A novel chaotic System For Color Image Encryption

Sadiq A. Mehdi[1] , Abid Ali H. Alta'ai[2] and Salim Ali ABBAS[3]

[1,3]Department of computer/ Al-Mustansiriyah University/ Baghdad –Iraq
[2]Department of Mathematics/ Al-Mustansiriyah University/ Baghdad –Iraq

Abstract

a new color image encryption algorithm is proposed by combining diffusion the image pixel and keys that generating by a novel chaotic system. The performance of the algorithm has been analyzed through analyzes statistical such as histogram analysis, correlation coefficient analysis, Information entropy analysis, key space analysis, key sensitivity analysis, and results show that the algorithm has good encryption performance and high security due to key space size can reach to 10^{308} which means that very long , and the high sensitivity for small changes in key which makes the algorithm immune to Brute force attacks, and it can resist the statistical attacks, so the key space was large enough to resist many statistical attack methods, the algorithm has been implemented and analysis done by using Matlab R2012b software.

Keywords: A novel Chaotic System; Image Encryption, new algorithm.

نظام فوضوي مبتكر لتشفير صورة ملونة

د.عبد علي حمودي د.سالم علي عباس صادق عبد العزيز مهدي

الجامعة المستنصرية / كلية التربية / قسم علوم الحاسبات

المستخلص

تم اقتراح خوارزمية جديدة لتشفير صورة ملونة من خلال الجمع بين انتشار قيم مواقع الصورة والمفاتيح التي تولدت من النظام الفوضوي المبتكر. وقد تم تحليل أداء الخوارزمية من خلال اجراء التحليلات الإحصائية مثل : تحليل المدرج التكراري ، وتحليل معامل الارتباط، وتحليل انتروبية المعلومات ، تحليل مساحة المفتاح، تحليل حساسية المفتاح، وأظهرت النتائج أن الخوارزمية لديها اداء جيد للتشفير وذات امنية عالية نظراً لحجم مساحة المفتاح الذي يمكن ان يصل الى 10^{308} وهوما يعني كبير جداً ، وان الخوارزمية ذات حساسية عالية لإجراء تغييرات صغيرة في المفتاح الذي يجعل

الخوارزمية في مأمن من هجمات القوة الوحشية ، وبالتالي فإن حجم مساحة المفتاح كبير بما فيه الكفاية لمقاومة العديد من أساليب الهجوم الإحصائية. تم استخدام برنامج الـ MatlabR2010a لتنفيذ الخوارزمية واجراء التحليلات.

1 Introduction

The 21st century is the era of global information. Information is related to personal privacy or commercial confidentiality, or even the national security. `Snowden' demonstrates that our information security is faced with severe challenges. Information security issues are becoming the focus of attention. Image is an important information carrier, which is used in all walks of life because of the bulk data capacity, high redundancy and correlation, and therefore the image security is particularly important. However, due to these features, traditional encryption methods such as DES [1], AES [2] are not so suitable for digital image encryption. Chaotic system possesses some excellent features for data encryption, such as good pseudo-random performance, sensitivity to initial conditions [1].Chaos for data encryption was first proposed by Mathews [4]. With the growing application of chaos, chaotic system has been widely used in image encryption, many researchers have investigated and began to propose encryption algorithms based on the low-dimensional chaotic systems [2, 3, 4]. But low-dimensional chaos has some defects such as limited key space and low security because of the small number of parameters, and chaotic sequences generated by low dimensional chaotic maps have shorter periodicity [5, 6]. The high-dimensional chaotic system with higher complexity, randomness and unpredictability, can resist the attack better, therefore high-dimensional chaotic system are widely used in image encryption [7]. The three-dimension chaotic system such as Chua's circuit is suitable to encrypt the three components of color image. Recently, more and more hyper-chaos are applied in image encryption algorithm because it has two positive Lyapunov exponents, better sensitivity and more complex dynamical characteristics [5, 8, 9]. It is common only using a single chaotic system, but using encryption algorithms constituted by one chaotic map are easy to be attacked [10, 11]. To solve the problems mentioned above, hybrid chaotic system is employed to enhance the key space and the complexity of the algorithm. At present, there are few encryption algorithms based on high-dimensional chaotic system and hyper-chaotic system. In this paper, we propose a color image encryption algorithm by the novel hyper-chaotic system.

