Secure Image Encryption Method Using Hyperchaotic Systems

Hayder Abbood Qasim

Al-Mustansiriyah University, College of Education, Department of computer science, Baghdad, Iraq

Abstract: ***With increase exchange of sensitive multimedia data like text, video, voice, image over unsecure networksand to meet the real time constraints, secure and efficient image encryption scheme becomes more and more urgent need to provide the desirable confidentiality and thwart attacks, in this paper a secure image encryption method is proposed, based on fast generation of large keys from two hyperchaotic systems to permuted and mask the plain image with the purpose of get the advantages of these systems, at the permutation step the chaotic numbers generated from systems utilized to shuffling rows and columns of image, will in diffusion step the image is split to 2 sup-images and each part XOR with chaotic mask generated from distinct hyperchaotic system, he main features of such method are high speed, large key space and low computational overhead, as well the experimental results demonstrate that the proposed method have more ability to thwart different attacks such as statistical, differential, entropy attack, and brute-force attack.***

Keywords: Hyperchaoc, Initial conditions, Histogram, Correlation

1. Introduction

Due to rapid advancement in the multimedia information and internet, ensure the security of information becomes more and more urgent demand, [1] digital image in different with text has many intrinsic characteristic's such as strong correlation among pixels, bulk capacity data and high redundancy, such properties make traditional encryption algorithms like Data encryption standard (DES), advanced encryption standard (AES) and Ron Shamir Adelman (RSA), are poorly suited to image encryption and show some disadvantages [2], to meet the increase demand for more secure and efficient cryptosystem, many different encryption technologies have been introduced, among them chaos based scheme was one of the optimal approach that can fulfillment the desirable secrecy and efficiency, the first who was proposed chaos based encryption scheme, Fridrich in 1997[3], many low dimension chaotic maps adopting for image encryption, due to simple structure and high speed for generating chaotic sequence, two serious security problems associated with used of such maps for encryption, in order to limiting range of chaotic behavior and small key space [4].

To overcome such problems and improve the security of image encryption schemes, some researchers suggested employ high dimension hyperchaotic systems that characteristics with more than one positive Lyapunov exponent, and complex chaotic behavior which lead to more randomness and large key space[5]-[10].

2. Proposed Image Encryption method

2.1Hyperchaotic systems

In our proposed encryption method, hyperchaotic sequences generated from two different hyperchaotic systems utilized, Rosslerhyperchaotic system used in cryptography is described as follows [11]:

$$\begin{aligned} \dot{x}&=-y-z, \\ \dot{y}&=x+ay+w, \\ \dot{z}&=b+xz, \\ \dot{w}&=-cz+dw, \end{aligned} \qquad (1)$$

The system (1) show the hyperchaotic behavior when the control parameters values chosen as: a= 0.25, b=3, c=0.5, d=0.05, and initial conditions taken as (-10, -6, 0, 10).

In addition, another new hyperchaotic system used given by the following equations [12]:

$$\begin{aligned} \dot{x}&=y-xz-yz+w, \\ \dot{y}&=axz+d, \\ \dot{z}&=y^2-bz^2, \\ \dot{w}&=-cy, \end{aligned} \qquad (2)$$

When the values of real parameters a=5, b=0.28, c=0.05, d= -0.001 and the initial conditions selected as (0, 0, 0.8, 0.02), the system (2) display hyperchaotic attractor.

2.2 Image encryption

In this paper, color plain image employ which is h×w×3 and denoted by p, the image composed of three bands R, G, B, each of size h×w×1, the detailed encryption procedure described as follows:

Step1: Iterate the system (1) and system (2) with the values of control parameters and initial conditions, after many rounds we can get two chaotic sequences $s, \acute{s}$, say $\{s_m$, m=1, 2…, h×w}, $\{\acute{s}_n$, n=1, 2…, h×w}, where h, w are the height and the width of p.

Step2: Truncate $\acute{r}$ vector from s and c vector from $\acute{s}$, where $\{\acute{r}_k, k = 1,2 \dots, h\}, \{c_g, g = 1,2.., w\}$, Sort $\acute{r}_k, c_g$ in increase order manner, use I$\acute{r}_k$, Ic_g to denote the positional index of the corresponding elements in unsorted vectors $\acute{r}_k, c_g$.

Step3: Apply row and column permutation, use I$\acute{r}_k$ and Ic_g in step2 to rearrange the rows, columns of matrix (R, G, B) respectively to get the scrambled image.

