Diyala Journal of Engineering Sciences

ISSN 1999-8716
Printed in Iraq

Vol. 09, No. 04, pp. 24-35, December 2016

MULTIMEDIA CRYPTOGRAPHY BASED ON LIU AND CHEN SYSTEMS

Jinan N. Shehab [1], Hussien Y. Radhi [2], Ruwaida A. Ibrahim[3]
[1] Department of Communications Engineering, University of Diyala
[2, 3] Department of Computers and Software Engineering University of Diyala
(Received: 6/9/2015; Accepted: 3/1/2016)

ABSTRACT: - Information security is an important matter in communication systems such as internet communication, multimedia systems, medical imaging, and especially military communication. This paper presents two types of multimedia cryptography; text and image cryptography depending on using Chen and Liu systems. The two systems together are used to generate a secret key to encipher multimedia. First by changing the position of characters in original text and changing position of pixels in original image, then changing the character value itself and pixel value depending on random numbers generated by Liu and Chen systems .The experimental and simulation results show that the proposed system is effective and has a high security level. Due to its key space, high key sensitivity, high entropy , low correlation, strong against differential analysis and finally low time complexity since the same set of numbers must be generated depending in the same key schedule to return original multimedia and this is impossible without knowing exact initial conditions, parameters at the same schedule.
Key words: image cryptography, text cryptography, Chen system, Liu system.

1. INTRODUCTION

With the development of the network technology, people are getting more and more information from the Internet. While enjoying the convenience brought by the Internet, we also start to worry about information security. Therefore, a variety of cryptography plans have emerged. Texts, images, audios and videos are the major means people used to obtain information and the majority of the cryptography algorithms nowadays are for the protection of texts [1]. Cryptography is a method of storing communication security since the data is transmitted in a form that can be obtained only by the receiver which has the key. It is a discipline of defending information by coding it into an indecipherable layout [2]. Even though, there are standard cryptosystem such as Advanced Encryption Standard (AES), for symmetric key cryptography, and Rivest-Shamir-Adleman (RSA) for public key cryptography, but AES algorithm is computationally intensive and RSA algorithm is too slow. Due to some inherent properties of images, such as the huge amount of information it contains and the correlation between adjacent pixels, traditional encryption methods like Data Encryption Standard (DES), RSA cannot work properly in image cryptography [1].

2- RELATED WORK

In [1] the encryption plan combines the sequence generated by one-dimensional and two-dimensional Logistic chaotic map to scramble the image. In [2], the digital signature algorithm is used with commutative codes to reassure the security of the transmitted data. In [3], it is found that the key is generated by proposing an n-array key stream generator, based on hierarchical combination of three chaotic maps, while [4] presents an image encryption algorithm based on two-dimensional (2D) Logistic map and complicated Chua's system. [5] use the R, G and B components of a color plain-image to form a matrix, then the matrix is permutated by using zigzag path scrambling and the resultant matrix is then passed through a

substitution process. [6] Concerned with enhancing the existing standards of cryptography (AES) to encrypt image data. Modifications are made on the S-box and on Mix-Column transformation.

In this work, a new cryptography algorithm is been proposed based on a combination of Chen and Liu systems that have higher-dimensional system to crypto the text and then the same algorithm to crypto each channel in color image. The trajectory of Chen and Liu system are more complicated and therefore has larger key space. The simulation also indicates that this algorithm has a good cryptography effect.

3- CRYPTOGRAPHY ALGORITHM BASED ON CHEN AND LU

The proposed system in this paper depends on three dimensional Chen and three-dimensional Liu systems which are combined to generate a random number sequence, with the iterative equations of them respectively being:-

3.1- Liu System

The master system is described by the Liu dynamics equation as [7]:-

$$\dot{x}_1 = a\,(y - x)$$

$$\dot{y}_1 = b\,x - xz \qquad \ldots\ldots\ldots (1)$$

$$\dot{z}_1 = -c\,z + dx^2$$

Where x, y, z are the state variables of the system and a, b, c and d are parameters of the system. The performance of Lu system is illustrated in Figure (1)