2 The novel chaotic system

The novel ten-dimensional autonomous system is obtained as follows:

$$\frac{dx}{dt} = \sigma(y - x) - \rho(z\,s + w)$$
$$\frac{dy}{dt} = \delta\,x - x\,z - y$$
$$\frac{dz}{dt} = x\,y - \eta\,z$$
$$\frac{du}{dt} = -v + \eta\,s\,q - u$$
$$\frac{dv}{dt} = -\lambda(v + w\,q) - u \qquad (1)$$
$$\frac{dw}{dt} = \gamma\,x + z\,x$$
$$\frac{dp}{dt} = \mu\,r$$
$$\frac{dq}{dt} = -\mu(q + p\,r)$$
$$\frac{dr}{dt} = -\varphi\,p + q\,x + \xi\,q\,s$$
$$\frac{ds}{dt} = -\beta\,p\,r - \omega(s - p)$$

Where x, y, z, u, v, u, w, p, q, r , s and t $\in \Re$ called the states of system and $\sigma, \rho, \delta, \gamma, \eta, \lambda, \gamma, \mu, \varphi, \xi, \beta$ *and* ω are positive parameters of the system.

The 10-D system (1) exhibits a chaotic attractor, when the system parameter values are chosen as:

$$\sigma = 20, \rho = 2.1, \delta = 15, \eta = 2, \lambda = 8, \gamma = 10, \mu = 5, \varphi = 25, \xi = 5.1, \beta = 1, \omega = 1.9 \qquad (2)$$

We take the initial conditions as:

$$x(0) = -1, y(0) = 4, z(0) = 1, u(0) = 0, v(0) = 0, w(0) = 1, p(0) = 0,$$
$$q(0) = -1, r(0) = 8, s(0) = 5.$$

This a novel ten-dimensional nonlinear system. Some basic properties of the system have been investigated .The new 10-D chaotic system has three unstable equilibrium points and calculated Lyapunov exponents, the Lyapunov exponents of the system are :

L_1= 18.94059 , L_2= 9.96383 , L_3= 1.00877,L_4= 0.828434 ,L_5= 0.0490522 ,L_6= -0.0132193 ,

L_7= -0.0646262 , L_8= -1.00973 , L_9= -28.8771 , L_{10}= -39.729, the maximal Lyapunov exponent (MLE) of the novel system is L_1= 18.94059. In addition

the Lyapunov dimension of the novel chaotic system is obtained as D_{KY} =9.04596.

Using MATHEMATICA program, the numerical simulation have been completed. This nonlinear system exhibits the complex and abundant chaotic dynamics behaviors, the strange attractors are shown in Figs.1&2.

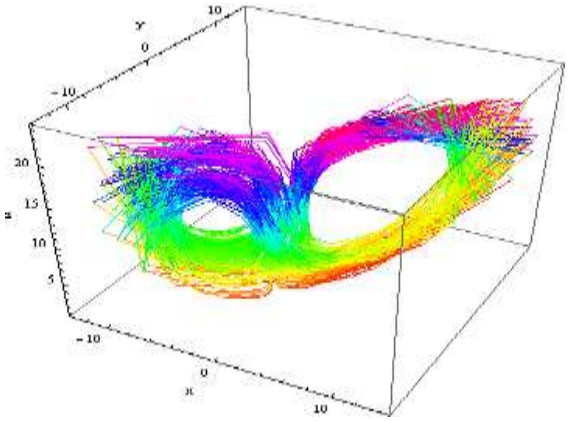


Fig.1. Chaotic attractors ,three- dimensional view (x-y-z)

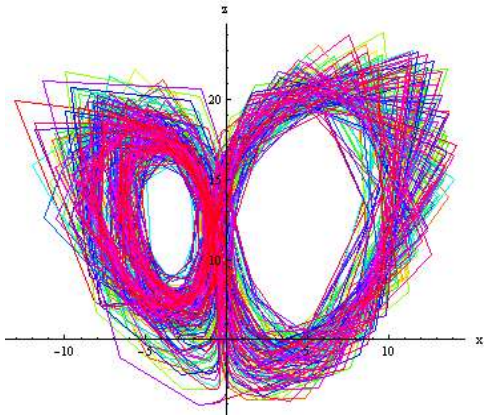


Fig.2 *Chaotic attractors* , *z–x* phase plane

3 Image Encryption Algorithm

The proposed algorithm combines pixel value diffusion process and chaotic keys. Suppose the original image is noted (OI)with size 256×256. The color image encryption scheme consists of 8 steps, which is detailed described as follows:

Step 1:
Read the data of Original Image (OI) and split the color image into R, G, B components. i.e. size of (OI) M×N×3.

Step 2:
Covert Original Image into (32) blocks of size 8×8

Step 3: (Diffusion Process1)
Transform row 1 by row 4 , Transform row 2 by row 5, Transform row3 by row 7 and Transform row 6 by row 8.

Step 4: (Diffusion Process2)
Transform column 1 by column 4 , Transform column 2 by column 5, Transform column 3 by column 7 and Transform column 6 by column 8.

Step 5:
Set the Parameters δ ,λ , β,μ ,λ , η, γ ,ϕ ,ω ,ξ ,ρ and initial conditions x_0 ,y_0 ,z_0 ,u_0 ,v_0 ,w_0 ,p_0 ,q_0 , r_0, s_0 , generate ten sequences {(x_i ,y_i ,z_i ,u_i ,v_i ,w_i ,p_i ,q_i , r_i, s_i) ; i = 1, 2,…, 65554} according to the novel chaotic system (1).