Step4: Modify each element of chaotic sequence $s, \acute{s}$using the following formula:

$$x = mod\ (\ ceil\left((x \times 10^{14}) \div 512\right), L) \qquad (3)$$

Where $ceil(i)$ returns the nearest integer less than or equal to i, and L represent the largest gray level for image and $mod\ (x, y)$ returns the remainder after division.

Step5: Reshape each chaotic sequence $s, \acute{s}$in step1 to two-dimensional array of size h×w×1, divide the three matrices (R, G, B) in step3 horizontally.

Step6: Perform XOR between the first part of (R, G, B) and the chaotic masks s employ the following formula:

$$\acute{G}(i) = \{G_1(i) \oplus S(i)\} \oplus S(j)(4)$$

$\acute{R}(i) =$

$\acute{B}(i) =$

Step7: Apply formula (4) in step5 to encrypt the second part of image, use the chaotic mask $\acute{s}$.

Step8: Combine the three two-dimensional images ($\acute{R}, \acute{G}, \acute{B}$)into a three-dimensional Image to get the encrypted image.
The decryption process is similar to that of the encryption process in the reverse order.

3. Experimental Results

The main measure for the quality of any cryptosystem is capability to thwart and resist the attempts of attackers or opponent to learn about the original information, some security analysis has been performed on the proposed encryption method to ensure its robustness and resistance against different attacks including, histogram analysis, correlation coefficient analysis, key space analysis, differential analysis and speed performance, the analysis have been done for many images, where Lena color image of size 256*256*3 is considered as plain image, the results show that the proposed method has high security characteristics and more resist attacks, as discussed in the following:

3.1 histogram analysis

For good cryptosystem the histogram of encrypted image must be vague and prevent extract any useful information about statistical nature for plain image to thwart statistical attack and know-plain text attack, the results show that the histogram for all encrypted images uniform or same flat in different with that for plain image and demonstrate there is no relationship with plain images [13], as show bellow:

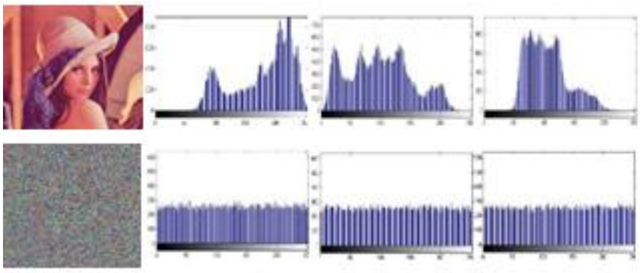

Figure 1: Histogram for plain image (Lena) and corresponding encrypted image. (**a**)–(**c**) plain R, G and B images, respectively; (**d**)–(**f**) Histograms of the cipher R, G and B images, respectively.

3.2 Correlation Coefficient Analysis

One of the dominant feature of images is a high correlation between adjacent pixels in vertical, horizontal and diagonal direction, and to block the attempting for speculated the values for neighbor pixel, for encrypted image the correlation must be reduce to ideal value zero, the correlation coefficient for two neighboring pixels can be calculated by the formula: [14]

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i-\acute{x})(y_i-\acute{y})}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i-\acute{x})^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}(y_i-\acute{y})^2\right)}} \qquad (5)$$

$$\acute{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (6)$$

$$\acute{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \qquad (7)$$

Where N is the total number of samples and x, y represent grayscale values for two neighboring pixels, the correlation calculated for horizontally, vertically and diagonally adjacent pixels Figure 2 and Table 1, show the correlation for plain image and encrypted image, where the correlation for plain image close to 1 and for encrypted image close to ideal value (zero).