3.2- Chen System

Chen system can be applied to design a cryptosystem with higher security. Chen dynamical system is described by the following system of differential equations [8]

$$\dot{x}_2 = a\,(y - x)$$

$$\dot{y}_2 = (c - a)x - xz + cy \qquad \ldots\ldots\ldots (2)$$

$$\dot{z}_2 = xy - b\,z$$

Where x, *y* and *z* are the state variables and *a*, b and c are three parameters. In Figure (2), the State Portrait of Chen system is shown. The trajectory of both Chen and Lu systems can be obtained by the fourth-order Runge-Kutta algorithm with step=0.001. The sixth discrete variables of Chen and Lu systems are adopted to Cryptography the text and the image. The optimization model of Chen and Liu systems are:-

$$X^*(i) = floor\,(X(i) \times 10^m)$$

$$Y^*(i) = floor\,(Y(i) \times 10^m) \qquad \ldots\ldots\ldots (3)$$

$$Z^*(i) = floor\,(Z(i) \times 10^m)$$

Where X^* , Y^* and Z^* ,are the random number sequences generated by the optimization model of Chen and Lu systems, and floor( ) is a rounded down function. One or more of the sequences can be used in the process of cryptography.

3.3- The Proposed System

In this work, the system which used for cryptography of image and text is illustrated in Figure (3).

3.3-1. Encoding System

Firstly, the proposed cryptographic algorithm is applied to the text and then to the color image. To apply the algorithm on color image; the first thing is to divide the color image (24bit/pixels) into three original colors (red (R), green (G) and blue (B) (each color have 8 bits/pixel) then start proposed algorithm is started for encoding. There are main algorithms in encoding system:-

3.3-1.1. Shuffling Algorithm (1-D)

The shuffling algorithm utilizes applying the 3-D (3- dimensions) Chen system and 3-D Liu system to generate anew key according to propose key schedule:-

$$x_3 = bitxor(x_1, y_2)$$

$$y_3 = bitxor(y_1, z_2) \quad \dots\dots\dots (4)$$

$$z_3 = bitxor(z_1, x_2)$$

This step gives a new key that makes the work very strong. The (x_3, y_3, z_3) is used to generate the new random numbers sequences and then rearrange these numbers in descending order. After dividing the color image (3× (M×N)) into three colors channels as (R (M×N), G(M×N) and B((M×N)), where $\boldsymbol{M}$ is the number of row in image and $\boldsymbol{N}$ is the number of column. Each channel is converted from 2-D to 1-D(one row ((M×N)×1) and use the indexed position of each element is the used in the descending sequence of the new key to rearrange channel, by using sort of X_3 to rearrange R-channel, X_3 to rearrange G-channel and X_3 to rearrange B-channel, taking into consideration their own initial conditions but same parameters. In shuffling, text uses X_3 once because a text is originally a 1-D of (8 bits/character).

3.3-1.2. Substitution of Pixels Value

The keys schedule for this step is shown as follows:-

$$E = bitxor(x_3, x_2)$$
$$E_1 = bitxor(y_3, y_2) \quad \dots\dots\dots (5)$$
$$E_2 = bitxor(z_3, z_2)$$
$$E_3 = bitxor(bitxor(E, E_1), E_2)$$

It is easy to suffer from chosen-plaintext attack if just shuffling pixels position. Is applied the attacker can get the corresponding relationship of pixel's position change by choosing a single pixel change, which is avoidable by the introduction of substitution mechanism [4].

The method is realized by using the random sequences generated by new key schedule as an XOR with pixel value in each channel to get new value for each pixel in the color image. The details are as follows:

a) Transforming the keys schedule sequence to eight unsigned integer as an XOR operand.

$$E4 = mod(E3,256) \quad \dots\dots\dots (6)$$

b) Changing the pixel value in each channel (R, G, and B) in the color image.

The resulting image of the shuffling process (1-D for each channel) is used in the process of changing pixels value are as follows (for R-channel and the same steps for both G and B-channel but with different initial conditions):-

New R =bitxor(E3, old R)…….. This step is for the first pixel only.

New R =bitxor(E3,bitxor(new R, old R))…… The new value depends on both the old value for pixel and the new value for the pixel before it.

After the completion of this step is returned to the (2-D) image for each channel.

3.3-1.3. Shuffling Algorithm (2-D)

The last step in the encoding process is the process of shuffling 2-D color image using the indexed position of each element in the descending sequence of the new key (y3 and z3)to rearrange channels as shown in figure(4) (for R-channel):-

From table(1) it can be seen that the row in R-channel in image rearrange according to the sort of secret key y3 and column according to the sort of secret key z3. In the same manner, both G and B channels are rearrangement with only difference of using different initial conditions in each state.