Step 5 :
Round the chaotic sequences
x_i=round(x_i*1000) , y_i=round(y_i*1000) , … , s_i=round(s_i*1000)
step 6 : Covert chaotic sequences into matrix 256×256

Step 7 :
Covert matrix chaotic sequences into 4 blocks of size 16×16

Step 8 :
Preform XOR operation between 4chaotic keys and blocks of Original Image after diffusion process. The flowchart of this algorithm shown in Fig.3
The decryption process is just the reverse process of the encryption process.

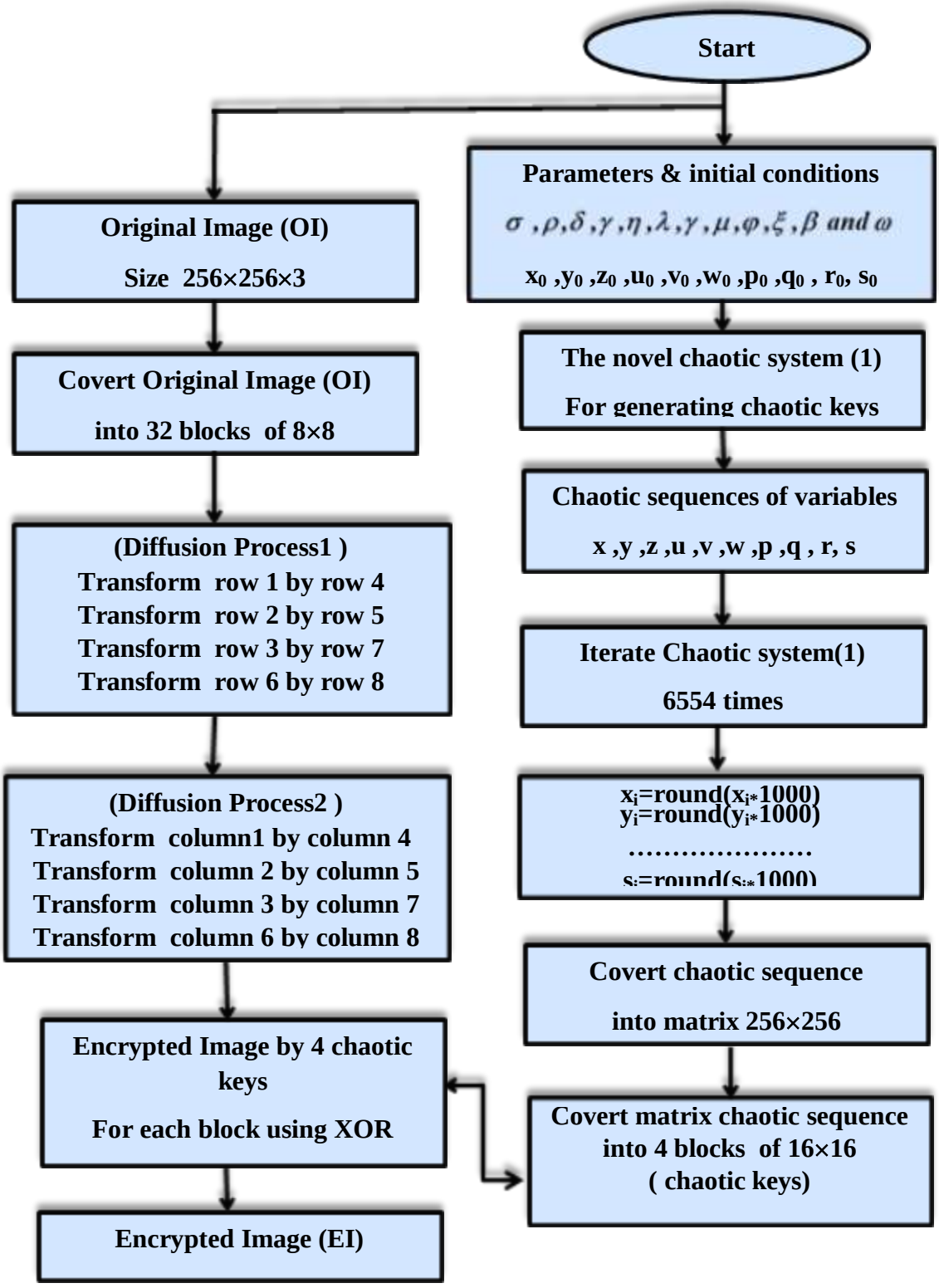


Fig.3 Flowchart of Encryption

4 Image Decryption Algorithm

The proposed algorithm combines pixel value diffusion process and chaotic keys.

