International Journal of Engineering & Technology, 7 (4.36) (2018) 270-276

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Image Encryption Algorithm Based on a Novel Five-Dimensional Hyper- Chaotic System

Sadiq A. Mehdi[1], Zynab M. jasim[2]

[1]departement of Computer Science / College of Education/ University of Al-Mustansiriya/Iraq.
[2]departement of Computer Science / College of Education/ University of Al-Mustansiriya/Iraq.
**Corresponding author E-mail: zynabjasim05@gmail.com*

Abstract

According to the fast growth of the Internet and communications networks, you must protect the secrecy of digital images sent over public networks. In recent times, researchers have developed ways to chaotic systems based image encryption. Specific characteristics of the disorder systems, such as dependence on initial conditions sensitivity, pseudorandom, ergodicity and system parameters, chaotic dynamics systems became as a promising alternative to traditional encryption algorithms. In this work, A fresh algorithm is presented to encrypt images depend on a novel five dimensional hyper-chaotic system to achieve High level of security, the chaotic sequence generated from system employ for permutation the original image to create a cipher image. The security of presented encryption algorithm evaluated by much security analysis such as Histogram Analysis, Correlation Coefficient Analysis, Information Entropy Analysis, Key Space Analysis, Key Sensitivity Analysis, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal to Noise Ratio , The experimental results demonstrate that the algorithm has good encryption effect, large key space equals to $10^{182}$and high sensitivity to a tiny change in secret key for decrypted images ,therefore, the presented encryption algorithm depend on a novel hyper- chaotic system is more secure against the statistical and deferential attacks.

Keywords: *Novel five dimensional hyper-chaotic system, Digital images, Image encryption.*

1 Introduction

The security of information is very important during deals with the internet. Most ofthe information is shared in the form of digital images. Thus, an excellent and safety image encryption scheme is needed all the time. [1, 2] Encryption is a way to keep the confidentiality of images. Images have an important role in communicating, such as; military, national-security agencies and diplomatic affairs. These images may carry highly secrecy data, thus, these images require considerable protection when stacking users somewhere across an untrusted warehouse [3]. Image encryption is an algorithm to transform ordinary image to an encrypted image therefore, without the secret key is true, no unauthorized users can restore the original image even if they get the encrypted image. Usually, image and video data have very big-sized and enormous, thus, the huge data encrypting process with the traditional ciphers incurs large cost, and it is too costly for real-time multimedia applications, such as video conference, image surveillance, which require real-time operations, such as copying, cutting, displaying, control the bit-rate or recompression. [4, 5] Chaos is appropriate for image ciphering, with close association some special characteristics dynamics. Chaos, having a kind of random, and unanimously affirmed in the academic community .Chaos, also has the first forecast sensitivity categories properties over the long term is sensitive to noise, ergodicity, mixed and spacing indicator, is very suitable for ciphering. There are two basic properties of confusion and diffusion are essential attributes of good encryption both are important features of chaotic systems too .[6, 7] Chaos is high sensitive to initial conditions and its sequences have randomness and a large key space therefore, it can be used to encrypt data such as images, Chaotic behavior is so difficult to predict by analytical methods without the secrete key being known thus, it is an excellent and strong encryption scheme against statistical attacks.[8, 9]

This paper is organized as follows: will introduce some related work in section 2, in the third section, the five dimensional hyper-chaotic system is introduced; a new color image encryption algorithm is described in Section four. Security analysis of results is displayed in section v. Finally, we will describe the outcome of this paper in section 6.

2 Related work

In recent times, many proposed encryption systems based on chaos system, Taiyong Lia et al in (10) propose a novel algorithm that combines the Fractional-Order Hyper-Chaotic Lorenz system and DNA computing for image encryption, the fractional order hyper-chaotic Lorenz system is adopted to generate the pseudorandom sequence that is utilized throughout the process of encryption. DNA operations such as DNA addition, DNA subtraction and DNA XOR are also introduced to the algorithm. Chong Fu et al in (11) suggest Color image coding a new alternative to replacement to meet the growing demand for secure image connections in real time byUsing sequence extracted from the orbit of the chaotic Chen system. Hong-Mei Yuan et al in (12) presented a new parallel image cryptosystem by using five dimensional hyper-chaotic system combined with Logistic map to generate a semi-random sequence of better characteristics .