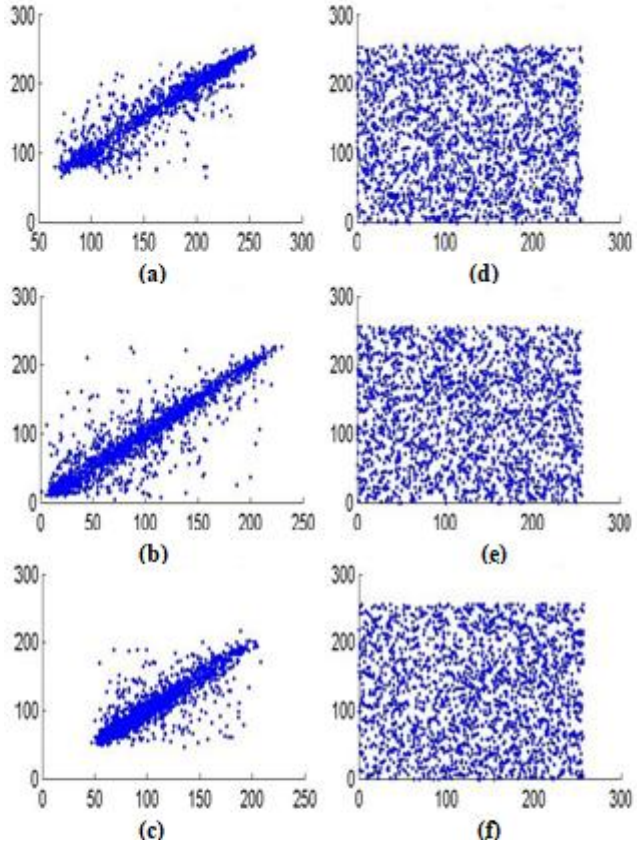

Figure 2: Horizontal correlation for (Lena) plain image and corresponding encrypted image, **(a)-(c)** Horizontal correlation for plain R, G and B images respectively and **(d)-(f)** Horizontal correlation for corresponding cipher R, G and B images respectively.

Table 1: Correlation for plain R, G and B bands

Bands	*Direction*	*Plain image Lena*	*Proposed algorithm*	*Ref [5]*	*Ref [10]*
R band	Horizontal	**0.9444**	**-0.0014**	**0.0085**	**-0.0025**
	Vertical	**0.9705**	**0.0006**	**0.0079**	**0.0913**
	Diagonal	**0.9219**	**0.00004**	**0.0167**	**0.0011**
G band	Horizontal	**0.9203**	**-0.0011**	**-0.0157**	**0.0058**
	Vertical	**0.9562**	**-0.0039**	**0.0002**	**-0.0372**
	Diagonal	**0.9000**	**-0.0042**	**0.0081**	**-0.0014**
B band	Horizontal	**0.8771**	**-0.0040**	**0.0054**	**-0.0058**
	Vertical	**0.9178**	**-0.0001**	**0.0072**	**0.0036**
	Diagonal	**0.8614**	**-0.0019**	**0.0034**	**0.0002**

From data listed in Table 1 it is clearly show that the plain image has highly robust correlation, while for encrypted image the correlation is reduced and very close to zero due to desirable cryptography characteristics for proposed method.

3.3 Differential attack analysis

To thwart differential attack and make it practically useless, any change in plain image even with one-bit must lead to completely different encrypted image and such encryption method can characteristics with desirable security features against differential attack, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are two important criteria used for analyzed, and expressed by the following: [15]

$$NPCR = \frac{\sum_{ij} D(i,j)}{M \times N} \times 100\% \quad (8)$$

$$UACI = \frac{1}{M \times N}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \quad (9)$$

Where
$D(i,j) = 0 \; if \; C_1(i,j) C_2(i,j); otherwise, D(i,j) = 1.$

Table 2: NPCR and UACI for various encryption algorithms

Algorithm	*NPCR*	*UACI*
Proposed	99.6292	30.4554
Ref [5]	99.6013	33.4134
Ref [8]	99.61	33.46

Data listed in Table 2 indicate that the NPCR and UACI for proposed method could effectively thwart differential attack in comparison with some existing algorithms.

3.4 Key space

The key space is the whole number of different and possible keys that can be employ for encryption method, the secrete key represented by initial conditions for the two hyperchaotic system used, if the precision 10^{-14} for each one, then the key space calculated as $(10^{14})^8 \approx 2^{370}$, it is clearly show that the key space for proposed method large enough to thwart all types of brute-force attacks.[16].

3.5 Encryption and decryption speed

In real-time multimedia applications fast processing requirement is important issue to evaluate the efficiency of algorithms, execution time for encryption and decryption should be as lower as possible, the time analysis done on Matlab2013a under Windows 7 ultimate (64-bit) using a personal computer Intel(R) Core(TM) i7 @2.67GHz CPU and 4GB RAM, Table 3 show that the proposed method consuming less processing time for different image size and more appropriate for real time applications.

