Proposed Hyperchaotic System for Image Encryption

Asst. Prof. Dr. Alia Karim Abdul Hassan
Computer Science Department, University of Technology/ Baghdad

***Abstract*—This paper presents a new hyper chaos system based on Hénon and Logistic maps which provides characteristics of high capacity, security and efficiency. The Proposed hyper chaos system is employed to generate the key for diffusion in an image encryption algorithm. The simulation experiments to the image encryption algorithm which based on the proposed hyper chaos system show that the algorithm security analysis it has large key space (10^{84} that ensures a strong resistance against attack of exhaustion as the key space will be greater), strong sensitivity of encryption key and good statistical characteristics. Encryption and decryption time is suitable for different applications.**

***Keywords*—hyperchaos; logistic map; Hénon map; image; encryption; decryption**

I. INTRODUCTION

Multimedia communications; such as, images audio, and video has become significantly more important, since communications of digital products over the network (wired/wireless) has expanded [1,2]. There is therefore, an increasing need to secure data and its transmission and also to identify the required levels of security depending on the purpose of the communication. A wide variety of cryptographic algorithms have been proposed to meet these requirements. Traditional ciphers methods are less efficient in securing real-time multimedia data encryption systems and exhibit some drawbacks and weakness in high stream data encryption[3,4]. The availability of a high computation machine may allow a brute force attack against these types of cipher. Furthermore, for cryptosystem applications that require high computation processes; large computational time and high computing power, as in the encryption of large-scale image encryption are seen to suffer from low efficiency levels [5]. Therefore, these encryption algorithms are not appropriate for many high-speed applications because of their slow real-time processing speed and some other issues related to the processing of different data formats. Current research into the development of new chaotic or hyperchaotic systems is highlighting the benefits of real-time encryption and communication applications. They show that chaotic systems are good schemes for designing cryptosystems, which have preferable characteristic [6]. Within this research a hyperchaotic system is proposed using a one-dimension logistic chaotic system and three-dimension Hénon chaotic system. The proposed hyperchaotic system is applied on image encryption.

II. CHAOSE THEORY

Chaos Theory has been a branch of mathematics that has generated much interest; the notion of being able to describe complex nonlinear phenomena, such as the weather or the stock market, using a series of deterministic dynamical equations is intriguing for many fields of study. The ability to generate 'chaotic', unpredictable data using a series of relatively simple deterministic equations is also attractive from a cryptographic point of view [7].

A. Logistic map

Logistic map is a very simple chaotic map and its mathematical expression formula is asin equation (1):

$$X_{n+1} = \mu X_n(1-X_n) \quad (1)$$

$\mu \in [0, 4]$ is called Logistic parameters.

When $\mu \in [3.569946, 4]$, Logistic map works in a chaotic state and produces non-periodic sequence [8]. The map is quadratic and thus nonlinear with equation(2):

$$X_{n+1} = bX_n (1 - X_n) \quad (2)$$

Where b is the control parameter governing the chaotic behavior and to ensure X_n in the range [0, 1], parameter b has to be in the range [0, 4].

B. Hénon map

The Hénon map is one of the discrete dynamical systems that exhibit chaotic behaviors. The Hénon map is defined by two equations and depends on two parameters *a and b*, and the system exhibits a strange attractor for a = 1.4 and b = 0.3 (system equation (3)). A Hénon map takes one point (x, y) and maps this point to a new point in the plane [9,10].

$$\left.\begin{aligned} X_{n+1} &= 1 - a\,(X_n)^2 + Y_n \\ Y_{n+1} &= b\,X_n \end{aligned}\right\} \quad (3)$$

The Hénon map is very sensitive to initial values, and different chaotic sequences with large translation can be generated by the adjustment of parameters and initial values indicating that is suitable for generation of cryptographic functions, due to the capability of generating massive chaotic sequences; and the is a periodic and non-convergent, so it has excellent pseudo randomness and unpredictability.

Three-dimensional Honen map as it refers to system equation (4).

$$\left.\begin{aligned} x_{n+1} &= a - y_n^2 - b\,z_n \\ y_{n+1} &= x_n \\ z_{n+1} &= y_n \end{aligned}\right\} \quad (4)$$

The Hénon map generated from this chaotic attractor is more complex than the maps from other chaotic attractors; when $1.54<|a|<2$, $0<|b|<1$.

