Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 31, Issue 1, 2020 DOI: http://doi.org/10.23851/mjs.v31i1.739

Research Article Open Access

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

Sadiq A. Mehdi, Zaydon L. Ali*

Department of Computer Science, College of Education, Mustansiriyah University, Baghdad, IRAQ.
*Correspondent author email: zaydon_90@yahoo.com

ArticleInfo

Received
06/09/2019

Accepted
27/11/2019

Published
01/03/2020

ABSTRACT

Due to the rapid evaluation in the field of communications and multimedia and the increasing use of the Internet, multimedia data security has become very urgent. of the best alternative way to achieve multimedia data security is encryption, which prevents unauthorized entities from accessing confidential data. In recent years, the chaotic system of image encryption becomes an efficient way to encrypt images due to its high security. It has certain special properties like sensitivity to initial conditions, and control parameters, pseudorandom, ergodicity, and non-convergence etc. chaotic dynamics systems became as a promising alternative to traditional encryption algorithms. This paper presents a new algorithm for the image encryption/decryption scheme depended on a novel six-dimensional hyper-chaotic system to achieve High level of security, the chaotic sequence generated from system employ for permutation and diffusion the original image to create an encrypted image. 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, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal to Noise Ratio, The experimental results show that the algorithm has good encryption performance, large key space equals to 10^{168} and the high sensitivity for small changes in secret key which makes the algorithm immune to Brute force attacks, and it can resist the statistical attacks, therefore, the presented encryption algorithm depends on a novel hyper chaotic system is more secure against the statistical and differential attacks.

KEYWORDS: Novel six dimensional hyper-chaotic system; Image Encryption; new algorithm

INTRODUCTION

The tremendous spreading out of the communication networks has evoked increased dependency on digitized information in our society. As a result information is more vulnerable to abuse now. Today the web is going towards Multimedia data due to the development of network and multimedia technology. Multimedia data consist of image, audio, video, text, etc. The digital images become one of the most important information carriers which are helpful for biometric authentication, medical science, military, online personal photograph album, etc.[1]. Image encryption is different from text encryption [2]. Encryption one of the effective approaches to provide the security for image data and prevent unauthorized access to information, in general the traditional encryption algorithms such as Data Encryption Standard (DES), Advance Encryption Standard (AES) and Ron Shamir Adelman (RSA), are not suitable for image encryption and exhibit some drawbacks and weakness due to the special properties of image like strong correlation between adjacent pixels, bulk data capacity and high redundancy, which makes encrypted image vulnerable and helps to attack via cryptanalysis[3]. Chaos theory is a branch of mathematics that studies the behavior of complex dynamic systems which are highly sensitive to change in their parameters and give unpredictable results. There are several popular examples of chaotic systems such as Lorenz attractor, Rossler attractor, Logistic map, Henon map, Tent map, and Piecewise linear chaotic map. In general, the security of cryptography systems was built based on difficult or unsolved mathematical problems.

Chaos theory has attracted the cryptography field due to its characteristics, such as deterministic nature, unpredictability, random-look nature and its sensitivity to initial value [4]. Chaos-based cryptography depends on the dynamics of nonlinear maps or systems that are deterministic but simple. As a result, it could offer a fast and secure means for protecting data that is transmitted over communication channels such as the internet [5]. Some researchers proposed chaos-based image encryption algorithm to provide high security and efficiency, chaotic systems have many desirable cryptography features, and can achieve confusion and diffusion proprieties related with cryptographic system [6]. One dimensional chaotic map with the benefits of high effectiveness and simplicity has been widely used, such as Logistic map. On the other hand, its drawback is the small key size and low security[7]. To solve the problems mentioned above, a novel hyperchaotic system introduced, the proposed system characteristics with large key space, more complexity, high randomness, and show chaotic behavior over wide range for parameter values, proposed system based for the color image encryption scheme to enhance the security and resist attacks.

RELATED WORK

In 2012, Jianming Liu and Huijing Lv , a new six-dimensional Duffing-Lorenz chaotic algorithm and a new dynamic mapping method are presented[8]. The presented new algorithm overcomes the weakness of poor safety by using single Duffing or Lorenz chaotic algorithm. The new complex six- dimensional Duffing-Lorenz chaotic algorithm and the new dynamic mapping are more suitable for the image encryption in cryptography. In 2014, Lequan Min *et al.*, Based on the chaotic map and a chaos generalized synchronization (GS) theorem, a 6-dimensional chaotic GS system is constructed[9]. Construct a chaos-based pseudorandom number generator (CPRNG) the key stream generated via the CPRNG with the RC4 PRNG shows that the random ness of the sequences generated via the CPRNG, the key space is large enough to against brute-force attacks. An image encryption algorithm is done where $\oplus$ represents the XOR operation with the key. In 2014, Xiangjun Wu *et al.* proposes a novel color image cryptosystem based on synchronization of two different six-dimensional hyper chaotic systems. we apply the drive system to generate the diffusion matrices and scrambling ones, which are used to change the image pixel value and position, respectively. Thus the ciphered image is obtained[10]. In 2016, Xiangjun Wu *et al.* proposes a new lossless encryption algorithm for color images based on a six-dimensional (6D) hyper chaotic system and the two-dimensional (2D) discrete wavelet transform (DWT) [11]. The pixel values of the intermediate image are changed by another key stream to enhance the security. The experimental results and performance analysis have illustrated the effectiveness and high security of the proposed encryption algorithm. In 2018, Shuqin Zhu and Congxu Zhu, introduces a six-dimensional discrete chaotic systems (SDDCS) with some simple sine functions and a chaotic pseudorandom number generator (CPRNG) that is designed based on the SDDCS[12]. A stream encryptions scheme with both key avalanche effect and plaintext avalanche effect (SESKPAE) is proposed by using the random sequence generated by the CPRNG. Therefore, this algorithm has more advantages than the traditional encryption algorithm with a permutation-diffusion structure. The experimental results and security analysis show that the algorithm has the advantages of large key space, no obvious statistical characteristics of cipher text, sensitive to plaintext and keys, and able to resist chosen-plaintext attack and active attacks.

