confuse the relationship between the encrypted image and the original image, thereby significantly increasing the resistance to attacks. The proposed system has a large keyspace and high sensitivity Chanil Pak and Lilian Huang in 2017 [11] proposed a method of making a simple and effective chaotic system by using a difference of the output sequences of two same existing one-dimension (1D) chaotic maps. Simulations and performance evaluation showed that the proposed system is able to produce a one-dimension chaotic system with better chaotic performance and larger chaotic ranges compared with the previous chaotic maps. Secondly, proposed an encryption algorithm of linear-nonlinear-linear structure based on complete shuffling to confirm its applications in image encryption. Experiments and security analysis proved that the algorithm has a distinguished ability to counter various attack. Rostami et al. in 2017 [12] proposed a parallel image encryption algorithm by chaotic windows based on the 1D logistic map. The image was divided into 16 ×16 blocks. Then, the XOR operation between a chaotic window and these blocks was performed to produce an encrypted image. The results showed that the algorithm was able to withstand the statistical attacks, brute force attack, differential attack, chosen-plaintext and chosen-ciphertext attacks. Zahmoul et al. in 2017 [13] proposed a Beta chaotic map that generates chaotic sequences for encryption. The image pixels position was shuffled with different pseudo-random sequences to obscure the correlation between the cipher and the original images. The proposed algorithm was capable of thwarting many attacks. Niyat et al. in 2017 [14] used hyper-chaotic system and cellular automata for color image encryption. The results observed that the encrypted image produced a uniform histogram and small correlation between pixels and large key space. Furthermore, the algorithm could withstand different attacks including differential attacks, statistical analysis, comprehensive attacks, and data lost attack and noise with different intensity. Thajeel et al. in 2018 [15] suggested an image encryption method using different chaotic maps. First, the duffing map was used to shuffle image pixels. Then, cross chaotic map to shuffle the image. In addition, a key sequences was generated using Quadratic number spirals. The results confirmed that the method provided large key space and countered many security attacks such as statistical attack, differential attack and entropy attack. Gan et al. in 2018 [16] introduced a new chaos-based image encryption algorithm for color images based on three-dimensional bit-plane permutation. In the proposed algorithm, the color plain image is first converted to 24-bit by RGB splitting and bit plane decomposition, next three-dimensional bit-plane permutation is performed on bit planes, position sequences for permutation are obtained from the 3D Chen chaotic system, and then the three confused components are acquired. The color cipher image is obtained by diffusing the confused components using key matrices generated by a 1D chaotic system and a multilevel discretization method. Simulation results and security analyses demonstrate that the algorithm not only has a good encryption effect but can also resist against common attacks, so it is reliable to be applied for image secure communications.

This paper is structured as follows: Section 2 gives a brief description of the adopted chaotic maps in this paper. In section 3, the proposed RGB image encryption method will be described in details. Section 4 clarifies the evaluation of the results concerning of security analysis of the image. Section 5 provides a conclusion of the proposed work.

2. Chaotic Maps

Chaos theory focuses on describing the behavior of a nonlinear dynamic system, which sensitivity to initial conditions is high. In this paper, three different chaotic maps including 1D Logistic, Sine and Chen hyper are utilized.

The 1D Logistic map is a simple and the most common used map that is described in Equation (1) [6]

$$x_{n+1} = r\,x_n\,(1 - x_n) \tag{1}$$

The Sine map is described in Equation (5) [6]:

$$y_{n+1} = rSin(\pi\, y_n) \tag{2}$$

Where

$r \in (0,4], y_n \in (0,1), n = 0,1,2,\ldots$

The Chen hyper-chaotic map is one of the hyper chaotic functions that have large space keys and is described as below [6]

$$\left.\begin{aligned} x &= a(y - x) \\ y &= -xz + dx + cy + q \\ z &= xy - bz \\ q &= x + k \end{aligned}\right\} \tag{3}$$

Where

$a, b, c, d, and\ \ k$ are parameters of the map.

3. The proposed Image Encryption and Decryption Scheme

This section is dedicated to explain the proposed image encryption scheme in detail as depicted in Figure-1.