III. Proposed Three Dimensions Hyperchaotic System

In this work the hyperchaotic system (hyper between 1D Logistic and 3D Hénon map) is employed to generate the key space which will be greater if generated using either one. The proposed hyperchaos system is described by system equation (5). Chaotic behavior of the proposed system when the parameters are **(a=1.6, b=0.2, μ=3.75)**. The proposed hyperchaotic (Hénon and Logistic) provide the high-dimensional hyperchaotic system which is more complex and unpredictable; through more 'chaotic sequences.' y_{n+1} in system equation 4 of henon chaos system can be computed by using equation 2 of the logistic map and the resulting system which represent the proposed hyperchoas shown in system equation 5:

$$\left.\begin{aligned} x_{n+1} &= a - y_n^2 - b\,z_n \\ y_{n+1} &= bX_n(1-X_n) \\ z_{n+1} &= y_n \end{aligned}\right\} \quad (5)$$

IV. Image Encryption Using Proposed Hyperchaos System

The proposed hyperchaos system is now used in the design of an image encryption algorithm. The proposed image encryption algorithm input is a plain image whilst the output is an encrypted one. The algorithm main steps are:

Step1. Transformation Process.

In this stage the plain image is divided into 8×8 non overlapping blocks that are transformed using 2-D (DCT). The embedding will be performed in YCrCb color space. Then split luminance (y) of image into 8×8 block the 2-Dimension Discrete Cosine Transform (DCT) will be applied on to these blocks, then a quantization process by Quantizing DCT coefficients to the nearest integer value. Cosine Transform(DCT) will be applied to on these blocks by equation (6) [11],

$$\left[G_{ij} = \frac{1}{4} C_i C_j \sum_{x=0}^{7} \sum_{y=0}^{7} p_{xy} \cos\left(\frac{(2x+1)i\pi}{16}\right) \cos\left(\frac{(2y+1)j\pi}{16}\right) \right] \quad (6)$$

Where $C_f = \begin{cases} \frac{1}{\sqrt{2}}, & f = 0, \\ 1, & f > 0 \end{cases}$

where C_f is C_i, C_j and P_{xy} are the values of image component $i,j = 0,1,...,7$, $x,y = 0,1,\ldots,7$.

Quantization process by using equation (7) [12]

$$q(i,j) = INT[\, f(x,y) / qm(i,j)] \quad (7)$$

Where

INT : rounding to the nearest integer.

$qm(i,j)$: Coefficient of inter and intra matrices.

$q(i,j)$: Final output of quantization process.

$f(x,y)$: DCT coefficients.

Step2. Diffusion key generation based on discrete hyperchaotic system generator (hyper between Logistic and Hénon map), *k*ey diffusion generated in two stages

step2.1 Pre-iterate equation system (5) for *N* times (number of iteration), where *N* is a constant. For computing the solutions of the equation system (5)

step2.2: The hyperchaotic system is iterated discretely. For each iteration, we can obtain three key stream elements from the current state of the hyperchaotic system according to the following formula:

$X_n = mod\ ((abs\ (x_n) - floor\ (abs\ (x_n))) \times 10^{14},\ 256)$
$Y_n = mod\ ((abs\ (y_n) - floor\ (abs\ (y_n))) \times 10^{14},\ 256)$
$Z_n = mod\ ((abs\ (z_n) - floor\ (abs\ (z_n))) \times 10^{14},\ 256)$

Where

N times (number of iteration) of the hyperchaotic system.

abs(x_n) returns the absolute value of *X*.

Floor(x) returns the value of x to the nearest integers less than or equal to X,

mod(x, y) returns the remainder after division.

The output from this stage three key (k1, k2, k3) for each iteration time (N) used to encrypt first (Dc,2AC) for each block.

Step3. Diffusion process

Diffusion process (change value of pixels) is where a selective encryption approach is applied on DC and the first two AC coefficients. Those coefficients are selected from each block and then encrypted using one key of three generated keys by the hyperchaotic system, the selection is made using the following formula:

$X_n = mod\ (X_n, 3),\ Y_n = mod\ (Y_n, 3),\ Z_n = mod\ (Z_n, 3)$

the key sequence that is used to perform encryption operation is selected randomly. The encryption operation according to equation (8):

$$C(n) = P(n) \oplus S(n) \quad (8)$$

Where

C:cihered image value
P:plain image value
S:one of the generated key(X_n, Y_n, Z_n)

The process does not end until the set P = {DC, AC, AC} is all encrypted. Then the encrypted pixel set C = {C (1), C (2)...C (M × N)} is written to the cipher-image.