Suppose the original image is noted (OI) with size 256×256. The color image encryption scheme consists of 10 steps, which is detailed described as follows:

Step 1:

Read the data of Encryption Image (EI) and split the color image into R, G, B components. i.e. size of (OI) M×N×3.

Step 2: Covert Encryption Image into (32) blocks of size 8×8

Step 3:

Set the Parameters δ ,λ , β,μ ,λ , η, γ ,ϕ ,ω ,ξ ,ρ and initial conditions x_0 ,y_0 ,z_0 ,u_0 ,v_0 ,w_0 ,p_0 ,q_0 , r_0, s_0, generate ten sequences {(x_i ,y_i ,z_i ,u_i ,v_i ,w_i ,p_i ,q_i , r_i, s_i) ; i = 1, 2,…, 65554} according to the novel chaotic system (1).

Step 4 : Round the chaotic sequences

x_i=round(x_{i*}1000) , y_i=round(y_{i*}1000) , … , s_i=round(s_{i*}1000)

step 5 : Covert chaotic sequences into matrix 256×256

Step 6 : (chaotic keys)

Covert matrix chaotic sequences into 4 blocks of size 16×16

Step 7 : Preform XOR operation between 4 chaotic keys and blocks of Encryption Image .

Step 8: (Reversed-Diffusion Process1)

Transform row 4 by row 1 , Transform row 5 by row 2, Transform row7 by row 3 and Transform row8 by row 6.

Step 9: (Reversed-Diffusion Process2)

Transform column 4 by column 1 , Transform column 5 by column 2, Transform column 7 by column 3 and Transform column 8 by column 6.

Step 10 :

We have the Original Image .