THE NOVEL CHAOTIC SYSTEM

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

$$\begin{aligned} \dot{x} &= -ax + by + cw - dv \\ \dot{y} &= ex - fxz - ge^{v} \\ \dot{z} &= -hz + xy + iv \\ \dot{w} &= -w - yz - gv \\ \dot{v} &= x + jy - iz \\ \dot{u} &= kx - Lu - jzw \end{aligned} \tag{1}$$

Where x, y, z, w, v and u called the states of system and a, b, c, d, e, f, g, h, i, j, k and L are positive parameters of the system. System 6-D (1) displays an chaotic attraction when system parameter values are selected as follows: a=9, b=11, c=0.1, d=0.3, e=30, f=2.5, g=5, h=3,

Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 31, Issue 1, 2020 DOI: http://doi.org/10.23851/mjs.v31i1.739

i=0.5, j=4, k=25 and L=15 . (2) We take the initial conditions as: x(0)=0.1, y(0)=0.5, z(0)=3.5, w(0)=0.6, v(0)=0.4, u(0)=0.1 .

This a novel six-dimensional nonlinear system. Some basic properties of the system have been investigated The novel 6-D chaotic system has three unstable equilibrium points and calculated Lyapunov exponents, the Lyapunov exponents of the system are : L1= 1.04609, L2= 0.121133, L3= 0.0260565, L4= -1.10258, L5= -13.0445 and L6=-15.0464, the maximal Lyapunov exponent (MLE) of the novel system is L1= 18.94059. In addition, the Lyapunov dimension of the novel chaotic system is obtained as DKY=4.00695.

Using mathematic program, the numerical simulation has been completed. This nonlinear system exhibits the complex and abundant chaotic dynamics behaviors; the strange attractors are shown in Figures.1-3.

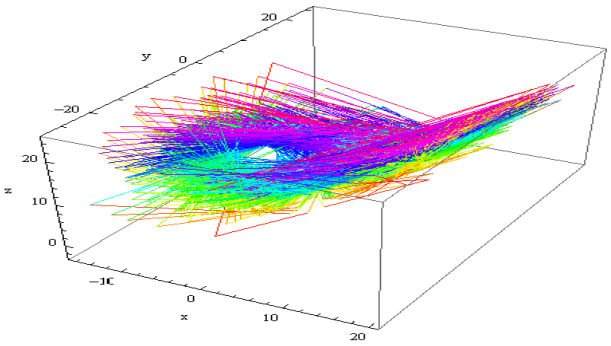


Figure 1. Chaotic attractors, 3D view (x-y-z).

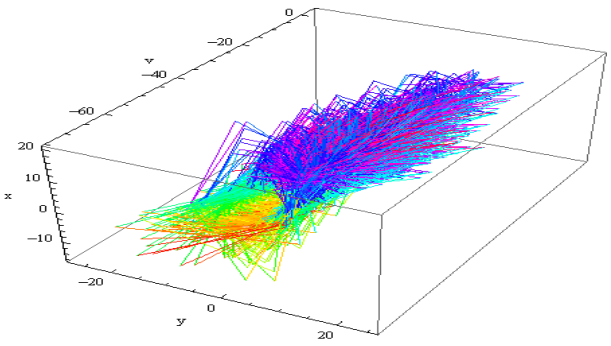


Figure 2. Chaotic attractors, 3D view (x-y-v).

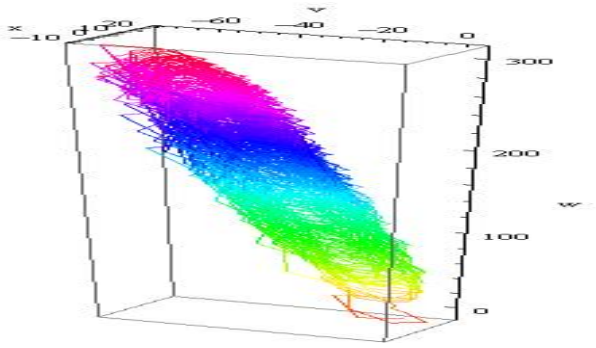


Figure 3. Chaotic attractors, 3D view (w-z-x).