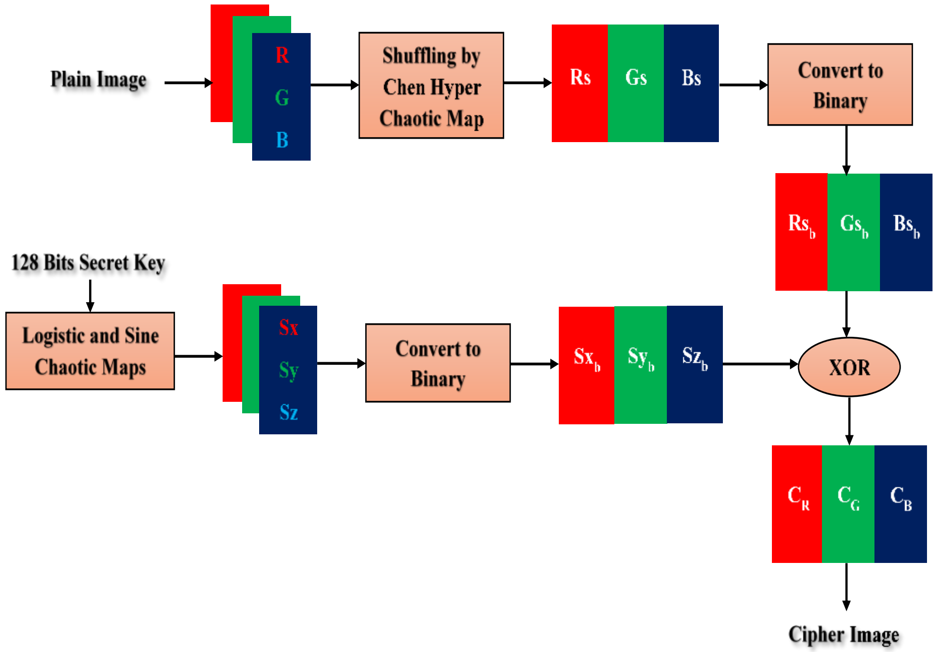

Figure 1-The proposed Image Encryption Scheme General Layout

3.1 key sequence Generation

One of the essential components of the proposed method is generating a key sequence for encrypting an image. A key sequence is generated by using 1D Logistic map in Equation 1, Sine chaotic map in Equation 2 and a new chaotic map that combines 1D Logistic and sine chaotic maps as formulated in 4

$$z_n = (x_{\mathrm{n}} + y_{\mathrm{n}}) \; mod \; 1 \qquad (4)$$

The initial value for 1D Logistic and Sine chaotic maps are obtained from a secret key $K = \{k_1, k_2, \ldots k_{112}\}$ of size 112-bit where k_i represents a 4-bit hexadecimal digit . $k_1, k_2, \ldots k_{28}$ are used to generate the control parameters x_0 and r of the 1D Logistic map and y_0 and r of Sine map as formulated in Equations 5, 6 and 7 respectively.

$$x_0 = \frac{k_1 k_2 \ldots k_6}{2^8} \; mod \; 1 \qquad (5)$$

$$r = 3.9 + \frac{(x_1 + x_2) \; mod 1}{10} \qquad (6)$$

$$y_0 = (x_0 + x_1 + x_2) \; mod \; 1 \qquad (7)$$

Where

$$x_1 = \frac{k_7 k_8 \ldots k_{12}}{2^8} \; mod \; 1 \qquad (8)$$

$$x_2 = \frac{k_{13} k_{14} .. k_{28}}{2^{16}} \; mod \; 1 \qquad (9)$$

To generate a key sequence to encrypt an image I of size $M \times N$. First, three chaotic sequences $S_x = \{x_1, x_2, \ldots x_{M \times N}\}, S_y = \{y_1, y_2, \ldots y_{M \times N}\}$ and $S_z = \{z_1, z_2, \ldots z_{M \times N}\}$ of length $M \times N$ are generated according to Equations 10, 11 and 12 respectively.

$$x_i = \lfloor (|x_i| \times 10^{14}) \; mod \; 256 \rfloor \qquad (10)$$

$$y_i = \lfloor (|y_i| \times 10^{14}) \; mod \; 256 \rfloor \qquad (11)$$

$$z_i = \lfloor (|z_i| \times 10^{14}) \; mod \; 256) \rfloor \qquad (12)$$

Then, the three generated sequences S_x ,S_y and S_z are transformed into the binary representation**.**

2.2. Image Encryption

Diffusion and confusion property should be satisfied to obtain a secure image encryption by following steps:

Step1: The plain image I is disintegrated into three $R = \{r_1, r_2, \ldots r_{M \times N}\}$ $G = \{g_1, g_2, \ldots g_{M \times N}\}$, and $B = \{b_1, b_2, \ldots b_{M \times N}\}$ components.