3 A novel hyper-chaotic system

In chaotic systems, the hyper-chaos system contains two or more of positive Lyapunov exponents. The chaotic sequences of chaotic system based on parameters and initial conditions, so its dynamic behaviors are more difficult to predict and the attractive clutter is more complex. Hyper-chaotic enjoys the distinctive feature excessive chaos system on a low level of chaos.[13] In this divisional, novel five dimensional hyper- chaotic system is establishment then investigates to be hyper- chaotic. The dynamic behaviors of the novel system are obtained. A proposed novel system will be employed in the propose encryption algorithm to permute and encrypt a color image, this system can be obtain as follows:

$$\begin{aligned} x' &= -ax + by + u + cz \\ y' &= dx - y - xz - w \\ z' &= -ez + xy + fu \\ u' &= -xz + gu + cw \\ w' &= hy - x - fxz \end{aligned} \qquad (1)$$

Where x, y, z, u, w and t $\in \Re+$ called states of system and *a,b,c,d,e,f,g* and *h* positive parameters of a novel system. The 5-D system which obtained from equations (1) shows a chaotic attractor, if parameter values of the system are chosen as: **a=9, b=4.6, c=0.5, d=25, e=0.1, f=2.5, g=2 and h=3.** Basic characteristics and complex dynamics of new chaotic system such as Equilibrium Point, Lyapunov exponents, fractal dimensions, and attractors are investigated, the results shows that the new system is hyper- chaotic and more suitable for image encryption .

3.1 Equilibrium Point

The new five dimensional (1) contains of three equilibrium points when the system parameter values are specified as: **a=9, b=4.6, c=0.5, d=25, e=0.1, f=2.5, g=2 and h=3.** And the nonlinear equations solved as follows:

$$\begin{aligned} 0 &= -ax + by + u + cz \\ 0 &= dx - y - xz - w \\ 0 &= -ez + xy + fu \\ 0 &= -xz + gu + cw \\ 0 &= hy - x - fxz \end{aligned} \qquad (2)$$

The three equilibrium points are:
E_0\{x=0, y=0, z=0, u=0, w=0\}
E_1\{x=-7.16838, y=-6.25877, z=16.1932, u=-43.8217, w=-56.8716\}
E_2\{x=6.32662, y=5.01097, z=13.7613, u=27.0085, w=66.0918\}
The eigenvalues that corresponding to equilibrium E_0 (0, 0, 0, 0, 0) are respectively obtained as follows:
$\lambda_1 =$ -16.3806, $\lambda_2 =$ 6.21146, $\lambda_3 =$ -2.50127 $\lambda_4 =$ 1.69082 and $\lambda_5 =$ 0.47954.

Therefore, the equilibrium E_0(0,0,0,0,0) is a saddle point, and a hyper-chaotic system is unsteady at the point E_0. So it is easy to prove that both the equilibrium points E_1 and E_2 are also unstable saddle points at the same time. So for equilibrium point E_1 and E_2 respectively, The eigenvalues will be: $\lambda_1 =$ **0.6675+7.28477i,** $\lambda_2 =$ **0.6675-7.28477i,** $\lambda_3 =$ **-0.132035+0.832712i,** $\lambda_4 =$ **-0.132035-0.832712i,** $\lambda_5 =$ **-11.5709** and $\lambda_1 =$ **1.15295 +5.68211i,** $\lambda_2 =$ **1.15295 -5.68211i,** $\lambda_3 =$ **-0.294002 + 0.92704i,** $\lambda_4 =$ **-0.294002-0.92704i,** $\lambda_5 =$ **-12.2179**. the results of the two equilibrium points E1 and E 2, show that λ5 is a negative real numbers, λ1 and λ2 become a pair of complicated conjugate eigenvalues, also λ3 and λ4 become a pair of complicated conjugate eigenvalues with positive real parts .Therefore, equilibrium points E1 and E2 are all saddle-focus points; so, these equilibrium points are all unstable.

3.2 Lyapunov Exponents and Lyapunov Dimensions

The new 5-D hyper-chaotic system has five Lyapunov exponents which are: L1= 0.369371, L2= 0.21519, L3= -0.0287322, L4= -0.529396, L5= -10.5262. Since the novel hyper-chaotic contains two positive Lyapunov exponents in *L*1 and L2, and the rest three Lyapunov exponents are negative. Therefore, this novel system is hyper-chaotic. For this new system , by noticing the values of five Lyapunov exponents, the Kaplan-Yorke dimension can be obtained due to L1+L2+ L3 +L4>0 and L1+L2+L3+L4+ L5 <0, the Lyapunov dimension of this system will be:

$$D_{KY} = j + \frac{1}{\left|L_{j+1}\right|} \sum_{i=1}^{j} L_i \qquad (3)$$

$$D_{KY} = 4 + \frac{1}{\left|L_{j+1}\right|} \sum_{i=1}^{4} L_i = 4 + \frac{L_1 + L_2 + L_3 + L_4}{L_5}$$