A. Equilibrium Point

We can obtain that the new six dimensional (1), contains three equilibrium points when system parameter values are specified as follows: a=9, b=11, c=0.1, d=0.3, e=30, f=2.5, g=5, h=3, i=0.5, j=4, k=15 and l=25. And the nonlinear equations should be solving as follows:

$$\begin{aligned} 0 &= -ax + by + cw - dv \\ 0 &= ex - fxz - ge^{v} \\ 0 &= -hz + xy + iv \\ 0 &= -w - yz - gv \\ 0 &= jy + x - iz \\ 0 &= -ku - jzw + lx \end{aligned} \quad (2)$$

Three equilibrium points for the new hyper chaotic system acquired as follows:

E0{x=0, y=0, z=0, u=0, w=0},E1{x=0.0539309, y=-0.0367507, z=-0.186144, w=5.55766, v=-1.1129, u=0.365758},Then the eigenvalues that corresponding to equilibrium E0(0,0,0,0,0,0) are respectively obtained as follows: λ_1=-22.9838, λ_2=-15, λ_3=13.0759, λ_4=-2.92751, λ_5=-1.10293 and λ_6=0.938297.

Therefore, the equilibrium *E0*(0,0,0,0,0,0) is a saddle point, and the hyperchaotic system is unstable at the point *E*1. At the same time, it is easy to prove that the equilibrium point *E*1 is also unstable saddle points.

For equilibrium point *E1*{x = 0.0539309, y = -0.0367507, z = -0.186144, w = 5.55766, v=1.1129, u=0.365758}, and a=9, b=11, c=0.1, d=0.3, e=30, f=2.5, g=5, h=3, i=0.5, j=4, k=15, and l=25, the eigenvalues that corresponding to equilibrium point *E*1 they were obtained as:

λ_1= -23.295, λ_2=-15, λ_3=13.9395, λ_4=-2.92163, λ_5=-1.13428 and λ_6=0.411404.

Therefore, the equilibrium *E1* (0.0539309, -0.0367507, -0.186144, 5.55766,

-1.1129, 0.365758) is a saddle point. So, and the hyperchaotic system is unstable at the point $E1$.

B. Lyapunov Exponents and Lyapunov Dimensions

The new 6-D hyper-chaotic system contains six Lyapunov exponents which are:

L_1= 1.04609, L_2= 0.121133, L_3= 0.0260565, L_4= -1.10258, L_5= -13.0445 and L_6=-15.0464, since the novel hyper-chaoticthree Lyapunov exponents L_1, L_2 and L_3 are positive, and the rest three Lyapunov exponents are negative. Thus, the novel system is hyper-chaotic.The fractal dimension is also a typical characteristic of chaos calculated Kaplan-Yorke dimension by Lyapunov exponents, and DKY for the new system could be obtained follows:

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

$$D_{KY} = 4 + \frac{1.04608 + 0.12113 + 0.02605 + -1.10257}{13.0445} = 4.00965$$

This means that the Lyapunov dimension for system (1) is fractional nature and that the new system has non-periodic orbits its nearby trajectories diverge. Therefore, there is really chaos in this chaotic system.

C. Sensitivity to initial conditions

Perhaps the most distinguishing feature of a chaotic system is its long-term unpredictability. This is due to the sensitive dependence of solutions on initial conditions. Two different initial conditions, no matter how close they are, will ultimately become are widely separated. Therefore, for any given number of precision numbers in the initial condition, there will be a future time when an accurate prediction of the system status cannot be made. Figures (4, 5) presented that the development of chaos trajectories is high sensitive to initial conditions. The initial values of the system are set to: x(0)=0.1, y(0)=0.5, z(0)=3.5, w(0)=0.6, v(0)=0.4 and u(0)=0.1, for the solid line and x(0)=0.00000000001, y(0)=0.5, z(0)=3.5, w(0)=0.6, v(0)=0.4 and u(0)=0.1, for the dashed line.

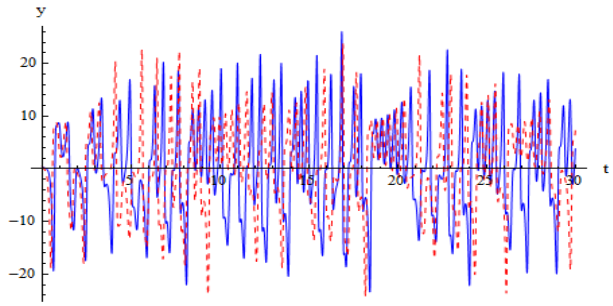


Figure 4. Sensitivity tests of the novel system x(t).