3.3-2. Decoding System

In order to decode the original image you should generate the same key in the same way used in encoding and use the same relations, but in reverse order to get the original image.

4- EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

4.1- Simulation Results

In this work, the simulation results are achieved for three different color images and text using secret key that generated from Liu and Chen systems using MATLAB 8.4. The results are shown in Figure (4).

4.2- Statistical Analysis

4.2-1. Grey-Scale Histogram

A histogram is a graph used for showing the distribution of pixel values of an image. Shannon presented that many encoding systems could be attacked by statistical analysis and proposed to resist attack based on statistical analysis by improving scrambling or shuffling and substitution [4,5]. In this work, it is shown that the processes of shuffling and substitution resistant to statistical analysis efficiently by analyzing the scheme presented which can be shown from the histograms of original color image and encoding color image. The simulation results show that the histogram of original color image (R,G,B-channel) and the encoding color image is changed as shown in Figure (5). The pixel value of the encoding image in [0 ,255] interval for each color is distributed and almost flat . So the algorithm can resist statistical attack effectively.

4.2-2. Correlation of Adjacent Pixels

Correlation between two random series indicates the strength and direction of their linear relationship [4]. To test the correlation between two adjacent pixels, the following procedures are carried out. First, randomly select 1000 pairs of two horizontal adjacent pixels from an image and then calculate the correlation coefficient $\boldsymbol{Corr_{xy}}$ of each pair using the following equations [5]:-

$$\boldsymbol{Corr_{xy}} = \frac{|\boldsymbol{cov}(x,y)|}{\sqrt{\boldsymbol{D}(x)}\times\sqrt{\boldsymbol{D}(y)}} \quad \dots\dots\dots (7)$$

Where x and y are the gray-scale values of two adjacent pixels in the image, while cov(.,.) and D(.) are computed, as follows: -

$$\boldsymbol{E}(x) = \frac{1}{N}\sum_{i=1}^{N} \boldsymbol{x_i} \quad \dots\dots\dots (8)$$

$$\boldsymbol{D}(x) = \frac{1}{N}\sum_{i=1}^{N} (\boldsymbol{x_i} - \boldsymbol{E}(x))^2 \quad \dots\dots\dots (9)$$

$$\boldsymbol{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N} \big(\boldsymbol{x_i} - \boldsymbol{E}(x)\big)\big(\boldsymbol{y_i} - \boldsymbol{E}(y)\big) \quad \dots\dots\dots (10)$$

Then the same process for horizontal line is repeated along the vertical and diagonal directions respectively. The simulation results shown in Table (2) and Figure (6) show that the correlation coefficients of the encoding images in the proposed system are very small as compared with original image and with [6,9], Therefore, the proposed system have high security against statistical attacks.

4.3- Differential Analysis

NPCR (Number of Pixels Change Ratio) shows the number of changed pixels when the value of a pixel in the original image is changed. The NPCR indicates the sensitivity of the scheme to similar original images with a tiny difference [5]. The $\boldsymbol{NPCR}$ can be calculated using:-

$$NPCR = \frac{\sum_{i,j} D(i,j)}{H \times W} \times 100\% \quad \dots\dots\dots (11)$$

Where $\boldsymbol{W}$ is the width of the image and $\boldsymbol{H}$ is the height of the image and $\boldsymbol{D(i,j)}$ is the difference between two images.

$$\boldsymbol{D(i,j)} = \begin{Bmatrix} \boldsymbol{1} & \boldsymbol{E1(i,j) \neq E2(i,j)} \\ \boldsymbol{0} & \boldsymbol{E1(i,j) = E2(i,j)} \end{Bmatrix} \quad \dots\dots\dots (12)$$

Where $E1$ is encoded vision of original image and $E2$ is encoding original image after changing one pixel.

Unified Average Changing Intensity (UACI) shows the average intensity of differences between the plain image and the corresponding encoded image [5]. The $UACI$ is calculated using the following equation:-

$$UACI = \frac{1}{H \times W}\left[\sum_{i,j}\frac{|E_1(i,j) - E_2(i,j)|}{255}\right] \times 100\% \quad \dots\dots\dots (13)$$

The NPCR measures the percentage of different pixel numbers between the two images and the UACI measures the average intensity of differences between the two images.