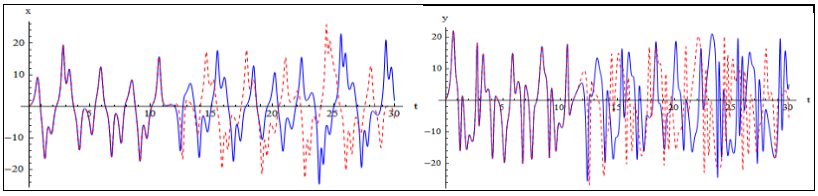
$$= 4 + \frac{0.369371 + 0.21519, + -0.0287322 + -0.529396}{10.5262}$$

$$= 4.00251$$

That means the Lyapunov dimension of new hyper-chaotic (1) is fragmentary, Due to the fragment nature, the new chaotic system contains non-periodic paths; its close trajectories diverge. Thus, there is really chaos in this nonlinear system.

3.3 Sensitivity to initial conditions

Also the new chaotic trajectories has high sensitivity towards initial conditions when the initial conditions of system(1) be **X(0)=0.1 , y(0)=0.5,z(0)=3.5,u(0)=0.6 and w(0)=0.4.** For the solid line and **X(0)=0.1 , y(0)=0.5, z(0)=3.5,u(0)=0.60000001 and w(0)=0.4.**for the dashed line. Fig1. shows that the evaluation of the chaos trajectories is high sensitivity to initial values.



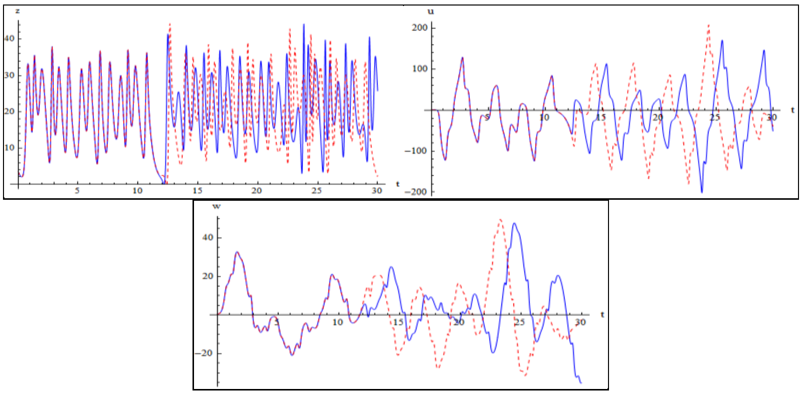


Fig.1. Sensitivity tests of the novel system *x(t), y(t), z(t), u(t), w(t)*

3.4 Phase portraits

The novel system has strange attractors in three and two dimensions When the parameters are chosen as: a=9, b=4.6, c=0.5, d=25, e=0.1, f=2.5, g=2 and h=3, Fig.2 and Fig.3 illustrate the strange attractors for this system.