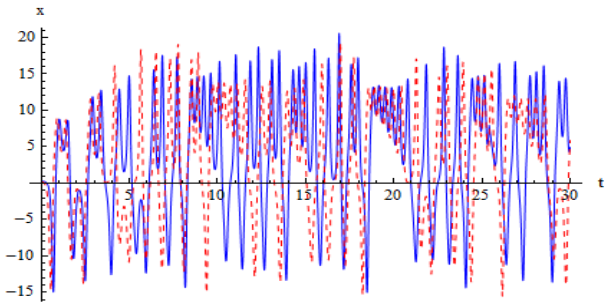


Figure 5. Sensitivity tests of the novel system y(t).

Clearly, that the waveform of system (1) is non-periodic and has a better sensitivity to the initial conditions and is called a sensitive dependence on the initial conditions.

PROPOSED ENCRYPTION ALGORITHM

In this paper illustrates design a strong encryption scheme depends on a hyper-chaotic system to enhance security and efficiency. Let I the plain image with size R*C*3 the encryption operation start by generating 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 plain image to get a permuted image, this operation will be implemented by use a sort operation in ascending order and swap operation between chaotic vectors and Red, Green and blue vectors of plain image . The Encryption algorithm consists of four stages : chaotic sequence generation , Latin square , permutation , diffusion . the encryption operation utilize Secret key to change over the colored plain image to encrypted image which has random attributes to resist statistical attacks, the plain image is encrypted with (Latin square matrix) using (bit-XOR) operation. The stage permutation incorporate scrambling the locations of encrypted image pixels in a private way, while the diffusion stage include Change the pixel values simultaneously by using (bit-XOR) operation. The Fig.6. explains the block diagram of proposed encryption scheme.

Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 31, Issue 1, 2020 DOI: http://doi.org/10.23851/mjs.v31i1.739

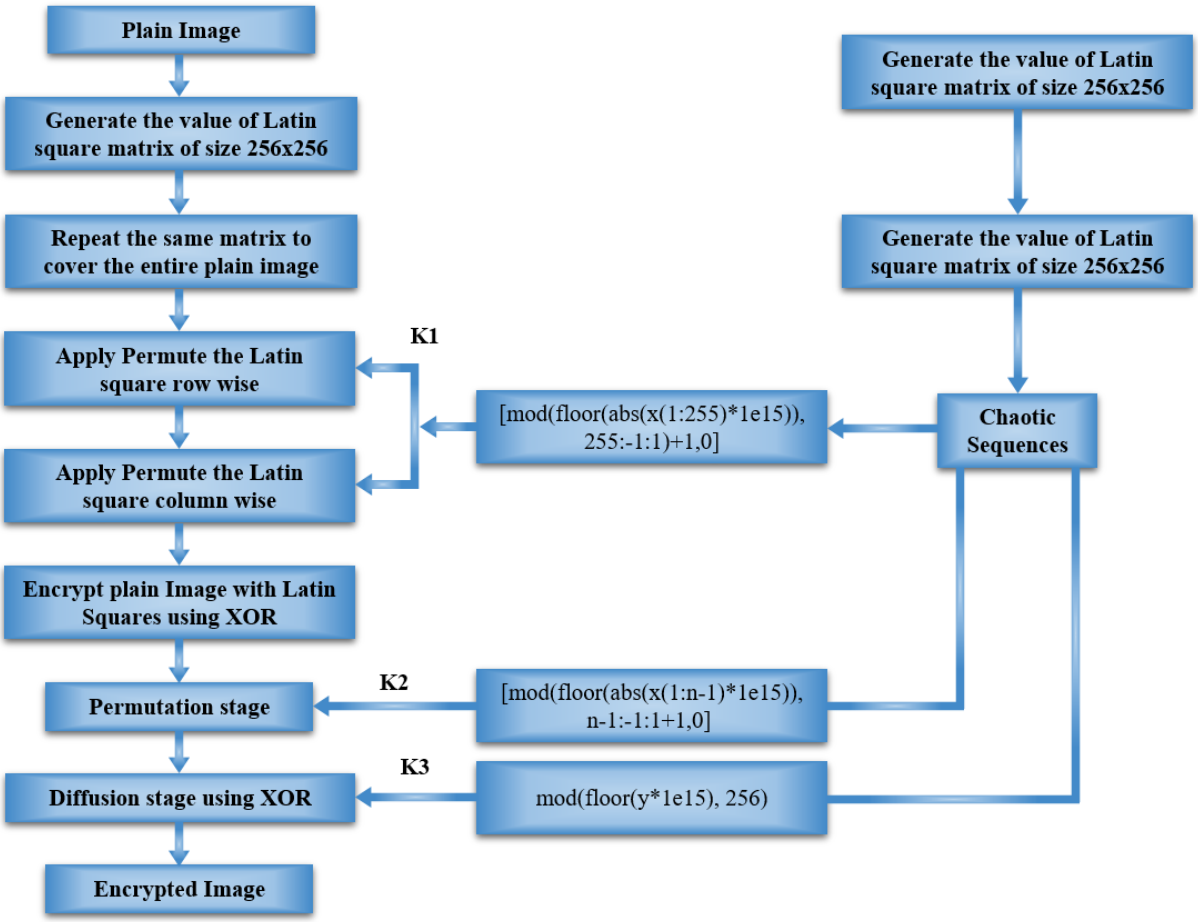


Figure 6. Flow chart of encryption scheme.