The flowchart of decryption algorithm shown in Fig.4

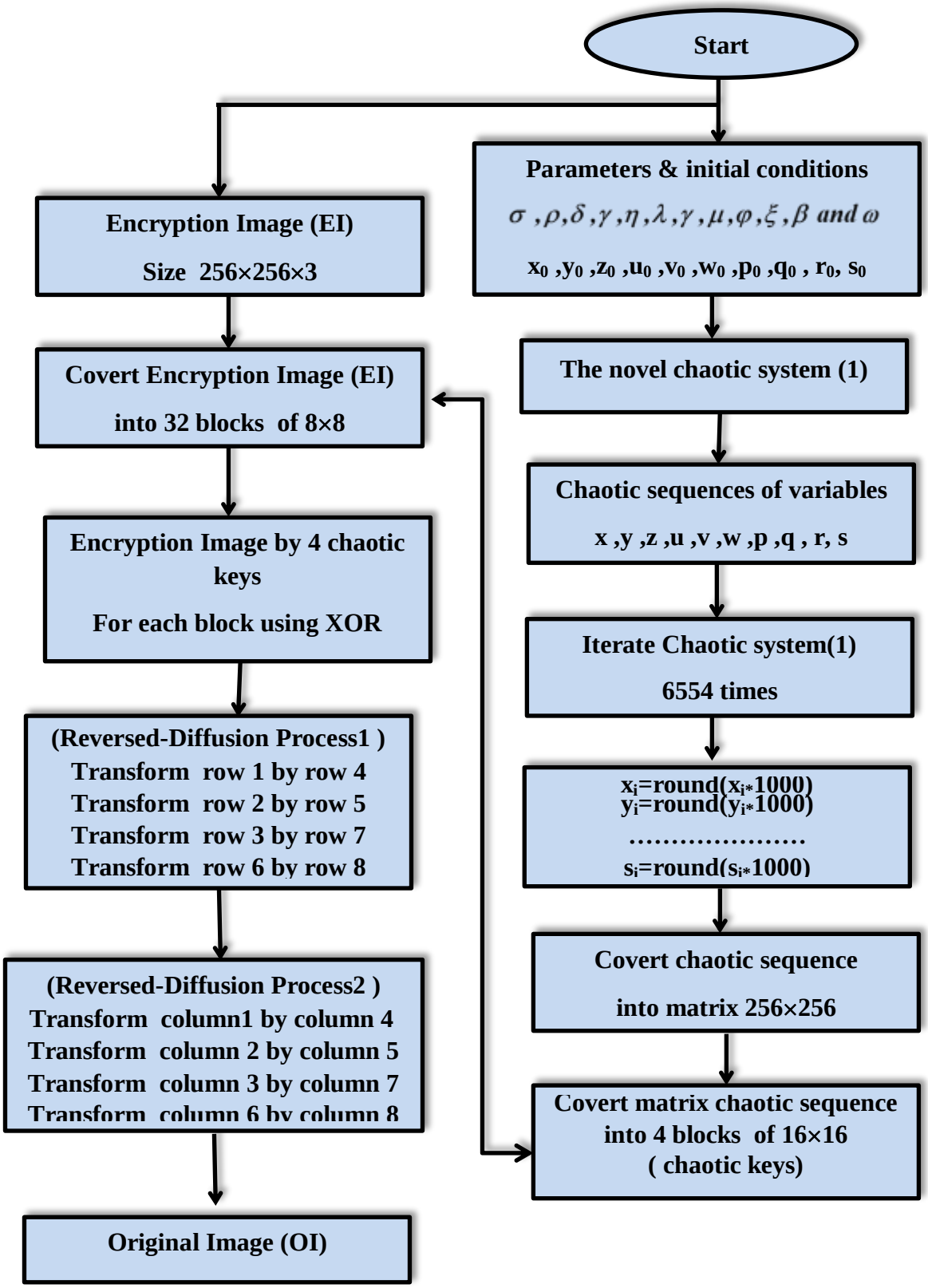


Figure 4: Flowchart of Decryption

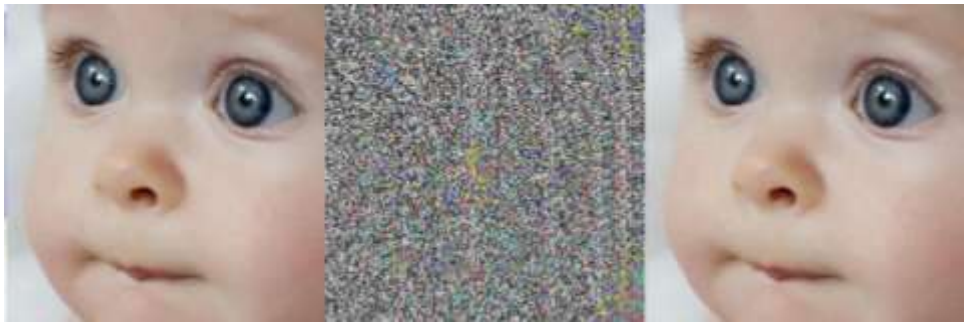
5 Experimental Results and Security Analyses

We utilize Matlab to simulate the experiment and choose the color image `baby' of size 256 ×256 to be encrypted. Parameters and initial values of a novel chaotic system(1) are set as:

$$x(0)=-1, y(0)=4, z(0)=1, u(0)=0, v(0)=0, w(0)=1, p(0)=0,$$
$$q(0)=-1, r(0)=8, s(0)=5.$$

Parameters and initial values of a novel chaotic system(1) are:
$\sigma=20, \rho=2.1, \delta=15, \eta=2, \lambda=8, \gamma=10, \mu=5, \varphi=25, \xi=5.1, \beta=1, \omega=1.9$.

The experiment results are shown as Fig. 5. Compared with Fig. 5(a) Original image 'baby' and Fig. 5 (b) Encrypted image of `baby' (hides the information effectively). The attackers cannot find any useful clues from the encrypted image.



(a) (b) (c)

Fig. 5: Experiment Results: (a) Original 'baby'. (b) Encrypted image of 'baby'.

(c) Decrypted image of 'baby'

6 Statistical Analysis

In this section, some performance metrics by which the quality of an encryption algorithm is checked statistically, are discussed in detail as follows:

6.1. Histogram analysis

Histogram analysis gives the idea to statistical analysis attackers, but in this proposed method by the use of histogram the attackers cannot find the any clue about the original image. The proposed method gives the original image and cipher image histogram, which is shown in fig. 6; it shows that the cipher image histogram is completely horizontal so if any statistical attackers attack, then opponent cannot break the proposed security. In this method the cipher image red, green and blue histograms are flat because of diffusion method, which altered the original values of pixels. Nearly horizontal histogram proves

that this proposed method is secure from external users. The R, G, B histograms of original Baby and encrypted image are shown as Fig. 6.