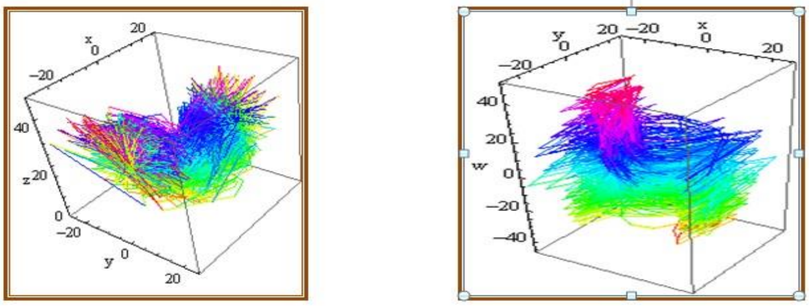


Fig.2. Chaotic attractors of novel system in three dimensions

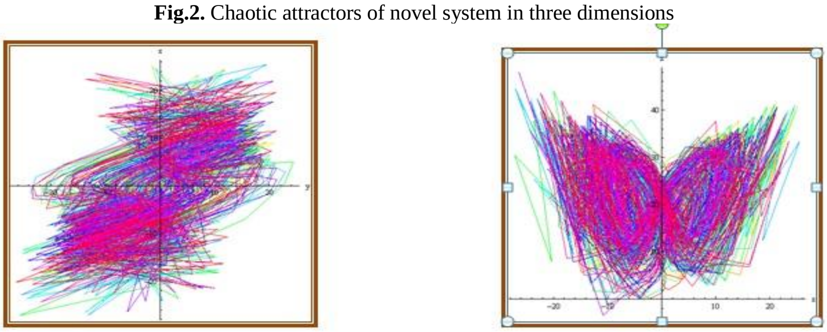


Fig.3. Chaotic attractors of novel system in two dimensions

4 Proposed encryption algorithm

The major goal of this paper is to design a strong encryption scheme depends on a hyper- chaotic system to promote the security and efficiency. Let W be the original image of size A*B*3 the enciphering operation start by generate a chaotic vectors from a new hyper- chaotic system, these vectors used to achieve a good confusion for plain image by change the pixels locations in original image to get a permuted image, this operation will implemented by use a sort operation in ascending order and swap operation between chaotic vectors and Red, Green and blue vectors of original image.in this enciphering algorithm the key that used for encrypt a permuted image is extract from a chaotic sequence , this key will encrypt each three component of a permuted image individually by use XOR operation, the encryption image will pass in two stages of diffusion to change the pixels values of image by subtract each pixel value from highest pixel value in encrypted image, in each stage the proposed algorithm is used a complement function for investigation this purpose . This encryption algorithm includes generate a magic matrix with size equal to size of image this matrix is used to create a final encryption image. The Fig.4. explains the block diagram of proposed enciphering scheme.

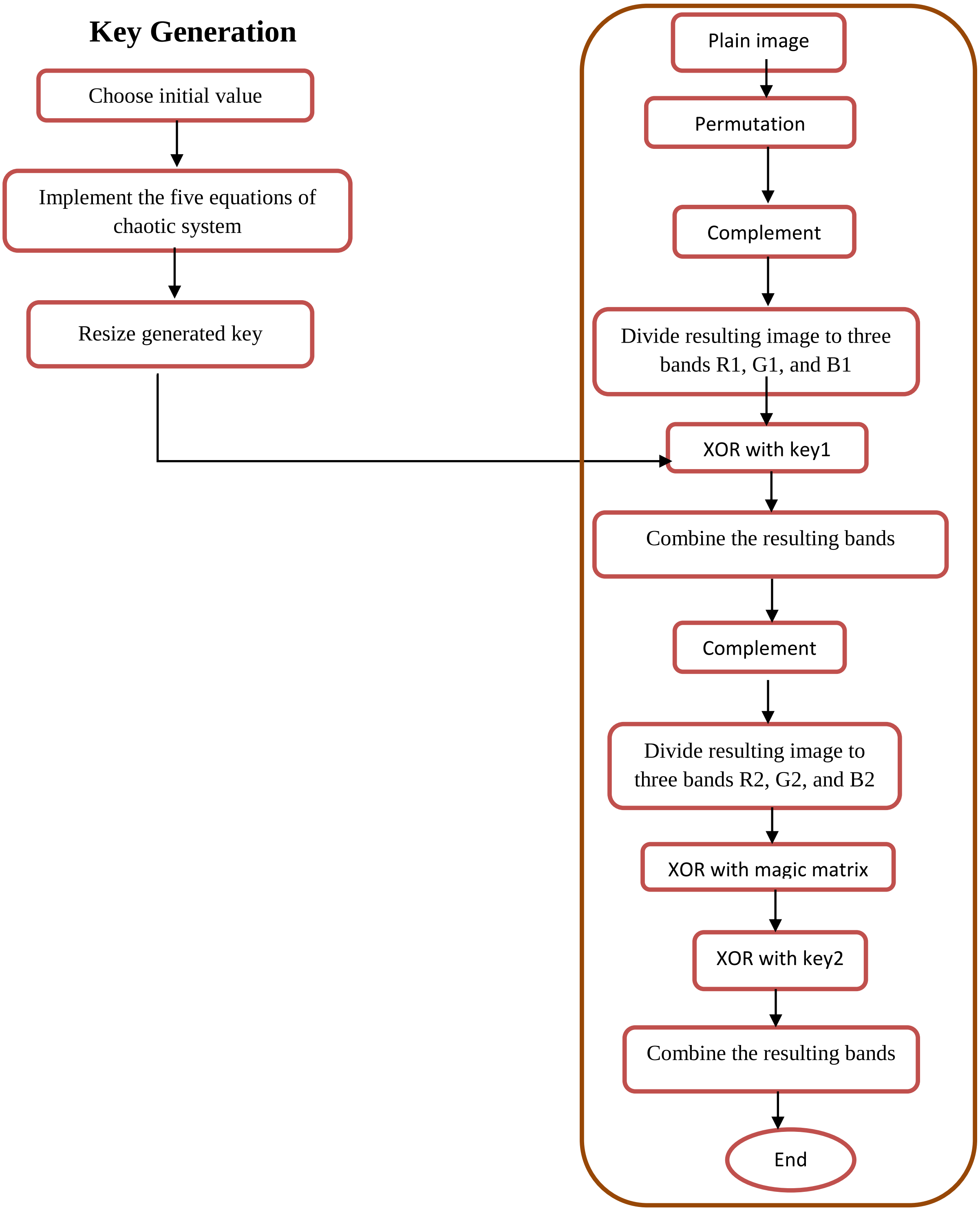
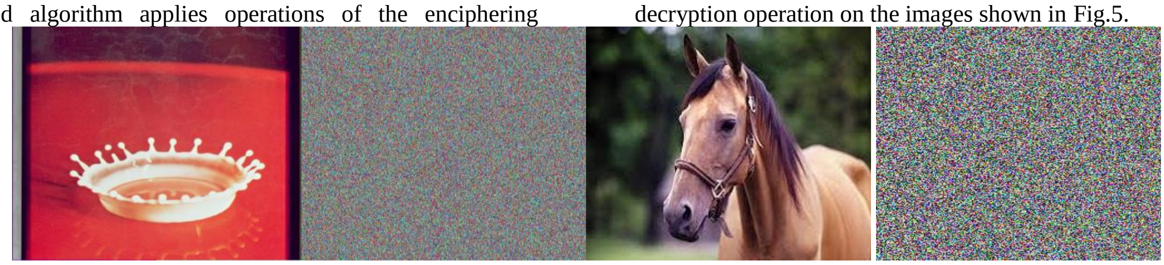