Where

r_i, g_i and b_i are the i^{th} pixel values for red, green and blue components.

Step2: Shuffle the pixel of image I using Chen hyper-chaotic map as in [1] that uses four-order Rung–Kutta method to get sequences. To shuffle each pixel of an image, the decimal part of x, y, z, q is reversed and the integer part is excluded.

$$[x_{ind}, x'] = sort(x)$$
$$[y_{ind}, y'] = sort(y)$$
$$[z_{ind}, z'] = sort(z)$$
$$[q_{ind}, q'] = sort(q)$$

Where

$x', y', z' and \; q'$ is the ascending x, y, z, and q respectively and x_{ind} ,y_{ind}, z_{ind}, and q_{ind} are the indices value of $x', y', z' and \; q'$ respectively.

$$\forall i, 1 \le i \le M \; and \; \forall j, 1 \le j \le N$$
$$R_s(i,j) = \mathrm{R}(x_{ind}(i), y_{ind}(j))$$
$$G_s(i,j) = \mathrm{G}(x_{ind}(i), z_{ind}(j))$$
$$B_s(i,j) = B(z_{ind}(i), q_{ind}(j))$$

Step3: Convert the $R_s \, (M,N), G_s \, (M,N)$ and $B_s \, (M,N)$ matrices from decimal form into binary matrices $Rs_b \, (M, N \times 8)$, $Gs_b(M, N \times 8)$ and $Bs_b(M, N \times 8)$

Step4: Confuse an image by making the pixel value sensitive to the key. The XOR operation between the generated sequences Sx_b, Sy_b and Sz_b and Rs_b, Gs_b and Bs_b are applied. After that, the obtained results are converted to decimal representation to produce an encrypted image C as shown below.

$$C_R = Rs_b \oplus Sx_b$$

$C_G = Gs_b \oplus Sy_b$
$C_B = Bs_b \oplus Sz_b$

2.3. Image Decryption

Image decryption process is similar to the encryption process, but the steps are taken by the reverse order as in follows.

Step1: The cipher image C is transformed into three $C_R = \{r_1, r_2, \dots r_{M\times N}\}$ $C_G = \{g_1, g_2, \dots g_{M\times N}\}$, and $C_B = \{b_1, b_2, \dots b_{M\times N}\}$ components

Step2: Convert the three matrices C_R, C_G and C_B to binary representation $CR_b, CG_b\ and\ CB_b$.

Step3: Perform ordinary XOR operation between CR_b**,** $CG_b\ and\ CB_b$ and the corresponding $Sx_b,\ Sy_b, Sz_b$ to obtain the shuffling matrices Rs_b, Gs_b and Bs_b as follows:

$Rs_b = CR_b \oplus Sx_b$
$Gs_b = CG_b \oplus Sy_b$
$Bs_b = CB_b \oplus Sz_b$

Step4: Covert the Rs_b, Gs_b and Bs_b matrices to decimal and perform inverse permutation for R_s , G_s and B_s to get the matrices R, G and B as follows:

$\forall i, 1 \le i \le M\ and\ \forall j, 1 \le j \le N\ and$
$R(x_{ind}(i), y_{ind}(j)) = R_s(i,j)$
$G(x_{ind}(i), z_{ind}(j)) = G_s(i,j)$
$B(z_{ind}(i), q_{ind}(j)) = B_s(i,j)$

Step4: Combine R, G, and B to get the plain image I.

3. Experimental Results

The proposed encryption and decryption scheme is coded in C# and the experiments are conducted on a *Lenovo Laptop* with Intel(R) Core (TM) i7-5500U, CPU @ 2.40GHz 2.40GHz and a Memory of 16.0 GB RAM and 64-bit system type. The performance of the proposed method is evaluated using three different images with two different sizes drawn from image dataset of Signal and Image Processing Institute (SIPI) [17]. The resulting analysis is depended on Mean Square Error (MSE) and Peak Signal-To-Noise Ratio (PSNR, Peak Signal to Noise Ratio (PSNR), Entropy, Correlation coefficient (CC) visual evaluation of histogram, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI).