Step4. The Inverse of DCT (IDCT) and Transform Y'CrCb to RGB color

After finishing selective image encryption (diffusion) of each block, the IDCT is applied using equation (9) [11] to transform the image to spatial domain then, *Transform Y'CrCb to RGB color.*

$$p_{xy} = \frac{1}{4} \sum_{i=0}^{7} \sum_{j=0}^{7} C_i C_j G_{ij} \cos\left(\frac{(2x+1)i\pi}{2N}\right) \cos\left(\frac{(2y+1)j\pi}{2N}\right) \quad (9)$$

Where Ci, C_j as indicated by eq. (6).

Step5: Return the encrypted image

The decryption algorithm is similar to the encryption algorithm. It is for the encrypted image, firstly, decrypt the image using hyperchaotic system with the same parameters and initial values as that used in encryption, we will get the original image.

V. EXPERMINTAL RESULT

The proposed algorithm was implemented using visual basic Net programming language. A set of examples were executed and analyzed as described in the following sub sections.

A. Key Space Analysis

The proposed algorithm took Logistic map parameter μ and iterative initial value x0, and Hénon map initial value (x, y, z) as the original key, iteration time *N*. Each digit has 14 digital numbers, therefore, the key space is $10^{14\times6}=10^{84}$, the key space will be greater, and therefore, the algorithm has a strong resistance against attack of exhaustion as the key space will be greater. For example diffusion key space consists of 3 initial parameters (3-sub keys). The key space of each one is equal 256 bit and the attacker needs $3*2^{256}$ operations to find the exact key. If the attacker employs 1000 million instructions per second of computer processing to guess the key by *brute force attack*, the computational load in years is:

$$\frac{3\times2^{256}}{1000\times10^{6}\times60\times60\times24\times365} \rangle\ 11.2634583\times10^{61}\ years$$

B. Key Sensitivity Analysis

The key sensitivity property of the proposed cryptosystem, the test image (Figure 3(a)) is firstly encrypted using a randomly selected key (*a = 1.6, b = 0.2, μ=3.75*, x0 = 0.82, y0 = 0, 1, z0 = 0, iteration time *N*=20), and the resultant cipher image is shown in Figure 1(a). Figure 1(b) decrypted image using the same as encryption key (correct key), then the ciphered image is attempted to be decrypted using the same key used for encryption except for X1***=0.82000001***, or decryption, process with only a change to the iteration time ***N=21*** in decryption the results will be as shown in fig.1 (c, d), from which we can see that even an almost perfect guess of the key does not reveal any information about the plain image. Therefore, it can be concluded that the proposed image cryptosystem fully satisfies the key sensitivity requirement. Fig.1 shows that the proposed cipher scheme has enough space and is sensitive to minor changes in the key that makes it impossible to get an original image of the decoded one in case of any minor changes. They generate completely different results and decryption cannot give the correct original image.

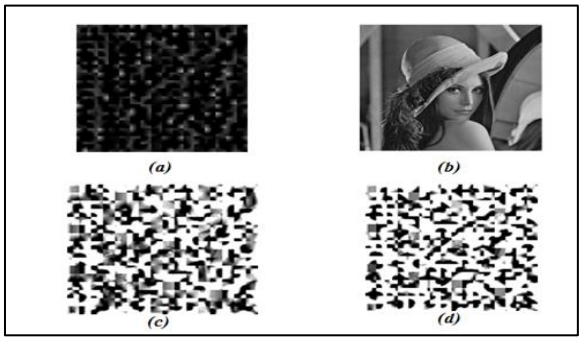

Fig. 1. a) encrypted image, b) decrypted image with correct key, c) decrypted image with slight change in the one bit in the key x=***0.82000001,***d) decrypted image with change the iteration number from n=20 to n=21

C. MSE (Mean Square Error), SNR (Signal to Noise Ratio) and PSNR

In order to determine that the proposed algorithm can successfully conceal the pure image information and also enable the deciphered image to be reconstructed back to the original image without missing any information the MSE, SNR, and PSNR [14] are used for this purpose and a set of standard images are shown in fig.2. TABLE. I ,TABLE.II, and TABLE.III, shows a large results of MSE which mean that the proposed key is successful in concealing the pure image information and a small amount of SNR and PSNR means the proposed key caused large noise (i.e. small result implies better image concealment of original image).