New Encryption Algorithm:

Input: colored Plain image of size M×N×3.

Secret key: Initial conditions, parameters and iteration x(0) ,y(0) ,z(0), w(0), v(0), u(0), a, b, c, d, e, f, g, h, I, j, k, L.

Output: Encrypted image of size M×N×3.

Begin

Step 1: I ← Read a plain image.

Step 2: let {r, c, d} ← size (I), Size of the plain image.

Step3: Iterate proposed hyper chaotic system with secrete key to create six chaotic sequences [{Xn}, {Yn}, {Zn}, {Wn}, {Vn}, {Un}]. // size of sequences ≥ I

Step 4: manipulate the chaotic sequences in step3 to generate three keys (k1, k2, k3) for confusion and diffusion technique.

Step 5: generate a 256×256 Latin square matrix, regardless of the size of the image.

Step 6: repeat the same matrix to cover the entire plain image

Step 7: Apply Permute the Latin square Row wise using chaotic sequence as key (k1) that obtain from proposed chaotic system.

Step 8: Apply Permute the Latin square column wise using chaotic sequence as key (k1) that obtain from proposed chaotic system.

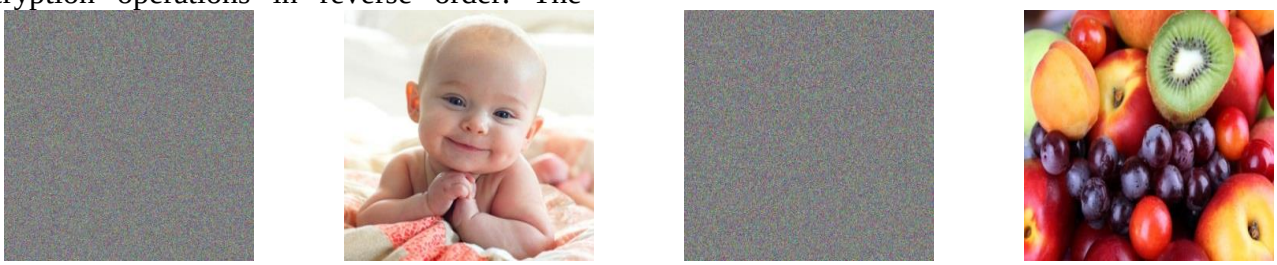
Step 9: Encrypt plain Image with Latin Squares using XOR operation.

Step 10: Appling chaotic sequence as the key (k2) to permute each component of the encrypted image randomly in step 9.

Step 11: Apply diffusion process to changing each pixel values of scrambling image in Step 10 using chaotic sequence as the key (k3) to obtain encrypted image.

End

To restore the original image, the decryption process for the proposed algorithm will run the encryption operations in reverse order. The results of the encryption and decryption process on the images shown in Figure 7.



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

Figure 7. Use the proposed algorithm for images encryption : (a) and (c) represent the plain images while (b) and (d) are the encrypted images.

SECURITY ANALYSIS

The quality of the cryptographic algorithm is examined statistically through some performance measures which include, histogram analysis, correlation between the plain and encrypted images , Information Entropy, 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.

Histogram Analysis

To prevent the extraction of important information about the plain image, should be avoided any statistical relationship between plain image and encrypted image, and to resist statistical attacks the histogram for an encrypted image should be completely flat and completely different from the plain image, which means uniform distribution on image range are random and complete. The histogram of original and corresponding encrypted images is shown in Fig.6. this Fig illustrates that histogram of encrypted image by proposed algorithm is different from the histogram of original image and completely uniform due to sturdy presented encryption scheme excellent diffusion stage.

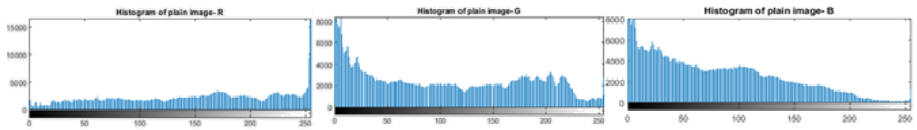
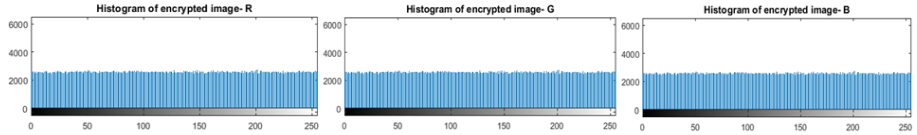
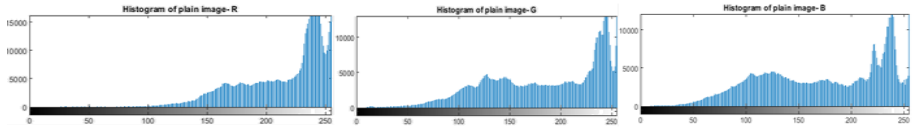
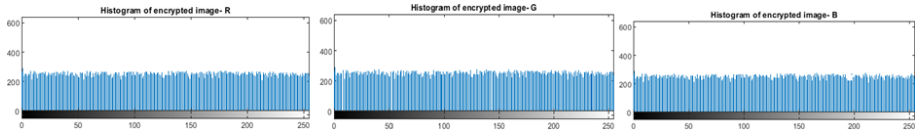
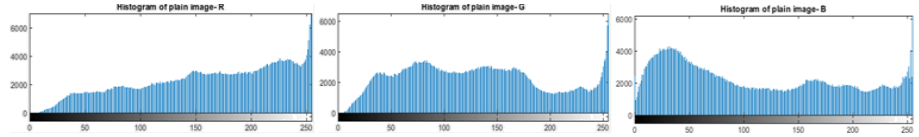
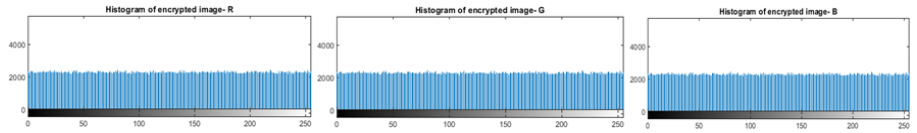
Images	Histogram		
	R	G	B
Original Fruit			
Encrypted Fruit			
Original Baby			
Encrypted Baby			
Original Tree			
Encrypted Tree			