The setting parameters of Chen hyper-chaotic map for all experiments are $a = 36, b = 3, c = 28, d = 16, x_0 = 0.3,\ y_0 = -0.4, z_0 = 1.2, q_0 = 1, and\ k = 0.2$

4.1 MSE and PSNR Results

The MSE is a quantitative measure that clarifies the distinction between plain image and cipher image as in Equation 13 [13].

$$MSE = \frac{1}{MN}\sum_{i=0,j=0}^{M,N}(P(i,j) - C(i,j))^2 \qquad (13)$$

Where

$P(i,j)$ is plain image pixel value, $C\ (i,j)$ is cipher image pixel value, M and N are the dimensions of the image.

The mathematical representation of the PSNR is as in Equation 14 [5]

$$PSNR = 20\ \log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \qquad (14)$$

The MSE value and $PSNR$ value of encrypted images and decrypted images using the proposed scheme are reported in Tables-(1 and 2). The results point out that MSE value between the cipher image and the plain image is large. Also, the results show that $PSNR$ values between the original and encrypted images using the proposed method are small compared with [15].

Table 1-MSE of the proposed scheme

		MSE			
Image Size	**Image Name**	**Image Component**			
		Red	**Green**	**Blue**	**Average**
512	**Lena**	10619.2144	9080.0907	7125.1720	8941.4924
	Baboon	8623.9103	7734.5994	9483.8955	8614.1351
	Pepper	7980.2737	11219.3951	11196.1918	10131.9535
256	**Baboon**	8598.8581	7805.6071	9544.5583	8649.6745
	Pepper	8034.7531	11239.0409	11230.6001	10168.1314

Table 2-PNSR of the proposed scheme

PSNR

Image Size	**Method**	**Image Name**	**Image Component**			
			Red	**Green**	**Blue**	**Average**
512	**Proposed scheme**	**Lena**	7.8645	8.5545	9.6065	8.6752
		Baboon	8.7698	9.2403	8.3617	8.7906
		Pepper	9.1066	7.6464	7.6434	8.1321
	[15]	**Lena**	-	-	-	9.7896
		Baboon	-	-	-	8.6000
		Pepper	-	-	-	8.9800
256	**Proposed scheme**	**Baboon**	8.7803	9.2004	8.3216	8.7674
		Pepper	9.1236	7.6042	7.6731	8.1336

4.2 Key Space Analysis

The ability to counter brute-force attack is determined by the keyspace. A brute-force attack is a method of breaking the cryptographic scheme by examining all possible keys. Brute-force attacks are very expensive from a resource and time aspect since the attacker exploits the vulnerabilities in the encryption by using the advantage of key length and simplicity of the key. The key space size for the proposed scheme is 2^{112} . The parameter x , y and r of 1D logistic and sine maps are considered as a secret key. x, y and z of chaotic sequences with the precision 10^{-14}. Therefore, the key space is $10^{14} \times 10^{14} \times 10^{14} = 10^{42} \approx 2^{140} \times 2^{24} \times 2^{112} = 2^{276}$ that appears to be sufficient to counter brute force attacks.

4.3 Statistical Attack

In a statistical attack, the attacker utilizes statistical weaknesses in a cryptographic scheme to identify data that is confidential. The ability of the proposed scheme to resist statistical attack is described by entropy, histogram analysis, and correlation coefficient. Information entropy (H) measures the randomness of an image as expressed in Equation 15.

$$H(m) = -\sum_{i=0}^{L} p(m_i) log_2 p(m_i) \qquad (15)$$

Where

$L = 255$, m_i is i^{th} pixel value of an image, and $p(m_i)$ is m_i probability.

The entropy of the cipher image using the proposed scheme is closer to 8 and slightly larger than the schemes in [6], [14] and [15] as reported in Table-3. This means the randomness of the cipher image is very high, the probability of deducing any information is too insignificant and the proposed scheme was able to resist the statistical attack more than the work in [6], [14] and [15].

Table 3-The entropy of cipher images of the proposed scheme against [6], [14] and [15]

Entropy

Method	**Image Size**	**Image Name**	**Image Component**			
			Red	**Green**	**Blue**	**Average**
Proposed scheme	**512**	**Lena**	7.9994	7.9993	7.9993	7.9993
		Baboon	7.9992	7.9993	7.9994	7.9993
		Pepper	7.9993	7.9994	7.9993	7.9993
	256	**Baboon**	7.9974	7.9972	7.9975	7.9974
		Pepper	7.9975	7.9976	7.9978	7.9976
[6]	**256**	**Baboon**	7.9973	7.9968	7.9976	7.9972
[14]	**256**	**Baboon**	7.9972	7.9972	7.9972	7.9972
		Pepper	7.9971	7.9975	7.9974	7.9973
[15]	**512**	**Lena**	-	-	-	7.9992
		Baboon	-	-	-	7.9992
		Pepper	-	-	-	7.9991

Regarding visual histogram analysis as depicted in Figure-2, it is clear that the histogram of red, green and blue components of cipher images are uniformly distributed and do not provide any information. This means the proposed scheme provides a good encryption because any information cannot be acquired from the cipher images.

