Research Journal of Applied Sciences, Engineering and Technology 14(1): 48-55, 2017
DOI:10.19026/rjaset.14.3988
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: October 31, 2016 Accepted: January 30, 2017 Published: January 15, 2017

Research Article

Robust Encryption System Based on Novel Chaotic Sequence

[1]Hadi T. Zeboon, [2]Hikmat N. Abdullah and [1]Atheer J. Mansor
[1]University of Technology,
[2]College of Information Engineering, Al-Nahrain University, Baghdad, Iraq

Abstract: The aim of this study is proposing a novel chaotic system in which the variables of the system are treated as encryption keys to achieve secure transmission of digital images. The proposed system has high sensitivity to the variation of its initial values and parameters producing unpredictable trajectories. The novel system successfully passes the 0-1 test and FIPS PUB 140-1 statistical tests that check the distribution of the distinguished elements by generated chaotic sequences. The results obtained proved the robustness of the image encryption/decryption system based on sequences generated from the proposed chaotic generator.

Keywords: Chaos, cryptography, image encryption, image security

INTRODUCTION

Many scientists and scholars for the last decades try to investigate the issue of data encryption and decryption with different methods and systems to promote communication security. Because of the properties of chaotic systems such as highly sensitivity to initial condition and parameters and the unpredictable trajectory of chaos, the application of chaotic systems in encryption and communication security become more and more used (Cuomo *et al*., 1993). Chaotic systems can be used in two ways in cryptography: -generate pseudo-random sequences, which are then used as key streams to mask the plaintext in manifold ways, the plaintext is used as initial state and the cipher text follows from the orbit being generated (Merah *et al*., 2013).

Many chaotic systems had been proposed to increase the security of encryption system such as Lorenz (Moghtadaei and Hashemi Golpayegani, 2012), Chua (Aziz and Faraj, 2012), R□ssler (Sambas *et al*., 2012), Nien (Nien *et al*., 2007), Lu (Vaidyanathan, 2011) and chen (Sprott, 2015). To improve security, the researchers suggested using hybrid chaotic systems. However, the previous works about proposing hybrid chaotic systems for encryption are few. The reason behind that is having hybrid chaotic system is not a straightforward operation by combining two different types of chaotic systems because the chaotic behavior will be lost unless a careful design is considered. Examples of successful hybrid chaotic systems are those presented by combining LIU and Lu systems (Nien *et al*., 2007).

In this study a novel chaotic system is proposed with its attracter characteristics. The system had been tested by using 0-1 test (Gottwald and Melbourne, 2009) and the FIPS PUB 140-1 (FIPS, 2002) standard test. Then, the novel system has been used later to create encryption keys and applied to encryption and decryption of digital color images. Because of the greater scatter and unpredictability characteristics of encryption keys, images lose original outline, colors and characteristics after encryption. After the encryption process, the encryption image could be sent in unsecure lines. Wider key space and the unpredictability of the system's trajectory make the predicting of the encryption key by an intruder unreachable.

MATERIALS AND METHODS

Before presenting the materials and methods of this study, we would like to point out that this study is a part of preparing for a Ph.D. thesis preparing at electrical and electronic engineering department, university of technology since 2015.

According to the prescription of FIPSPUB 140-1, the data (any random number (key) generator) must pass the following four tests for randomness. The numbers must be converted to a single bit stream of 20,000 bits then pass though the tests. If any of the following test fail, then the module shall enter an error state (in other word, the system is predictable).

The monobit (frequency) test: This test counts the number of ones in the 20,000 bit stream. The system

Corresponding Author: Hadi T. Zeboon, University of Technology, Baghdad, Iraq

Table 1: Passing values for runs test

Length of run	Required intervals
1	2,267-2,733
2	1,079-1,421
3	502-748
4	223-402
5	90-223
+6	90-223

pass if 9,654 < X < 10,346, where X is the number of ones (FIPS, 2002)

The poker test: This test is used to find the number of occurrence of each value for every 4 bits. First, divide the 20,000 bit stream into 5,000 contiguous 4 bit segments. Then counting and string the number of occurrences of each of the 16 possible 4 bit:

$$\text{Values: } x = \left(\left(\frac{16}{5000}\right) * \left(\sum_{x=1}^{15}\left(f(x)\right)^2\right)\right) - 5000 \quad (1)$$

Denote f(x) as the number of each 4 bit value x where 0 < x < 15
The test is passed if 1.03 < X < 57.4 (FIPS, 2002)

The runs test: Runs test is the 3rd test which is used to find a maximal sequence of consecutive bits of either all ones or all zeros, which is part of the 20,000 bit sample stream. The incidences of runs of all lengths in the sample stream should be counted and stored. The system pass the test if it is applied according to the values in Table 1 (FIPS, 2002).