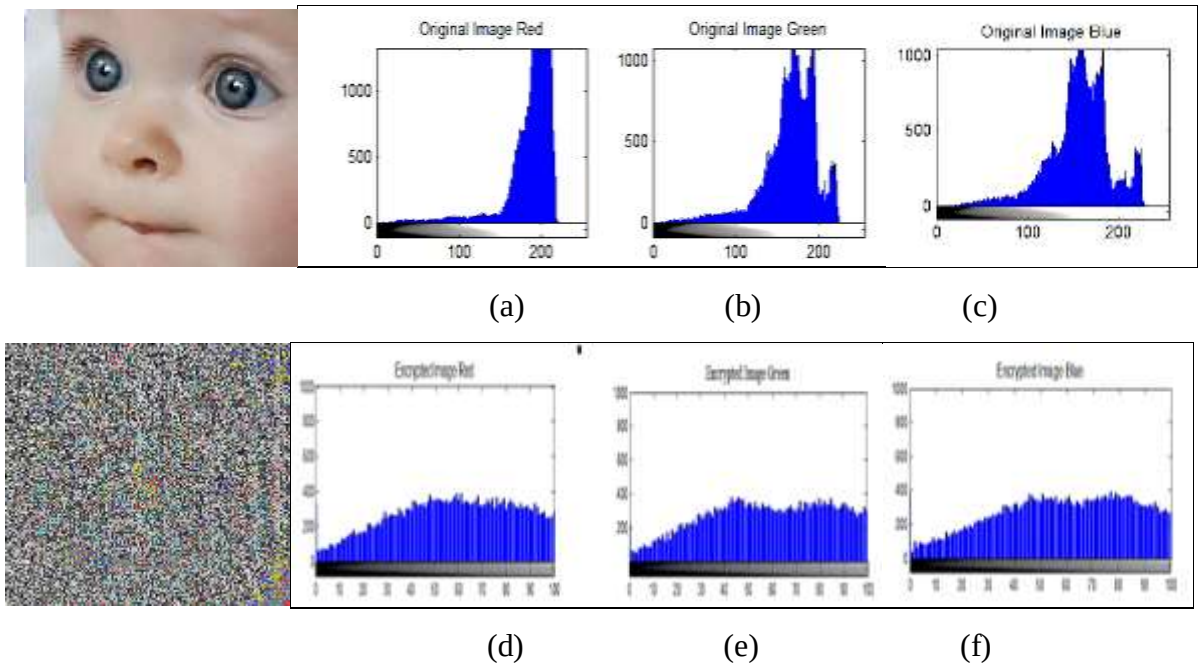


Fig. 6: Histograms of original image and encrypted image: (a), (b), (c) are histograms of R, G, B from original 'Baby'. (d), (e) and (f) are histograms of R, G, B from encrypted 'Baby'.

Compared the original histogram, the encrypted image histogram is smoother and more uniform.

So the algorithm can cover up the information and distribution of the original image. It has a certain role to resist the statistical attack.

6.2 Correlation coefficient analysis

The correlation coefficient give the relationship between two neighboring pixels, if correlation between two pixels is nearly 1 then the image is highly correlated but if it is nearly 0 the image pixels are highly uncorrelated. In the proposed method the experiments on the images proves that the original image correlation nearly one, and cipher image correlation is nearly zero. So this saves the system from statistical attacks. Table 1. (a) and Table 1. (b) show the results of experiments. The formula of correlation coefficient of two adjacent pixels gives as follow:

$$cov(x,y) = E(x - E(x))(y - E(y)),$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{var(x)}\ \sqrt{var(y)}}$$

Where x and y are the values of two adjacent pixels in the image. We can calculate cov(x,y) , var(x) and var(y) by the use of following equation.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \qquad var(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \text{and}$$

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

Correlations between two vertically , horizontally and diagonally adjacent pixels in various original images and their corresponding cipher images have been analyzed . In Fig. 6, the distributions of horizontally adjacent pixels of red, green and blue components in the image '*Baby*' and their corresponding cipher image is shown. Particularly, in Frames (a), (b) and (c), depict the distributions of two horizontally adjacent pixels of red, green and blue components respectively in the original image. Similarly in Frames (d), (e) and (f) respectively, the distributions of two horizontally adjacent pixels in its corresponding cipher image have been depicted. Similarly, in Figure 7, the distributions of vertically adjacent pixels of red, green and blue components in the original image '*Baby*' and its corresponding cipher image is shown. Similarly, in Figure 8, the distributions of horizontally adjacent pixels of red, green and blue components in the original image '*Baby*' and its corresponding cipher image is shown and in Figure 9, the distributions of diagonally adjacent pixels of red, green and blue components in the original image '*Baby*' and its corresponding cipher image is shown It is observed from correlation charts and Table 1 that there is a negligible correlation between the two adjacent pixels in the cipher image. However, the two adjacent pixels in the original image are strongly correlated. Correlation in the cipher images is very small or negligible when the proposed encryption scheme is used. Hence the proposed scheme has good permutation and substitution properties.

Table 1. Correlation for two adjacent pixels in the original and its cipher image.

		Correlation coefficient between adjacent pixels		
		Red	**Green**	**Blue**
Horizontal	**original image**	0.9871	0.9880	0.9881
	Cipher Image	0.0062	0.0079	0.0019
Horizontal	**original image**	0.9841	0.9850	0.9855
	Cipher Image	0.0070	0.0094	0.0037
Diagonal	**original image**	0.9748	0.9765	0.9772
	Cipher image	0.0092	0.0095	0.0079