From above tables, one can see the proposed algorithm has high NPCR sensitivity and high UACI also as compared with work [6, 9] it can be said that the proposed system is strong and powerful against differential attack.

4.4- Key Space and Sensitivity Analysis

Key space size is up to the total number of different keys that are used in the encoding. Cryptosystem is completely sensitive to all secret keys [4]. Only use the initial conditions of system as the key in this work using different initial condition for each color , then key space is 10^{90} for one color and key space up to $\approx 10^{270}$ for all proposed system compared with secret key in [5] is 2^{16} only. Apparently, the key space is large enough to resist all kinds of brute-force attacks.

The sensitivity to secret keys means that when a small change occurs in keys, then encoding image cannot be correctly decoded [8]. For the encoding image, only the correct secret key can get the clear image. In figure (7) (c), only the initial value of Chen system has been slightly changed from x_0 = 0.1 to be x_0 =0.1000000000001 at which decoding of the same encoded image fails completely. Therefore, this test shows that the algorithm is very sensitive to the initial values.

4.5- Information Entropy Analysis

Entropy is a measurement of the uncertainty associated with a random variable in information theory which represents an important parameter to characterize the confusion of encrypted image [6]. It can be calculated as [5]:

$$\sum_{i=0}^{2^{n-1}} \boldsymbol{P(m_i) log_2(\frac{1}{P(m_i)})} \dots\dots\dots (14)$$

Where mi is the pixel value and $P(m_i)$ represents the probability of m_i. Theoretically, a true random system should generate 2^8 symbols with equal probability for bit depth. Therefore, the entropy of the system will be H(8)=8 [5]. The calculation of the entropy of proposed images with different initial conditions is done. Results show that all values are very close to 8, with an average of 7.99, as shown in Table (5) which proves the ability and robustness against entropy attacks.

In this work, the entropy of the original and encoding texts are (4.4339) and (7.4497) respectively. It is obvious from the entropy of the encoding text that this value is near to the ideal value.

4.6 Speed Test

The time required to perform the proposed cryptography system is obtained by MATLAB (R2014a) in a computer (Intel Core i5), and compare it with the time required in the algorithm that proposed by [6, 9]. It can be found that the time of the proposed algorithm is very short as compared with the algorithms in [6, 9] as shown in Table (6).

From Table(6), it is obvious that the execution time of proposed system is small as compared with the algorithms of [6,9] for two reasons, the first is the using of function in this work and the second is the simplicity of the system design.

5. CONCLUSION

In this paper, the cryptography of three color images and text is proposed using two systems Chen and Liu. From the results of this work, it can be found that the proposed algorithm provides very powerful and secret cryptography method. It has a large key space to resist brute-force attacks, high key sensitivity, the system is strong against differential attack,

achieve good randomness, high security against statistical attacks, the execution time is very small and final simple of the system design.

6. References

1) Yuye Wang& Jingwen Wang,“ A New Image Encryption Algorithm Based on Compound Chaotic Sequence”, International Conference on Measurement, Information and Control (MIC), 978-1-4577-1604-1112/ 20121EEE
2) P. Karthik, P. S. Ranjith & M. Jayagnesh, “SCCE: Secure Communication Based on A Chaotic System for Modern Wireless Communication”, International Journal of Research in, Engineering & Technology (IMPACT: IJRET), ISSN (E): 2321-8843; ISSN(P): 2347-4599, Vol. 2, Issue 3, Mar 2014, 163-172.
3) Rakesh S, Ajitkumar A, Kaller, Shadakshari B & Annappa B “Image Encryption using Block Based Uniform Scrambling and Chaotic Logistic Mapping”, International Journal on Cryptography and Information Security (IJCIS),Vol.2, No.1,March.
4) Xiang Fei & Guo Xiao-cong, “An Image Encryption Algorithm based on Scrambling and Substitution using Hybrid Chaotic Systems”, Seventh International Conference on Computational Intelligence and Security, 978-0-7695-4584-4/11/ 2011 IEEE.
5) Xing-Yuan Wang , Ying-Qian Zhang & Xue-Mei Bao ,“ A Colour Image Encryption Scheme Using Permutation-Substitution Based on Chaos”, ISSN 1099-4300, 9 June 2015.
6) ali Abdulgader, mahamod Ismail, nasharuddin Zainal & Tarik Idbe “ Enhancement Of Aes Algorithm Based On Chaotic Maps And Shift Operation For Image Encryption”, Journal of Theoretical and Applied Information Technology, January 2015. Vol.71 No.1.
7) Dr. V. Sundarapandian, “Anti-Synchronization of Liu and Chen Chaotic Systems by Active Nonlinear Control”, International Journal of Advances in Science and Technology, Vol. 2, No.3, 2011.
8) A Jun Peng[1], Du Zhang[2] and Xiaofeng Liao[3],“Design of A novel Image Block Encryption Algorithm Based on Chaotic System”, Prlc.lib IEEE lIt Cllf.II Cillidlillflr.adcs (ICCI'09) I. Bacil, Y. Wall, Y.Y. Yal, W.l ilsllr, I. Chal& L.A. Zadlh (Eds.) 911-1-4244-4642-1/09/$25.00 ©20091EEE.
9) Kamali, S. H., Shakerian, R., Hedayati, M., & Rahmani, M. “A new modified version of Advanced Encryption Standard based algorithm for image encryption.” In Electronics and Information Engineering (ICEIE), 2010 International Conference On, Vol. 1, 2010, pp. V1-141, IEEE.
10) aphorism George Bernard Shaw (1856- 1950), “http://www.alfaseeh.com/vb/showthread.php?t=55737”,.