Table 3: Encryption and decryption time

Image	*Encryption time (sec)*	*Decryption time (sec)*
Baboon (500*480)	0.0563	0.0571
F16 (512*512)	0.0635	0.0652
Lena (256*256)	0.0165	0.0158
Pepper (512*512)	0.0611	0.0612

4. Conclusion

In this paper, an image encryption method is introduced, which utilized two hyperchaotic systems to permute and mask the plain image, with purpose of overcome disadvantages or drawbacks of some chaotic encryption method that represented by small key and weak security, the row and column of image will permute using the chaotic sequence generated from systems and then the image divide to 2-sub image, each part mask with different chaotic sequence numbers, from the experimental results it's found that the histogram for encrypted images flat and no relationship with that for plain image, and the correlation for encrypted image very close to ideal value zero, while the NPCR and UACI values closely matching with the existing methods, the proposed method more suitable to real time applications and characteristic's with large key space.

References

[1] Kumar Gulshan, Pandey Praveen, Saha Rahul and RaiMritunjay, Chaotic Image Encryption Technique based on IDEA and Discrete Wavelet Transformation, Indian Journal of Science and Technology, Vol 9, No 15, April 2016.

[2] Soumya Paul, PranjalDasgupta, PrabirKr.Naskar and AtalChaudhuri, Secured image encryption scheme based on DNA encoding and chaotic map, International Information and Engineering Technology Association, Vol 4, No 2, June 2017.

[3] MoussaFarajallh, RawanQumsieh and SamerIsayed, Selective Hybrid Chaotic-Based Cipher for Real-Time Image Application, The Tenth International Conference on Emerging Security Information, Systems and Technologies, 2016.

[4] Xiaoheng Deng, Chunlong Liao, Congxu Zhu and Zhigang Chen, A novel image encryption algorithm based on hyperchaotic system and shuffling scheme, IEEE International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous computing, 2013.

[5] Xia Huang, Tiantian Sun, Yuxia Li and Jinling Liang, A Color Image Encryption Algorithm Based on a Fractional-Order Hyperchaotic System, Entropy, Vol. 17, 2015.

[6] M. Bala Kumar, P. Karthikka, N. Dhivya, and T. Gopalakrishnan, A Performance Comparison of Encryption Algorithms for Digital Images, International Journal of Engineering Research & Technology, Vol. 3 Issue 2, February 2014.

[7] ShaheenAyyub and Praveen Kaushik, Secure Searchable Image Encryption in Cloud Using Hyper Chaos, The International Arab Journal of Information Technology, Vol. 16, No. 2, March 2019.

[8] Yueping Li, Chunhua Wang and Hua Chen, A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, Optics and Lasers in Engineering, Vol. 90, 2017.

[9] Alia Karim Abdul Hassan, Proposed Hyperchaotic System for Image Encryption, International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016.

[10] Peng Li, JiXu, Jun Mou and Feifei Yang, Fractional-order 4D hyperchaoticmemristive system and application in color image encryption, EURASIP Journal on Image and Video Processing, 2019.

[11] JafarBiazar, TaherehHoulari and Roxana Asayesh, ”Implementation of multi-step differential transformation method for hyperchaoticRossler system”, International Journal of Applied Mathematical Research, Vol 6 No 1, 2017.

[12] Viet-Thanh Pham, Christos Volos, SajadJafari and Xiong Wang, Generating a novel hyperchaotic system out of equilibrium, Vol. 8, No. 5-6, May - June 2014.

[13] G.A.Sathishkumar, k.Bhoopathybagan and N.Sriraam, Image Encryption Based on Diffusion and Multiple Chaotic Maps, International Journal of Network Security & Its Application, Vol.3, No 2, March 2011.

[14] Jean De DieuNkapkop, Joseph Yves Effa, Jean Sire Armand EyebeFouda, MohamadouAlidou, Laurent Bitjoka and Monica Borda, “ A Fast Image Encryption Algorithm Based on Chaotic Maps and the Linear Diophantine Equation “, Computer Science and Applications, Vol 1, N 4, 2014.

[15] QaisH.Alsafasfeh and AoudaA.Arfoa, Image Encryption Based on the General Approach for Multiple Chaotic Systems, Journal of Signal and Information Processing, Vol.2, 2011.

[16] Tao Song, A Novel Diffusion Approach with Chen System for Chaotic Cryptosystems, International Journal of Advancements in Computing Technology, Vol.4, No 20, 2012.