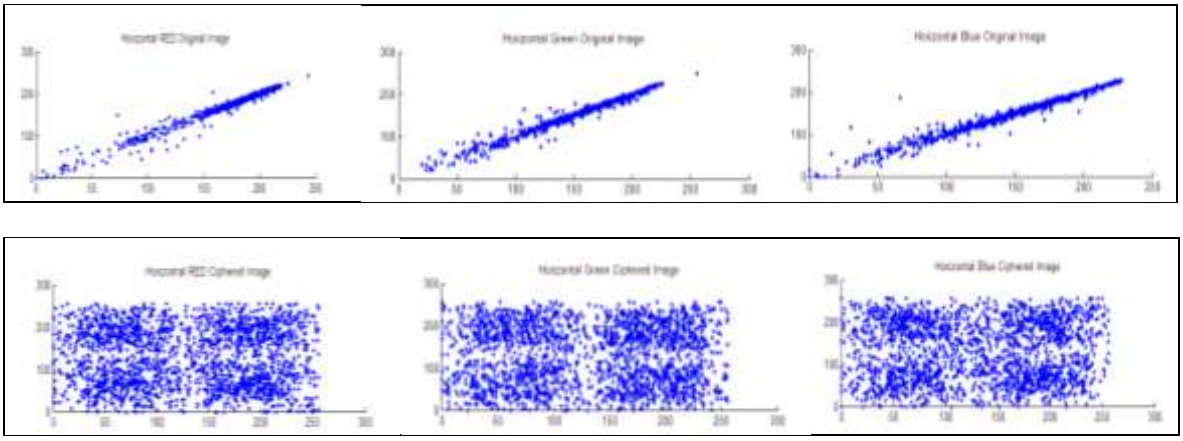


Fig. 7 : Distributions of horizontally adjacent pixels of RGB components in the original image '*Baby*' and its cipher image.

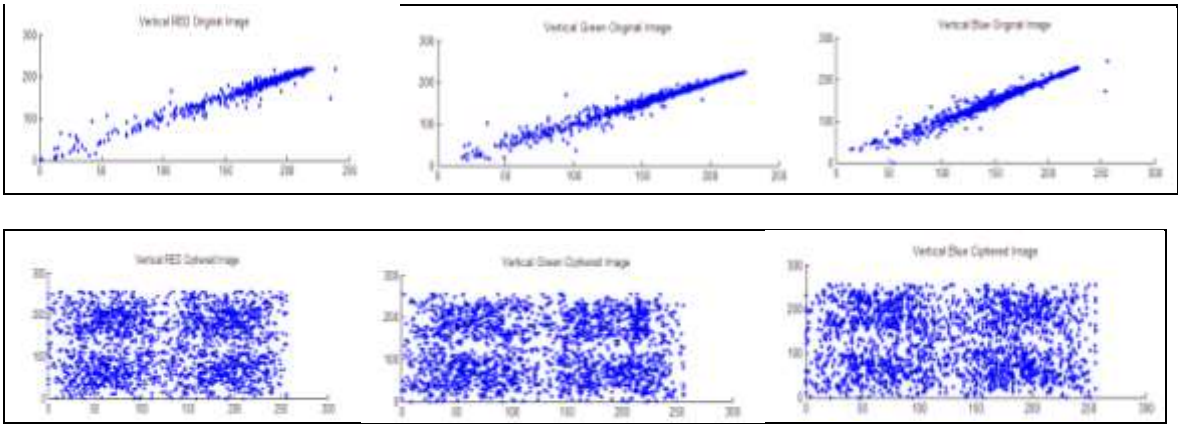


Fig. 8 : Distributions of vertically adjacent pixels of RGB components in the original image '*Baby*' and its cipher image.

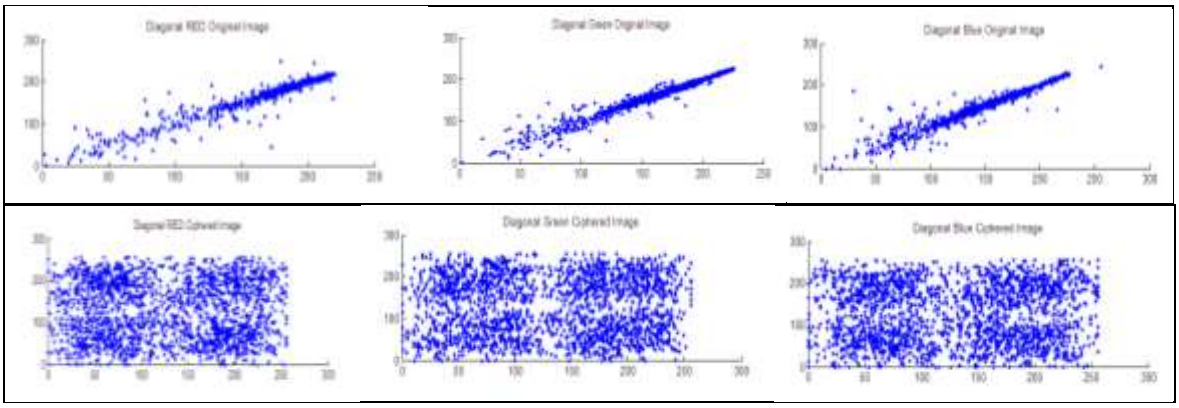


Fig. 9 : Distributions of diagonally adjacent pixels of RGB components in the original image '*Baby*' and its cipher image.