Key Generation
Choose initial value
Implement the five equations of chaotic system
Resize generated key
Plain image
Permutation
Complement
Divide resulting image to three bands R1, G1, and B1
XOR with key1
Combine the resulting bands
Complement
Divide resulting image to three bands R2, G2, and B2
XOR with magic matrix
XOR with key2
Combine the resulting bands
End

Fig. 4. Block diagram of enciphering scheme.

To restoration the original image the decryption operation of proposed algorithm applies operations of the enciphering operation in reverse order. Results of encryption and decryption operation on the images shown in Fig.5.



(a) (b)

(c) (d)

Fig.5. Use the propose algorithm for images encryption, (a) and (c) represent the plain images while (b) and (d) are the encrypted images.

5 Experimental Results of Proposed Algorithm

To estimate the security degree of the suggested enciphering algorithm some security analysis are performed to illustration that the suggested algorithm is safe versus the statistical attack and differential attack such as the distribution of pixels of the cipher images (histogram), information entropy , the correlation between the original and encrypted images, the number of pixels change rate (NPCR) ,the unified average changing intensity (UACI), PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error), Key Space Analysis, Key Sensitivity Analysis

5.1 Histogram Analysis

Histogram is a method that discovers the distribution information of pixel values of images, by graphing the number of pixels at each color intensity level. The histogram of the enciphering image must have a uniform and totally different histogram versus the original-image. From Fig.6. there is a difference between the two histogram can be observed, the histogram of enciphered image by suggested algorithm is differed from the histogram of plain image and has a uniform distribution.