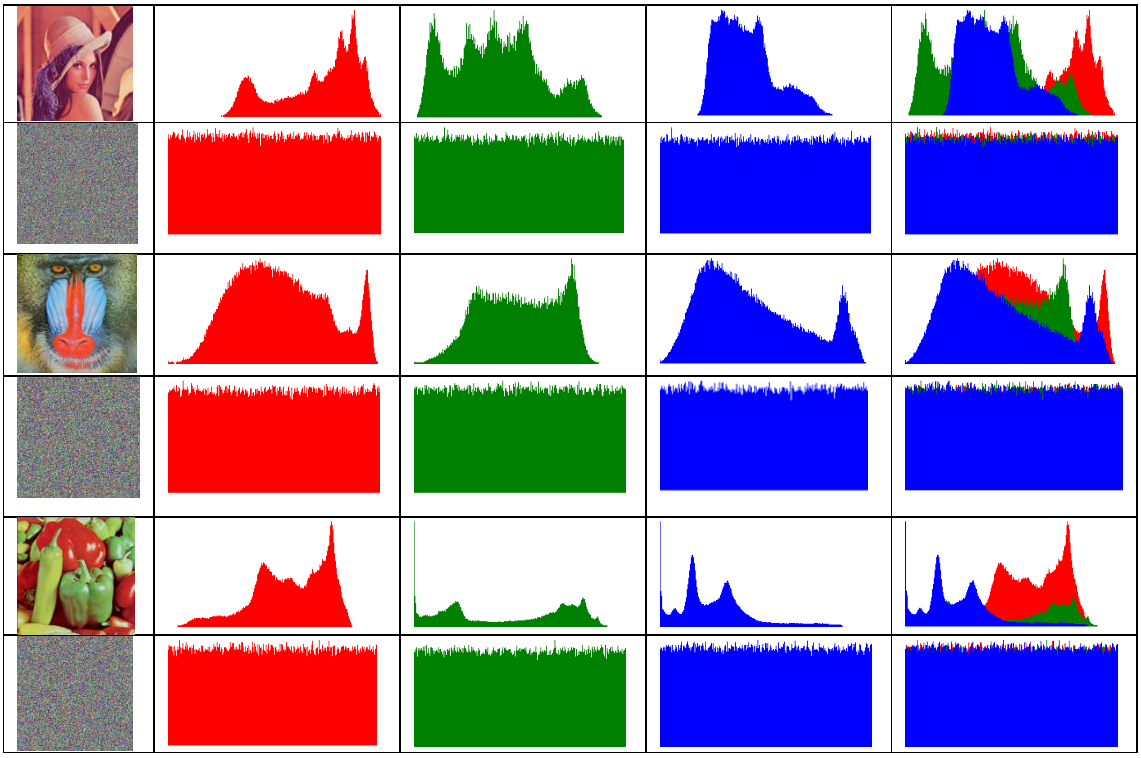

Figure 2-Red, green and blue components histograms of plain images of Lena, Baboon and pepper and their corresponding cipher images

Correlation coefficient measures the correlation of adjacent pixels in an image as in Equation 16 [14]:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \qquad (16)$$

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

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

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x_i)\right)\left(y_i - E(y_i)\right)$$

Where

x and y are two neighboring pixels values in the image,

$D(x)$ is the variance,and N is the number of chosen neighboring pixels of the image.

Figures-(3 and 4) depict the correlation coefficients of each direction of Lena and the corresponding cipher image respectively. The figures illustrate the plain image correlation distribution is aggregated alongside the vertical, horizontal and diagonal. However, cipher image correlation distribution is spread over the plane.