Figure 8. The histogram for the plain image and encrypted image.

Al-Mustansiriyah Journal of Science
ISSN: 1814-635X (print), ISSN:2521-3520 (online) Volume 31, Issue 1, 2020 DOI: http://doi.org/10.23851/mjs.v31i1.739

Correlation Coefficient Analysis

One of the basic characteristics of plain image, each pixel is highly correlated with its adjacent pixels either in the horizontal, vertical or diagonal direction. Then the correlation coefficients between the adjacent pixels of an encrypted image should be close to zero in order to protect the system from statistical attacks. The correlation coefficients are calculated as follows:

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}(y_i - \bar{y})^2\right)}} \quad (3)$$

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \ , \ \bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i$$

Where x and y represent gray scale values of two neighboring pixels in the image and N is the total number of samples, the correlation value should be as close as possible to zero.

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

Image	plain images			encrypted image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Fruit	0.9952	0.9953	0.9924	-0.0001	0.0013	-0.0008
Baby	0.9983	0.9976	0.9961	0.0019	0.0003	0.0008
Tree	0.9791	0.9790	0.9639	-0.0019	-0.0019	0.0013

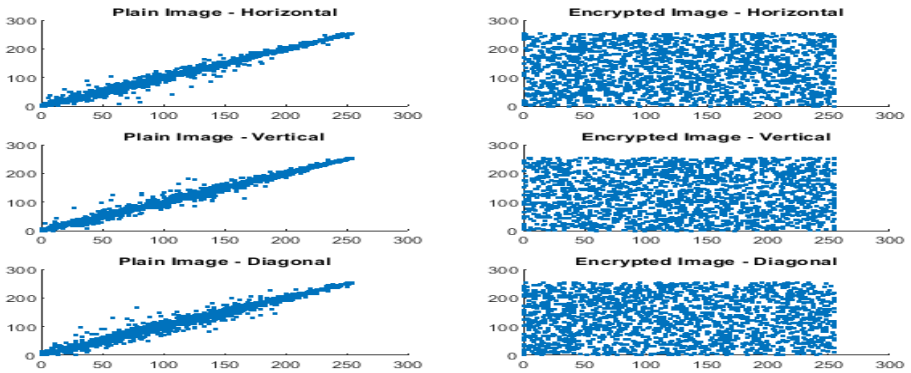
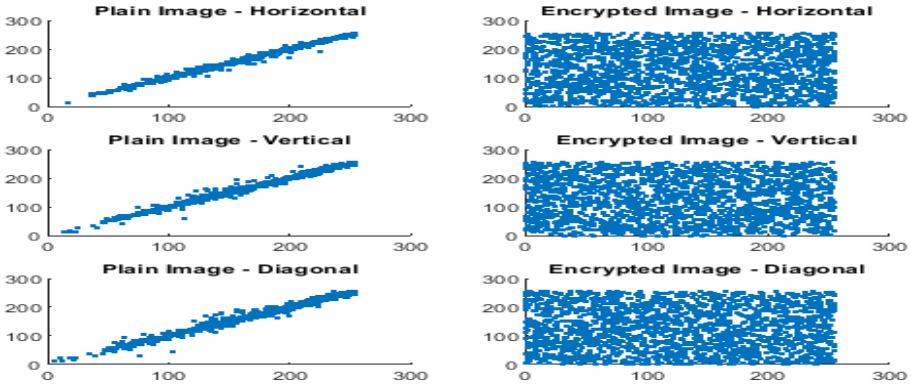
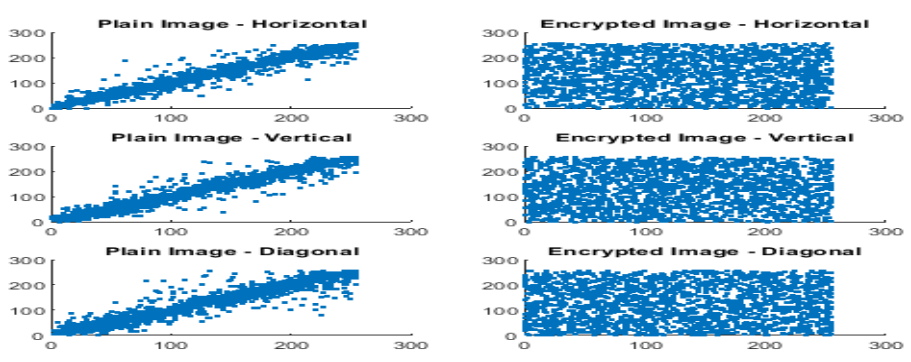
Images	Correlation coefficients for plain and enciphering images
Fruit	
Baby	
Tree	