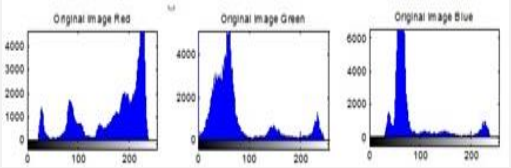
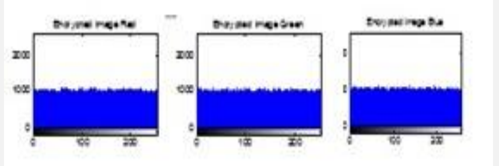
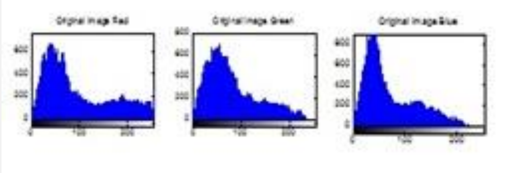
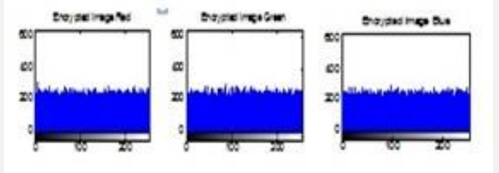
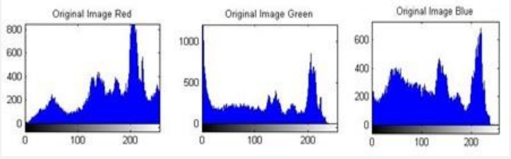
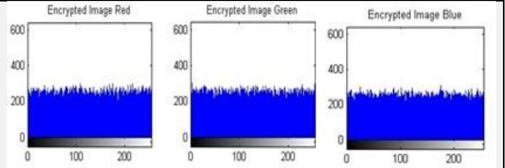
Images	Histogram for plain image	Histogram for enciphered image
Splash		
Horse		
Flower		

Fig.6. The histogram for (RGB) components for the plain image and enciphered image

5.2 Correlation Coefficients Analysis

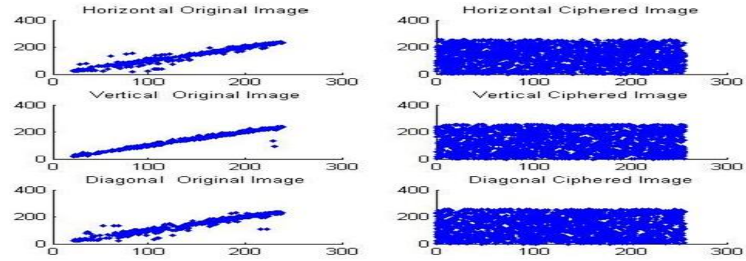
The relationship between neighboring pixels in an encrypted image should be as low as possible in order to resist correlation analysis. The correlation coefficients are calculated as follows:

$$\boldsymbol{ccr} = \frac{\sum_{im}\sum_{jn}(AA_{ijn}-\overline{AA})(BB_{mij}-\overline{BB})}{\sqrt{\left(\sum_{im}\sum_{jn}(AA_{ijn}-\overline{AA})^2\right)\left(\sum_{im}\sum_{j}(BB_{ijn}-\overline{BB})^2\right)}} \quad \textbf{(3)}$$

Where A represents original-image, B represents encrypted-image. $\bar{A}$ And $\bar{B}$ are the mean values of the elements of arrays A and B.

Table 1. The correlation coefficients for the encrypted images that were encrypted using the suggested algorithm in horizontal, vertical and diagonal directions.

images	**plain images**			**Enciphered images**		
	Horizontal	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
splash	o.9936	0.9951	0.9894	8.4562e-0.4	0.0036	-0.0020
Horse	o.9723	0.9900	0.9701	-7.8311e-04	0.0040	0.0030
flower	0.9649	0.9723	0.9525	-0.0082	0.0019	0.0018

Images	correlation coefficients for plain and enciphering images
Splash	

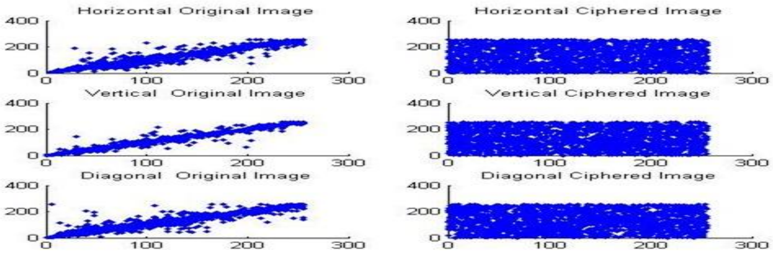
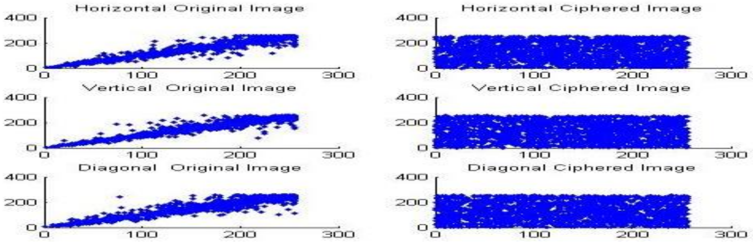
Horse	
flower	

Fig.7. Correlation coefficients for images in vertical, horizontal, and diagonal direction

5.3 Entropy Analysis

Information entropy is one of the most significant properties of randomness and it is major for an encryption planner analysis. The measurement of entropy for source n can be obtained from the following formula :

$$E = -\sum_{i=0}^{n-1} p(x_i) \times \log_2 p(x_i) \qquad (4)$$

the ideal value of entropy must be close to (8) From the Table 2., the entropy values for enciphered images near to perfect value and the presented encryption scheme have the robustness and resistant against entropy attack.