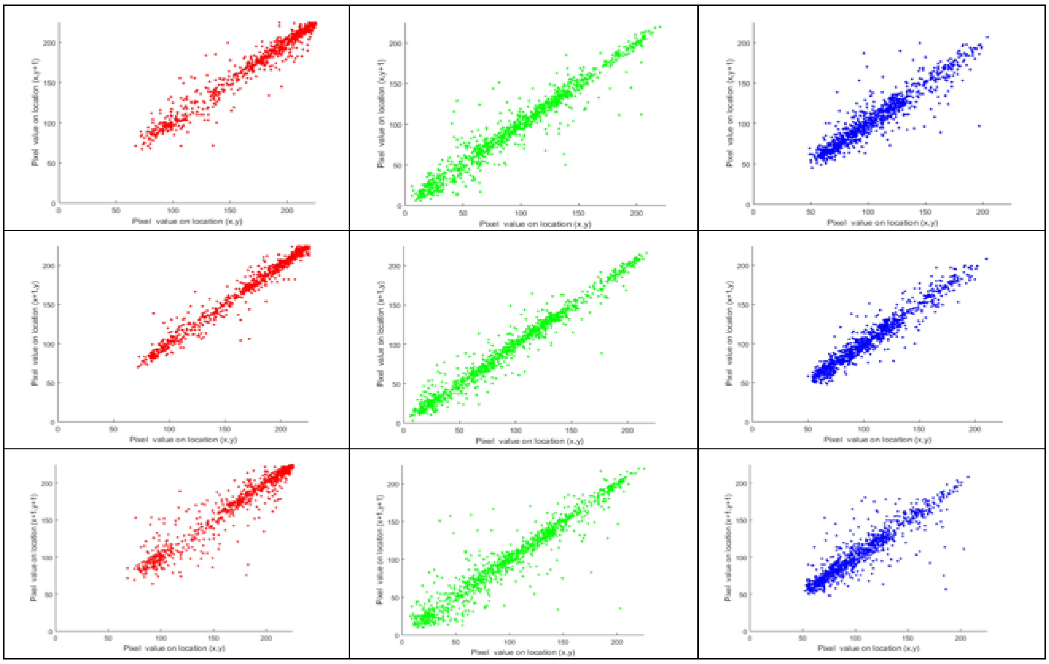

Figure 3-Vertical, horizontal and diagonal correlation coefficients for Lena plain image.

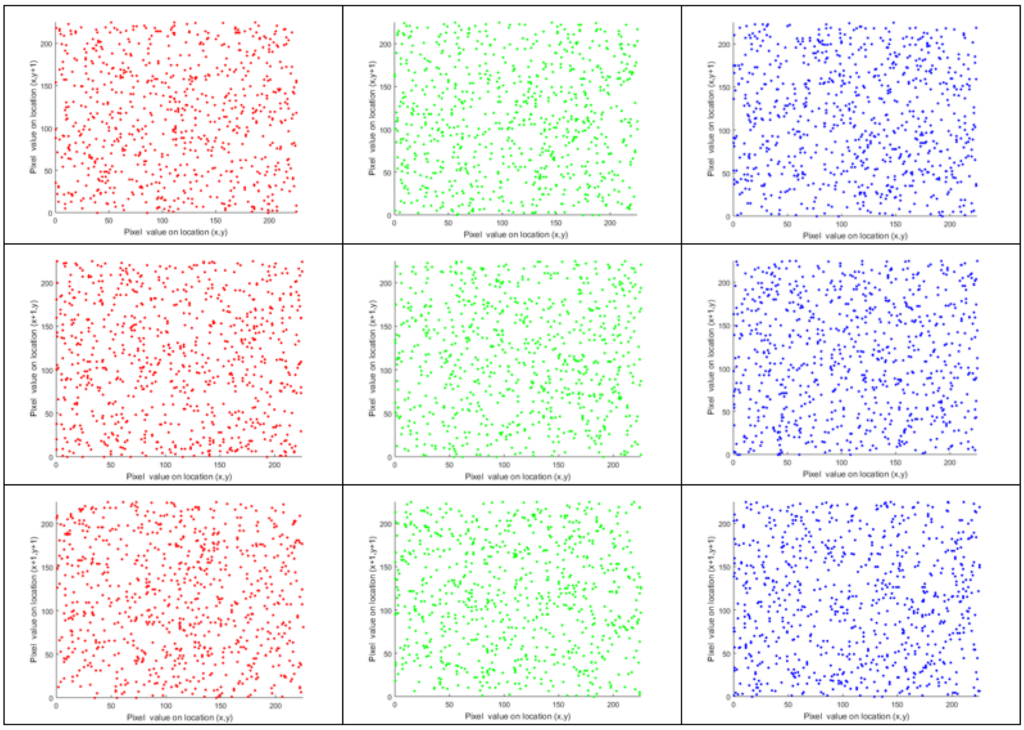

Figure 4-Vertical, horizontal and diagonal correlation coefficients for Lena cipher image