Figure 9. Correlation coefficients for images in vertical, horizontal, and diagonal direction.

Information Entropy Analysis

Entropy information is one of the most important characteristics of randomization and is essential for analyzing the encryption scheme. The entropy measurement of source n can be obtained the following formula:

$$H(m) = -\sum_{i=0}^{N-1} P(m_i) log_2[P(m_i)] \quad (4)$$

the entropy value must be close to (8) From the Table (2), show that entropy values for encrypted images are very close to (8) and the presented encryption scheme have the durableness and resistant against entropy attack.

Table 2. Information entropies of encrypted image.

Images	Entropy
Fruit	7.99990
Baby	7.99991
Tree	7.99990

NPCR and UACI Analysis

Number of pixels change rate (NPCR) and Unified Average Changing Intensity (UACI) are the two most common quantifiers are used to measure the sensitivity of the cryptographic system to small modifications in the plain image. These two analysis can define as follows:

$$\frac{\sum_{i=1}^{w}\sum_{j=1}^{H} D(i,j)}{W \times H} \times 100\% \quad (5)$$

$$UACI(c_1, c_2) = \frac{100}{H \times W}\sum_{i=1}^{w}\sum_{j=1}^{H}\frac{|C_1(i,j) - C_2(i,j)|}{255} \quad (6)$$

Table 3 shown that all NPCR values and UACI values close to the ideal value which are greater than 99.6% and UACI is between 33.25 and 33.48%, respectively.

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

Images	UACI	NPCR
Fruit	33.4728	99.9235
Baby	33.4789	99.9475
Tree	33.4862	99.9759

PSNR and MSE Analysis

Peak Signal-to-Noise Ratio (PSNR) . PSNR One of the most important criteria in the context measuring the quality of encryption, this criterion is applied between the standard test images and their corresponding decrypted image . Mean square error (MSE) is the cumulative squared error between the plain and decrypted image, and the results presented in the Table 4 .

Table 4. PSNR and MSE values.

Images	PSNR	MSE
Fruit	∞	0
Baby	∞	0
Tree	∞	0

We denote that the value of the MSE is equal to 0, the metric indicates a good quality image for the retrieval of the decrypted image, and the PSNR values are infinity or undefined then indicates the higher similarity between plain image and decrypt image [13].

Key Space Analysis

Where key space means all possible and different key values can be used in the encryption process, and the minimum key size for encryption scheme should be at least 2^{100} (bits) to resist brute force attacks. the key space size can reach the $(10^{14})^{12}=10^{168}\approx 2^{554}$, and it is very large to resist brute force attacks.

Key Sensitivity Analysis

When a small change is applied to any one of the parameters control others without change, will result in a change in the encrypted image. Any simple change in any of the controls leads to Change the encrypted image. This can be defined from pixel to pixel difference from the encrypted image. Similarly, the decryption process also needs a valid key to decrypt the encrypted image. A small change in the key cannot provide decryption of the encrypted image. We using initial condition (x0) with value (0.1) change to (0.10000000000001) to test the key sensitivity, where with very slight differences in key cannot recover the decrypted image correctly and Fig (8) illustrate the resulted images completely different from plain image, and the presented encryption scheme has a good key sensitivity and enough ability to resisting exhaustive attacks.