Table (1) Shuffling Algorithm (2-D)

R-channel from image			
(1,1)	(1,2)	(1,3)	(1,4)
(2,1)	(2,2)	(2,3)	(2,4)
(3,1)	(3,2)	(3,3)	(3,4)
(4,1)	(4,2)	(4,3)	(4,4)

Sort of y3
4
2
1
3

Sort of z3
2
1
4
3

New position of pixel in R-channel according (y3,z3)			
(4,2)	(4,1)	(4,4)	(4,3)
(2,2)	(2,1)	(2,4)	(2,3)
(1,2)	(1,1)	(1,4)	(1,3)
(3,2)	(3,1)	(3,4)	(3,3)

Table 2 Correlation Coefficient Values

Original and encrypted images	Correlation coefficient values		
	Horizontal	Vertical	Diagonal
Original images	0.9798	0.9755	0.9613
Method by [9]	0.0019	0.0030	0.0012
Method by [6]	0.0013	0.0020	0.0080
Proposed method	3.589×10^{-4}	1.8838×10^{-4}	8.2914×10^{-4}

Table 3 $NPCR\%$ Values

Image name	Color	Image of [9]	Image of [6]	Proposed Encrypted Image
Girl	R	99.484	99.461	99.66
	G	99.623	99.641	99.60
	B	99.600	99.592	99.62
Mandrill	R	99.565	99.580	99.60
	G	99.588	99.604	99.60
	B	99.627	99.614	99.62
Flower	R	99.599	99.601	99.60
	G	99.610	99.621	99.61
	B	99.617	99.612	99.62

Table 4 $UACI\%$ Values

Image Name	color	Image of [9]	Image of [6]	Proposed Encrypted Image
Girl	R	33.4007	33.4948	33.46
	G	33.5740	33.4955	33.49
	B	33.3635	33.5165	33.57
Mandrill	R	33.5295	33.4439	33.44
	G	33.4733	33.5012	33.43
	B	33.4897	33.5328	33.50
Flower	R	33.4869	33.4749	33.47
	G	33.4875	33.5063	33.49
	B	33.4402	33.4698	33.48

Table 5 Entropy Values for Red , Green, and Blue colors				
Image	color	Girl	Mandrill	Flower
Original Image	R	7.2711	7.6515	7.4815
	G	7.0319	7.3488	7.2924
	B	6.8594	7.6692	7.5072
Image of [9]	R	7.9972	7.9992	7.9999
	G	7.9970	7.9993	7.9999
	B	7.9974	7.9993	7.9999
Image of [6]	R	7.9974	7.9993	7.9999
	G	7.9975	7.9992	7.9999
	B	7.9972	7.9992	7.9999
Image of the Proposed algorithm	R	7.9970	7.9993	7.9998
	G	7.9972	7.9993	7.9998
	B	7.9974	7.9994	7.9998