The result of correlation coefficients is so small in the proposed scheme when compared with the schemes in [5], [6], [14] and [15] as reported in Table-4. This means that the correlation is significantly reduced in the ciphered image and the ability of the proposed scheme to counter the statistical attacks is better than other schemes in [5], [6], [14] and [15].

Table 4-Comparison regarding correlation coefficient of proposed scheme vs. [5], [6], [14] and [15]

Method	**Image Size**	**Image Name**	**Correlation Coefficient**		
			Direction		
			Vertical	**Horizontal**	**Diagonal**
Proposed scheme	**512**	**Lena**	0.0002	0.0004	-0.0005
		Baboon	-0.0003	-0.0001	0.0003
		Pepper	-0.0001	-0.0002	0.0004
	256	**Baboon**	-0.0005	0.0002	0.0002
		Pepper	0.0002	0.0001	-0.0002
[5]	**512**	**Lena**	0.0030	0.0089	0.0019
[6]	**256**	**Baboon**	0.0760	0.0782	0.0707
[14]	**256**	**Baboon**	0.0002	−0.0008	−0.0006
		Pepper	0.0018	0.0052	0.0010
[15]	**512**	**Lena**	0.0242	-0.0091	-0.0137
		Baboon	0.0045	0.0086	-0.0065
		Pepper	-0.0112	0.0376	-0.0262

4.4 Differential Attack

It is the examination of how variations in information input can influence the resultant variation at the output to recover the secret key. The sensitivity of a cipher image should be high to the slight modifications in a plain image or a secret key. NPCR and UACI metrics as in Equation 17 and 18 respectively are used to examine the impact of changing one bit/pixel in the plain image on the cipher image.

$$UACI(C1,C2) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|C1(i,j)-C2(i,j)|/255}{M\times N} \times 100 \qquad (17)$$

Where

M and N are image width and height respectively.

and

$C1$ and $C2$ are encrypted images of the plain image and the modified one.

$$NCPR(C1,C2) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N} \times 100 \qquad (18)$$

Where

$$D(i,j) = \begin{cases} 0, if\ C1(i,j) = C2(i,j) \\ 1, if\ C1(i,j) \neq C2(i,j) \end{cases}$$

Tables-(5 and 6) report UACI and NPCR of the proposed scheme against schemes in [5], [14] and [15] respectively. The results show NPCR of the proposed scheme is more near to 100% than [5], [14] and [15], which means the sensitivity of the proposed scheme to the modification of plain image is high and it is effective to counter plaintext attack. Moreover, UACI is more close to 33.50 than [5], [14] and [15] that indicates the capability of counter the differential attack of the proposed scheme is better than [5], [14] and [15]

Table 5-Comparison regarding UACI of the proposed scheme against [5], [14] and [15]

UACI

Method	Image Size	Image Name	Image Component			
			R	G	B	Average
Proposed scheme	512	Lena	33.4860	33.5102	33.4963	33.4975
		Baboon	33.4936	33.5458	33.4318	33.4904
		Pepper	33.4237	33.5605	33.4551	33.4798
	256	Baboon	33.5256	33.6832	33.2911	33.5000
		Pepper	33.5923	33.5081	33.4242	33.5082
[5]	512	Lena	33.2829	33.3459	33.3270	33.3186
[14]	256	Baboon	33.4753	33.5090	33.4176	33.4673
		Pepper	33.4570	33.4705	33.4423	33.4566
[15]	512	Lena	-	-	-	33.1470
		Baboon	-	-	-	33.1890
		Pepper	-	-	-	33.1650

Table 6-Comparison regarding NPCR of the proposed scheme against [5], [14] and [15]