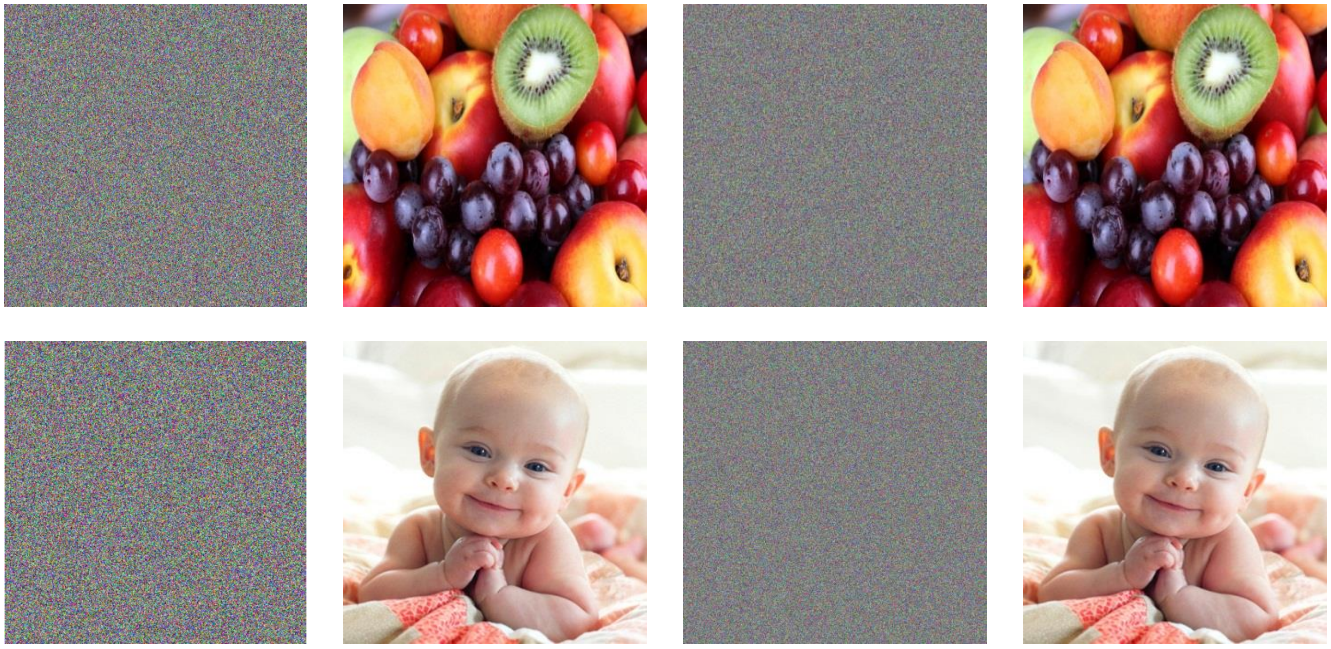


Figure 10. Sensitivity Analysis of Image (Fruit) and (Baby) (a) plain image, (b) Encrypted of (a), (c) decrypted of (a) with right key, (d) decrypted with wrong key.

CONCLUSIONS

In this paper, represent a color image encryption algorithm depended on a novel 6D hyper chaotic system Image encryption and decryption can be performed using this algorithm, The encrypted mages have excellent confusion and diffusion properties compared to other algorithms. 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, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI), Peak Signal to Noise Ratio, The experimental results show that the algorithm has good encryption performance, large key space , and it can resist the statistical attacks, therefore, the presented encryption algorithm depends on a novel hyper chaotic system is more secure against the statistical and differential attacks.

REFERENCES

[1] Srivastava, A., "A survey report on Different Techniques of Image Encryption", International Journal of Emerging Technology and Advanced engineering, Vol. 2, pp. 163-167, 2012.

[2] Kwok H. and Tang W., "A Fast Image Encryption System Based on Chaotic Maps With Finite Precision Representation", Chaos, Solitons and Fractals, vol. 32, no. 4, pp. 1518-1529, 2007.

[3] Hala Bahjat and May A. Salih, "Dynamic Shuffling for Speed Image Encryption", Volume -89, Number- 7, 2014.

[4] Maqableh, M., A.B. Samsudin, and M.A. Alia, " New Hash Function Based on Chaos Theory (CHA-1)". IJCSNS International Journal of Computer Science and Network Security 2008. 8(2): p. 20-26.

[5] Shubo Liu, Jing Sun and Zhengquan Xu, "An Improved Image Encryption Algorithm based on Chaotic System", Journal of computers, Vol. 4, No. 11, November 2009.

[6] Vishnu G. Kamat and Madhu Sharma, "Symmetric Image Encryption Algorithm Using 3D Rossler System", International Journal of Computer Science and Business Informatics, Volume -14, Number -1, 2014.

[7] Ruisong Ye and Weichuang Guo, "A Chaos-based Image Encryption Scheme Using Multimodal Skew Tent Maps", Journal of Emerging Trends in Computing and Information Sciences, Vol. 4, No. 10, October 2013.

[8] Jianming Liu and Huijing L , "A New Duffing-Lorenz Chaotic Algorithm and Its Application in Image Encryption", International Conference on Control Engineering and Communication Technology, 2012.

[9] Lequan Min et al.," A 6 Dimensional Chaotic Generalized Synchronization System and Design of Pseudorandom Number Generator with Application in Image Encryption", Tenth International Conference on Computational Intelligence and Security, 2014.

[10] Xiangjun Wu, Chenxi Bai and Haibin Kan, " A new color image cryptosystem via hyperchaos synchronization", Commun Nonlinear Sci Numer Simulat, 2014.

[11] Xiangjun Wu, Dawei Wang *et al.*, " A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system", Information Sciences, 2016.

[12] Shuqin Zhu and Congxu Zhu, " Image encryption algorithm with an avalanche effect based on a six-dimensional discrete chaotic system ", Multimed Tools Appl, part of Springer Nature, 2018.

[13] 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.