Table 2. The information entropies of cipher-images

Images	Entropy
Splash	7.9980
Horse	7.9972
Flower	7.9973

5.4 NPCR and UACI Analysis

Unified average changing intensity (UACI) and the number of pixels change rate (NPCR) are very important differential attack measurements used for valuation the sensitivity to small modifications in the plain image. These two analysis can defined as follows:

$$NPCR = \frac{\sum_{i=0}^{w-1}\sum_{j=0}^{H-1} D(i,j)}{w \times H} \times 100\% \qquad (5)$$

$$UACI = \frac{1}{w \times H}\left[\frac{\sum_{i,j} G1(i,j) - G2(i,j)}{255}\right] \times 100\% \qquad (6)$$

The outcomes for NPCR and UACI shown in Table 3., it's clearly show that all NPCR values and UACI values close to the ideal value which are (99.6093%) for NPCR and (33.464 %,) for UACI.

Table 3. The results of NPCR and UACI for encrypted image

Images	NPCR	UACI
Splash	99.6168	33.8093
Horse	99.6241	33.4042
Flower	99.6109	33.5638

5.5 PSNR Analysis

Peak Signal to Noise Ratio and Mean Square Error are more popular tests in image encryption algorithm, the lower value of PSNR of the three plains Red, Green and Blue and the high value of MSE represents better encryption quality. From the Table 4., the result values of PSNR and MSE is very appropriate for secure encryption scheme.

Table 4. The outcomes of PSNR and MSE for enciphered image

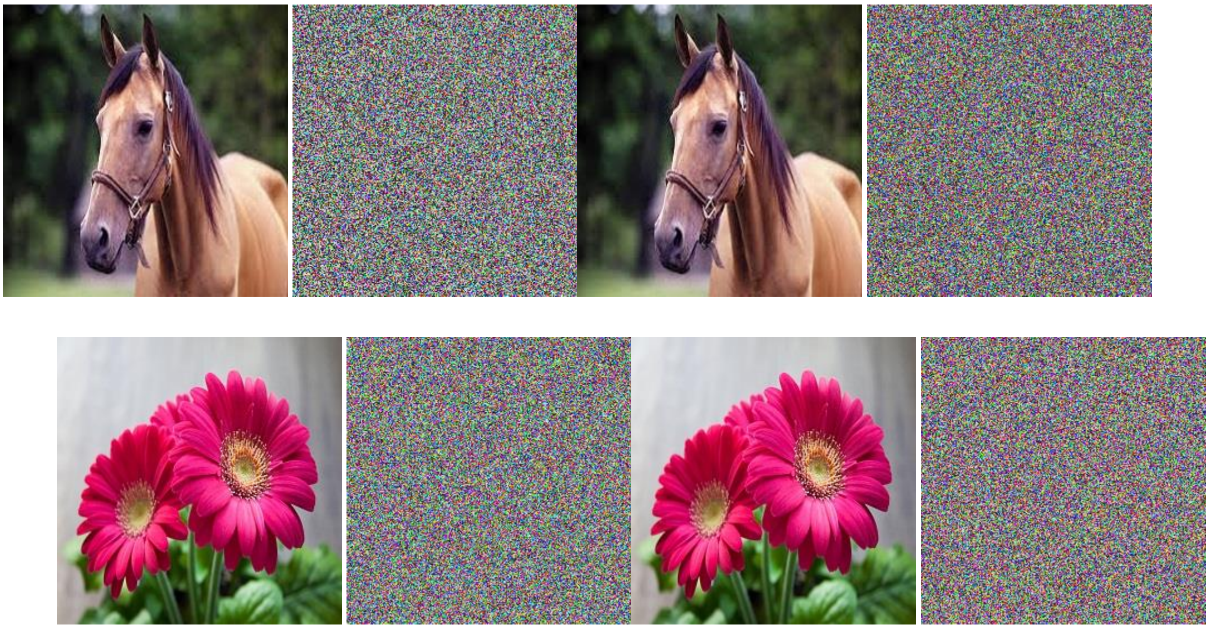
Images	**R**	**G**	**B**	**MSE**
Splash	7.5820	7.2374	8.1985	**2221.13321521**
Horse	7.6491	7.9717	7.6887	**2718.11036025**
Flower	7.86633	7.26927	8.06976	**2746.96533225**

5.6 Key Space Analysis

Size of the key space is the number of encryption/decryption key pairs that are found in the encryption system; the key space should be big enough to defeat brute-force attacks. Result key space for proposed algorithm equal to $\mathbf{(10^{182})} \approx \mathbf{2^{600}}$ and it is very large to resist brute force attacks.