NPCR

Method	Image Size	Image Name	Image Component			
			R	G	B	Average
Proposed scheme	512	Lena	99.6307	99.6033	99.6143	99.6161
		Baboon	99.6307	99.6033	99.6143	99.6161
		Pepper	99.6307	99.6033	99.6143	99.6161
	256	Baboon	99.6368	99.6140	99.6368	99.6292
		Pepper	99.6368	99.6140	99.6368	99.6292
[5]	512	Lena	99.5659	99.5658	99.5959	99.5759
[14]	256	Baboon	99.6536	99.6078	99.6520	99.6378
		Pepper	99.6357	99.6158	99.6247	99.6254
[15]	512	Lena	-	-	-	99.6960
		Baboon	-	-	-	99.4030
		Pepper	-	-	-	99.2170

5. Conclusions

In this paper, a new encryption scheme for RGB image is proposed. Color image component shuffled by Chen hyper chaotic map and then converted to binary form. The key of the proposed scheme is generated by utilizing Sine chaotic map and 1D logistic chaotic map in addition to the proposed combination between the two chaotic maps. Then XOR operation is applied with the binary shuffled image to produce cipher image. Experimental results reveal that the proposed scheme capable of countering various attacks including brute force attack, statistical attack, differential attack, and known plaintext attack. Furthermore, the proposed scheme provides large keyspace and very sensitive to any simple change in the secret key.

References

1. Zhang Q., Guo L., Wei X. **2013.** A novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Optik*, **124**: 3596– 3600.

2. Wu, Y., Noonan, J.P., Yang, G. and Jin, H. **2012.** Image encryption using the two-dimensional logistic chaotic map. *Journal of Electronic Imaging*, **21**(1):3014.

3. Huang, X. **2012.** Image encryption algorithm using chaotic Chebyshev. *Nonlinear Dynamics*, **67**(4): 2411-2417. DOI 10.1007/s11071-011-0155-7

4. Zhou, G., Zhang, D., Liu, Y., Yuan, Y. and Liu Q. **2015.** A novel image encryption algorithm based on chaos and Line map. *Neurocomputing*, **169**: 150-157.

5. Kumar, M., Powdur,i P., Reddy, A. **2015.** An RGB image encryption using diffusion process associated with chaotic map. *Journal of Information Security and Applications*, **21**: 20-30.

6. Niyat, A. Y., Hei, R. M. H. and Jahan, M.V. **2015.** A RGB image encryption algorithm based on DNA sequence operation and hyper-chaotic system. International Congress on Technology,Communication and Knowledge (ICTCK).

7. Jha Y., Kaur, K. and Pradhan, CH. **2016.** Improving Image Encryption using Two-Dimensional Logistic Map and AES, India. in International Conference on Communication and Signal Processing.

8. Liu, L. and Miao, S. **2016.** A new image encryption algorithm based on logistic chaotic map with varying parameter. *SpringerPlus*, **5**: 289. DOI 10.1186/s40064-016-1959-1

9. Wang, X., Zhao, Y., Zhang, H. and Guo, K. **2016.** A novel color image encryption scheme using alternate chaotic map.ping structure. *Optics and Lasers Engineering*, **82**: 79–86.

10. Zahmoul, R. and Zaied, M. **2016.** Toward new family beta maps for chaotic image encryption," IEEE International Conference on Systems,Man and Cybernetics (SMC).

11. Pak, C. and Huang, L. **2017.** A new color image encryption using combination of the 1D chaotic map. *Signal Processing*, **138**: 129-137.

12. Rostami, M.J., Shahba, A., Saryazdi, S. and Nezamabadi-pour H. **2017.** A novel parallel image encryption with chaotic windows based on logistic map. *Computers and Electrical Engineering*, **62**: 384-400

13. Zahmoul, R., Ejbali, R. and Zaied, M**. 2017.** Image encryption based on new Beta chaotic maps.*Optics and Lasers in Engineering*, **96**: 39–49.

14. Niyat, A. Y., Moattar M. H. and Torshiz, M. N**. 2017.** Color image encryption based on hybrid hyper-chaotic system and cellular automat. *Optics and Lasers in Engineering*, **90**: 225–237.

15. Thajeel, S. A. and Al- Tamimi M. S. H. **2018.** An Improve Image Encryption Algorithm Based on Multi-level of Chaotic. *Iraqi Journal of Science*, **59**: 179-188.

16. Gan, Z., Chai, X., Han, D. and Chen, Y. **2018.** A chaotic image encryption algorithm based on 3-D bit-plane permutation. *Neural Computing and Applications*,1-20.DOI 10.1007/s00521-018-3541-y

17. Signal and Image Processing Insititute, [Online]. Available: http://sipi.usc.edu/database/database.php?volume=misc.. [Accessed 1 10 2017].