Table 6 Encryption and Decryption Speed				
Image		Girl	Mandrill	Flower
Algorithm in [9]	Encryption time	96.92	382.09	1546.19
	Decryption time	118.51	469.48	1899.02
Algorithm in [6]	Encryption time	31.81	119.30	463.65
	Decryption time	31.69	110.82	446.64
Proposed Algorithm	Encryption time	1.736270	5.552880	18.967109
	Decryption time	1.220269	4.185547	13.780178

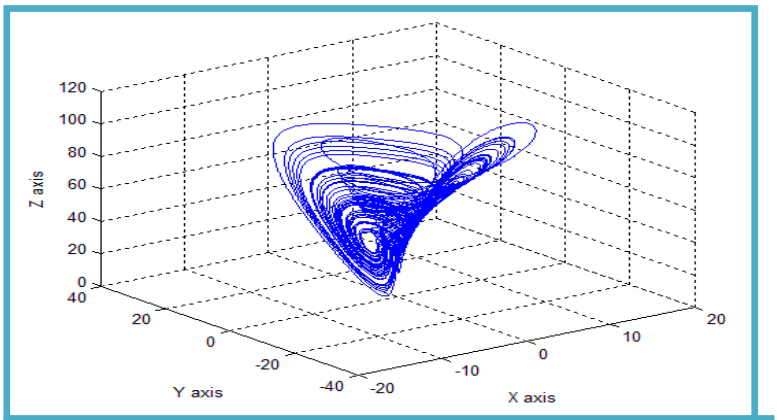


Fig.1: The Phased Diagram of the Liu System

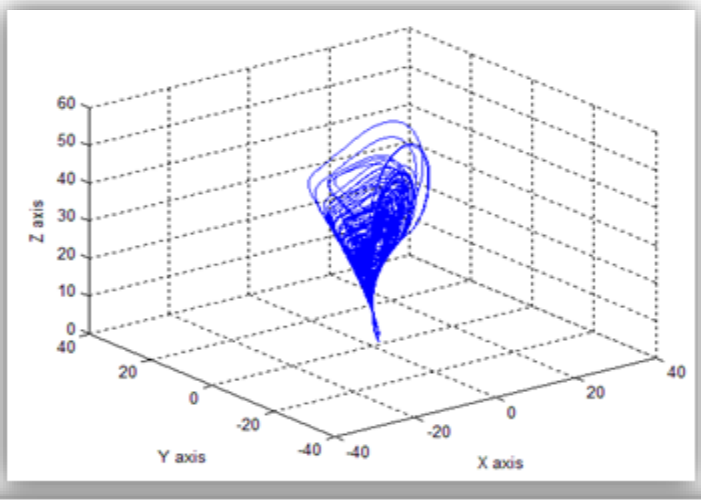


Fig. 2 The Phase Diagram of The Chen System

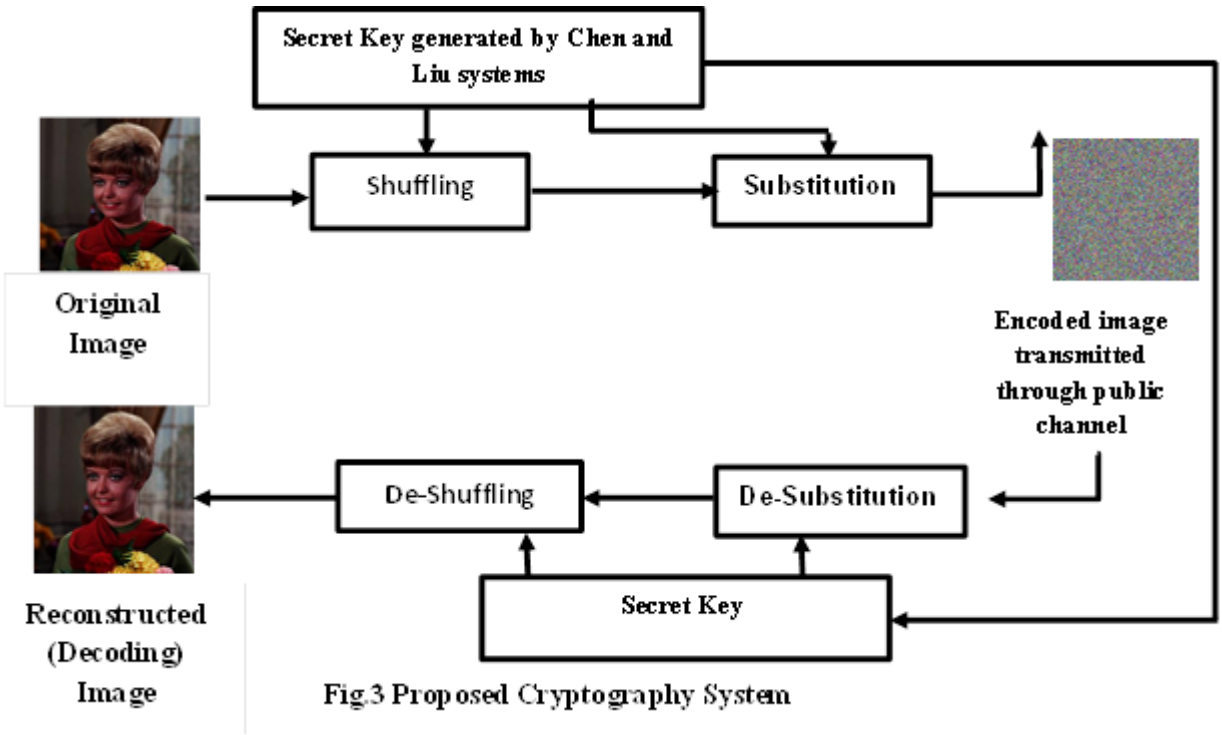


Fig.3 Proposed Cryptography System

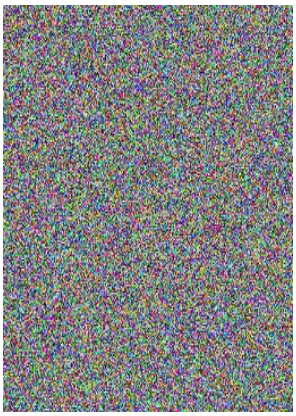
Original image	Encoded image	Decoding image
		
Original text	**Encoded text**	**Decoded text**
University of Diyala / College of Engineering /Communications Department and / Computer and Software Department/ George Bernard Shaw (1856-1950) say ((If you have an apple and I have an apple