Fig. 2. the standard image used for test

TABLE I. MSE RESULT

Image Name	***MSE***		
	Red	***Green***	Blue
Lena	15824.7	12588.4	12137.36
Pepper	15263.12	15676.95	6398.761
Fruit	25098.19	23590.67	18118.46
Camera man	22392.24	22392.24	22392.2

TABLE II. SNR RESULT

Image Name	*SNR*		
	Red	*Green*	*Blue*
Lena	2.299523	1.170863	1.199166
Pepper	1.589982	1.20896	1.013237
Fruit	1.598209	1.225291	1.099732
Camera man	1.230251	1.23025	1.23025

TABLE III. PSNR RESULT

Image	*PSNR*		
	Red	*Green*	*Blue*
Lena	7.137497	8.131199	8.289662
Pepper	7.2944	7.17822	11.07015
Fruit	6.134367	6.403363	7.549595
Camera man	4.62987	4.62987	4.62987

D. Processing Time

Processing time for encryption and decryption is also an important issue in real-time multimedia applications. To estimate the execution time of the proposed encryption scheme, different tests are performed on a PC with a 2.2 GB dual core processor and 3 GB RAM. Tests results of encryption time and decryption time are shown in table. II. We conclude from the results of input images that the proposed encryption system is of high-speed and flexible for various applications.

TABLE IV. PROCESSING TIME

IMAGE	*ENCRYPTION (SEC)*	*DECRYPTION (SEC)*
Lena	0.38411625	0.30611750
Pepper	0.39861708	0.30511745
Fruit	0.30811762	0.37991601
Camera man	0.33831708	0.3399160

VI. CONCLUSION

In this paper, an algorithm for image encryption was designed utilizing a proposed hyperchaos system. The simulation experiments showed that this algorithm was capable of achieving relatively good effects in terms of encryption and decryption methods. The proposed scheme provides large key space, which is sensitive to slight change. The large values of MSE prove that the proposed key is successful in concealing pure image information; while the small results of SNR and PSNR indicate that the proposed key causes large noise (i.e. small result implies better original image concealment). The encryption execution time of the proposed encryption scheme is relatively fast and flexible to different applications. The future work is to employ the proposed hyperchaos system in design an authentication system.

REFERENCES

[1] L. Shiguo, S. Jinsheng and Zhiquan W. "*A Novel Image Encryption Scheme Based-On JPEG Encoding"* , Proceedings Of The Eighth International Conference On Information Visualization , Department Of Automation, Nanjing University Of Science And Technology, 2004 .

[2] L. Tao, Z. Shaowu, Z. Zhaofu , and O. Qingli, "*A New Scrambling Method Based On Semi-Frequency Domain And Chaotic System"*, School Of Information And Electrical Engineering, Hunan University Of Science And Technology, Xiangtan, China, IEEE, Vol. 2, PP. 607 – 610,2005.

[3] M. Y. Roueida , " A Cryptographic Scheme For Color Images" , M.Sc. Thesis, Iraqi Commission For Computers & Informatics, Informatics Institute For Postgraduate Studies 2006.

[4] C. Yun, Q. Runhe, F. Yuzhe , "*Color Image Encryption Based On Hyper-Chaos*" ,Information And Technology Department, Donghua University, Shanghai, China, PP.1-6, IEEE 2009.

[5] C. Zaiping, L. Haifen, D. Enzeng, and D. Yang, " *A Hyper-Chaos Based Image Encryption Algorithm"*, Tianjin University Of Technology, Second International Conference On Intelligent Human-Machine Systems And Cybernetics, IEEE. Vol. 2, PP. 188 – 191,2010.

[6] S. Sadoudi**,** C. Tanougast**,** M. Salah Azzaz, and A**.** Dandache, **"**Design and FPGA Implementation of A Wireless Hyperchaotic Communication System for Secure Real-Time Image Transmission", EURASIP Journal on Image and Video Processing , 43 doi:10.1186/1687-5281-2013-43,2013.

[7] S. Bredin, "Chaos Theory and Cryptography", Cryptography II, Spring, 2012.

[8] L. Li-hong, Feng-ming, and H. Xue-hui, "New Image Encryption Algorithm Based on Logistic Map and Hyper-chaos", International Conference on Computational and Information Sciences, 2013.

[9] M. Mohammad, " Analysis and Design Security Primitives Based on Chaotic Systems for e- Commerce". A Thesis presented for the degree of Doctor of Philosophy Durham University, United Kingdom,2012.

[10] L. Zhang, and J. Guo, "A Symmetric Image Encryption Scheme Based on Composite Chaotic Dispersed Dynamics System, Proceedings of the Second Symposium", International Computer Science and Computational Technology(ISCSCT 09), Huangshan, P. R. China, 26-28, Dec. 2009, PP. 191-194.

[11] J. Jiang, Y. Weng,and P. Li, " Dominant colour extraction in DCT domain. Image and Vision Computing", 24, 1269-1277, 2006.

[12] S. Matondo, and G. Qi, *"*Two-Level Image Encryption Algorithm Based on Qi Hyper-Chaos", *Fifth International Workshop on Chaos-fractals Theories and Applications, pp. 181–185,2012.*