5.7 Key Sensitivity Analysis

A safe encryption system must be sensitive to any tiny change in the secret key for encryption and decryption operations, the sensitivity can be observed from the changes of the decryption images with the correct key by little change. We test the key sensitivity by using initial condition (u_0) with value (0.6) change to (0.60000000000001) , with this little change in key , the original images cannot recover and the result images completely differed from plain image.



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

Fig.8. Sensitivity Analysis of Image (splash) and (flower) (a) plain image, (b) Encrypted of (a), (c) decrypted of (a) with right key, (d) decrypted with wrong key

6. Conclusions

This paper, presented a new color image encryption scheme depend on a novel 5D hyper- chaotic system .This algorithm is explained in detail. The Security analyses are employed to improve the safety of the suggested encryption algorithm. The experimental outcomes Show that the encrypted images contains uniform histogram and the entropy values were between the range **7.9972** and **7.9982,** as for the values of the NPCR , UACI are near to the perfect value which are (99.6093%) for NPCR and (33.464 %,) for UACI. Therefore, and according to these results the proposed algorithm has high security.

References

[1] H. M. Al-Najjar, Digital Image Encryption Algorithm Based on Multi-Dimensional Chaotic System and Pixels Location , International Journal of Computer Theory and Engineering, Vol. 4, No. 3, June 2012.

[2] S. Mohanty, A. Shende, K. A. K. Patro and B. Acharya, A DNA Based Chaotic Image Fusion Encryption Scheme Using LEA – 256 AND SHA – 256 ,Indian J.Sci.Res , 14 (2): 190-201, 2017.

[3] M. Kumar, A. Aggarwal and A. Garg , A Review on Various Digital Image Encryption Techniques and Security Criteria , International Journal of Computer Applications , Volume 96– No.13, June 2014 .

[4] Z. Gan , X. Chai, K. Yuan and Y. Lu, "A novel image encryption algorithm based on LFT based S-boxes and chaos , Springer Science+Business Media New York , DOI 10.1007/s11042-017-4772-0 , April 2017.

[5] I. Karydis, Multimedia - A Multidisciplinary Approach to Complex Issues , ISBN 978-953-51-0216-8 , March, 2012 .

[6] Z. Yun-peng, Z. Zheng-jun, L. Wei, N. Xuan, C. Shui-ping and D. Wei-di , Digital Image Encryption Algorithm Based on Chaos and Improved DES, IEEE International Conference on Systems, Man, and Cybernetics , San Antonio, TX, USA - October 2009 .

[7] A. Raman , Parallel processing of chaos-based image encryption algorithms, M.Sc. Thesis, University of California, Irvine, 2016 .

[8] S. A. Mehdi and H. A. Qasim, Analysis of a New Hyper Chaotic System with six cross-product nonlinearities terms , American Journal of Engineering Research (AJER) , e-ISSN: 2320-0847 p-ISSN : 2320-0936 Volume-6, Issue-5,2017, New York ,USA, pp-248-252.

[9] R.R. Kumar, A. Sampath and P.Indumathi, Enhancement and Analysis of Chaotic Image Encryption Algorithms , Computer Science & Information Technology , CS & IT 02, pp. 143–153, 2011.

[10] T. Li, M. Yang, J. Wu and X. Jing, A Novel Image Encryption Algorithm Based on a Fractional-OrderHyper-chaotic System and DNA Computing, aSchool of Economic Information Engineering, Southwestern University of Finance and Economics, 55 Guanghuacun Street, Chengdu 610074, China, October 6, 2017.

[11] C. Fu, Z. Chen, W. Zhao and H. Jiang A New Fast Color Image Encryption Scheme Using Chen Chaotic System, IEEE computer society , June , 2017.

[12] H. Yuan, Y. Liu, T. Lin, T. Hu and Li-Hua Gong, A new parallel image cryptosystem based on 5D hyper-chaotic system, Elsevier B.V., January, 2017.