and we exchange these apples then you and I will still each have one apple. But if you have an idea and I have an idea and we exchange these ideas, then each of us will have two ideas)).	ªé*ƒ*„©´¡ü„'Is·ô2…øÙaâ□úä•SµF2k, Î'Í! • f#'.Òû • AíLd‡eîÌ¾×B=]År?ŸS 'i~-Ê¥]1@6/Ÿ ½@¾«Ð- "Ã[ß!~áÀwŸ=ÐtïL›HMpÌ□ªŸ<j'Æ ýû<V|g}P~Ff)D3p",8×Æ@û¡hGø¿ Ž ,_□†□‡¬fçÜš„)¢1w— 6 • åº×Éy.H}„›`-yÂJ …ÈûLU Ì$— Ýüµâ¦– ÂÂ…'õ-†åê` • ×`1´ýÝSÓí²œ,xÙì'¢I *ƒ*M¦Œ‰ª¼bs,F*Ý- ½vtZßoˆØÃÛ2ÂéD— ³d2MŠFÁW-îÖ Q- 97Æ»Vaº»– ¶CÝ¡êÙ±~c77âøogÏ¥ÄïÐ·¬ñ$çþ Ë3 „¼ŸÿBq —————————ž Ûkz ®Je zjbÊ&Ç?| • °*2äh ,Ã[ÏxÍ½ö¾5 iÆL	University of Diyala / College of Engineering /Communications Department and / Computer and Software Department/ George Bernard Shaw (1856-1950) say ((If you have an apple and I have an apple and we exchange these apples then you and I will still each have one apple. But if you have an idea and I have an idea and we exchange these ideas, then each of us will have two ideas)).