6.3 Information entropy analysis

Illegibility and indeterminateness are the chief objectives of image encryption. his indeterminateness can be displays by one of the most commonly used notional measure of entropy. Entropy states the degree of uncertainties in the system and the formula of entropy is given as follow:

$$H(s) = -\sum_{i=0}^{N-1} P(s_i) \log_2 p(s_i)$$

Where $p(s_i)$ is the beginning probability of s_i . If each symbol has an equal probability, i.e. $s=(s_0,s_1, s_2,\ldots ,s_{256})$ where $p(s_i)$ is equal to $1/2^8$ then the entropy is $H(s)=8$. This resembles to an ideal case. Practically the entropy of the systems is less than the ideal case in the proposed image encryption method the entropy of the encrypted images close to 8, the information entropy of encrypted image given in table 2. So the very less information outflow in the proposed cryptosystem, this proves that the proposed method is secure against entropy attacks.

Table 2: Information entropy of encrypted image

Encrypted image	Image size	R Layer	G Layer	B Layer
Baby	256×256	7.6087	7.4231	7.8956

6.4 Key Space Analysis

A good image encryption algorithm should have a large key space to make the brute-force attack infeasible. In the proposed algorithm, the keys are the novel chaotic system (1) are initial conditions and parameters . Therefore, if the computational precision is 10^{-14}, the key space of the algorithm is 10^{308} and it is bigger than 2^{128} . So the algorithm has a sufficiently large key space to resist the brute-force attack.

6.5 Key sensitivity Analysis

An ideal image encryption procedure should be sensitive to cipher key. In order to test the sensitivity, we select 'Baby' to be the original image, keep other parameters the same and employ the initial value of $s_0 = 5$ to decrypt the encrypted image. The results are illustrated in Fig. 10. By comparing the two decrypted images, we can find that even with a tiny difference of 10^{-14}, attacker cannot decrypt the original image correctly. The proposed algorithm has good key sensitivity and ability of resisting exhaustive attack.

(a) (b) (c) (d)

Fig. 10: Results of sensitivity test: (a) Original image of 'Baby'. (b) Encrypted image of (a). (c) Decrypted image of (a) with the correct key. (d) Decrypted image of (a) with a change in initial value of s (s_0= 5.000001)

7 Conclusion

A color image encryption algorithm based on a novel chaotic system is putted forward. The pixel values of the R, G, B from the color image are combined diffusion image and keys of a novel chaotic system. The complexity and key space of the algorithm is greatly enhanced. Simulation results show that the proposed algorithm is simple to implement and has good performance. It can effectively resist statistical attack, entropy attack, brute-force attack and exhaustive attack.

References

[1] C. Peng, Y. X. Li, Algorithm for image encryption using couple chaotic system and cellular automata, Journal of Computational Information Systems, 10(5), 2014, 1993-2000.

[2] J. Fridrich, Symmetric, Ciphers based on two-dimensional chaotic map, International Journal of Bifurcation and Chaos, 8(6), 1998, 1259-1284

[3] N. K. Pareek, V. K. Patidar, K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, 24(9), 2006, 926-934

[4] A. Akhshani, S. Behnia, A. Akhavan et al., A novel scheme for image encryption based on 2D piecewise chaotic maps, Optics Communications, 283(17), 2010, 3259-3266.

[5] C. X. Zhu, A novel image encryption scheme based on improved hyper-chaotic sequences, Optics Communications, 285(1), 2012, 29-37

[6] F. Y. Sun, Z. W. Lu, S. T. Liu, A new cryptosystem based on spatial chaotic system, Optics Communications, 283, 2010, 2066-2073

[7] H. J. Liu, X. Y. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications, 284(16-17), 2011, 3895-3903.

[8] T. G. Gao, Z. Q. Chen, A new image encryption algorithm based on hyper-chaos, Physics Letters Application, 372, 2008, 394-400

[9] H. Zhu, C. Zhao, X. Zhang, A novel image encryption-compression scheme using hyper-chaos and Chinese remainder theorem, Multimedia Systems, 28(6), 2013, 670-680.

[10] T. V. Laptyeva, S. Flach, K. Kladko, The weak-password problem: Chaos, criticality, and encrypted p-CAPTCHAs, Europhys Lett., 95(5), 2011, 1031-1037

[11] L. L. Liu, Z. Qiang, X. P. Wei, A RGB image encryption algorithm based on DNA encoding and chaos map, Computers and Electrical Engineering, 38(5), 2012, 1240-1248.