Fig. 4 Proposed Cryptography System Results

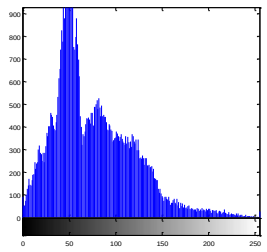
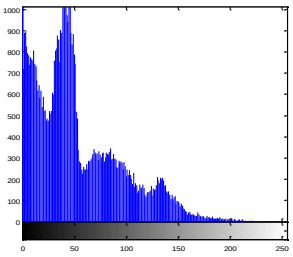
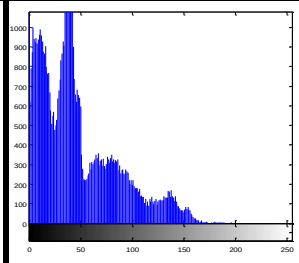
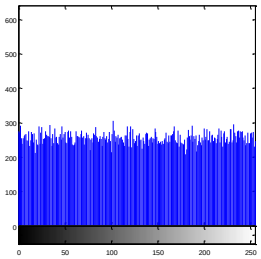
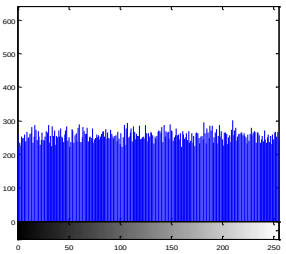
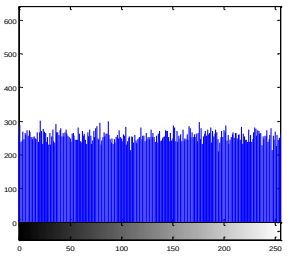
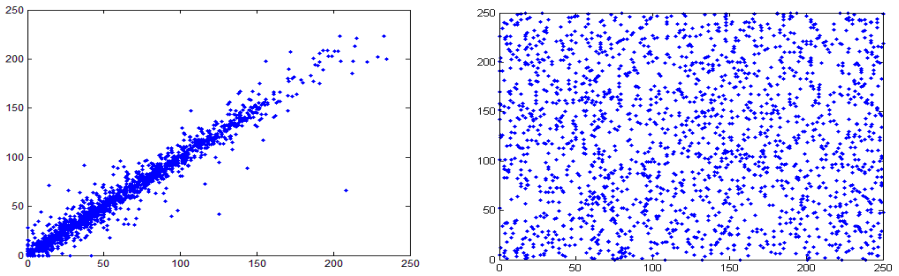
Image Type	R-channel	G-channel	B-channel
Original color image			
Encoding color image			

Fig.5: Histogram of Original and encoded Images



a *b*

Fig. 6 Correlation Distribution of Adjacent Pixels for a) Original and b) Encoding Image in Red Channel

(a) (b) (c)

Fig.7 Key Sensitivity a) Original Image b) Decoding by correct Secret Key (x0 = 0.1) c) Decoding by Secret Key (x0 = 0.1000000000001)

تشفير الوسائط المتعددة باستخدام نظامي ليو و تشن

جنان نصيف شهاب[1] ,حسين يوسف راضي[2] ,رويدة عبد الله ابراهيم[3]

[1]م.م. قسم هندسة الاتصالات ,[3,2] م.م. قسم هندسة الحاسبات والبرامجيات

كلية الهندسة, جامعة ديالى

الخلاصة:

ان أمن المعلومات هو مسألة هامة في أنظمة الاتصالات مثل الانترنت ، وأنظمة الوسائط المتعددة، والتصوير الطبي، والاتصالات العسكرية على وجه الخصوص. يقدم هذا البحث نوعين من تشفير الوسائط المتعددة النص والصورة. اعتمد التشفير على استخدام أنظمة تشن وليو. وتستخدم النظامين معا لتوليد مفتاح سري لتشفير الوسائط المتعددة. أولا عن طريق تغيير موقع الحروف في النص الأصلي وتغيير موقع البكسل في الصورة الأصلية ثم تغيير قيمة الحرف نفسه في النص وقيمة بكسل في الصورة اعتمادا على أرقام عشوائية تم توليدها باستخدام أنظمة ليو وتشن. التجارب ونتائج المحاكاة تبين أن النظام المقترح هو فعال وذو مستوى أمني عالي. لأنه لديه فضاء واسع للمفاتيح ، درجة تحسس عاليه للمفتاح ، يمتلك انتروبية عالية، الارتباط والتشابه منخفض ، قوي ضد التحليل التفاضلي وأخيرا وقت التنفيذ قليل إذ لابد أن تتولد نفس مجموعة الأرقام اعتمادا على نفس قيمه المفتاح عند الارسال لاستعادة الوسائط المتعددة الأصلية (النص او الصورة) وهذا مستحيل دون معرفة دقيقة بالشروط الابتدائية والمعاملات ونفس جدول المفاتيح المستخدمة عند الارسال.