The long run test: A long run is defined to be a run of length 34 or more (of either zeros or ones).On the sample of 20,000 bits, the test is passed if there are NO long runs (FIPS, 2002)

The 0-1test: A 0-1 test is used to define the system as chaotic or not, which is proposed by Gottwald and Melbourne (2009). The advantages of this test over Lyapunov exponent (Dawes and Freeland, 2008) is that this test applied directly on the key generated from the system and there is no need to reconstruct the phase space of the system. The test generates a number between zero and one. The system is called a chaotic system if the result very near to one.

Let f(n) is a set of data sampled at time n = 1, 2, 3 … N which represents a one dimensional data set:

$$p(n) = \sum_{i=1}^{n} f(n)\cos(i * a) \quad (2)$$

$$s(n) = \sum_{i=1}^{n} f(n)\sin(i * a) \quad (3)$$

where, a is a real positive number

The mean square displacement is calculated from the following equation:

$$M(n) = \lim_{N\to\infty}\left(\frac{1}{N}\right)\sum_{j=1}^{n}\left(p(j+n) - p(j)\right)^2 + \left(s(j+n) - s(j)\right)^2 \quad (4)$$

The asymptotic growth rate is obtained using:

$$k = \lim_{N\to\infty}\left(\frac{\log M(n)}{\log n}\right) \quad (5)$$

Now if k ≈ 0, the system is predictable (regular) while k ≈ 1 the system is chaotic (Gottwald and Melbourne, 2009)

The correlation coefficient: The correlation coefficient is a statistical analysis which is used to obtain the relationship between two random variables or data sets. In image processing, it is used to obtain the similarity between two images. So, for image encryption, it is one of statistical analysis that is used to calculate the encryption algorithm strength. When the result of it equals to zero, that's mean the images are totally different (original and the encrypted images). If it is equal to one, that's mean the encryption process failed to hide the details of the original image. The correlation coefficient could be obtained as following:

$$CC = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}\left((x_i - E(x))\right)^2}\sqrt{\sum_{i=1}^{N}\left((y_i - E(y))\right)^2}}$$

where, $E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$, x and y are the pixel's value of the original and the encrypted image respectively (Song and Qiao, 2015)

Maximum deviation analysis: Maximum Deviation analysis is a statistical analysis which is used to calculate the deviation between the original and the encrypted images. This analysis depends could be calculated according to the following equation:

$$MD = \frac{h_o + h_{255}}{2} + \sum_{i=1}^{254} h_i \text{ Where} h = |H - H'|$$

where, H and H' are the histogram distribution of the original and the encrypted image. Higher MD means higher encryption degree and the encrypted image faraway (deviated) from the original one (Ahmad and Ahmed, 2012)

Irregular deviation analysis: One of the effective factors to calculate the encryption quality is Irregular Deviation analysis. The irregular deviation used to measure how the encryption process changed the values of the original image irregularly and randomize it in uniform manner to make the statistical distribution of changing the pixels' values uniformly. So, for good encryption process, the Irregular deviation is near to uniform distribution.

The irregular deviation analysis can be obtained from the following steps:

- Calculate the absolute difference between the original and the encrypted images: $D = |O - E|$

where O and E represent the original and encrypted images respectively.

- Obtain the histogram of the absolute difference:

  $H=histogram\ (D)$

- Calculate the average value of the histogram deviation:

  $$Av = \frac{1}{256}\sum_{i=0}^{255} H(i)$$

- Evaluate the absolute deference between the histogram deviation and the average deviation value:

  $$H_{D_i} = |h_i - Av|$$

- Compute the irregular deviation factor value:

  $$I_D = \sum_{i=0}^{255} H_{D_i}$$

Smaller I_D means higher encryption strength, where it is a pointer for the uniform distribution between the original and encrypted pixels' values (Ahmad and Ahmed, 2012)

Entropy: One of the well-known analyses for randomness and encryption quality measurements is Information Entropy Analysis. The encryption quality could be measured by calculating the entropy of the plain image and the entropy of the cipher image, then comparing between them. The entropy if the image could be evaluated by the following equation:

$$E = \sum_{i=0}^{2^n-1}[\ P(i) * \log_2\left(\frac{1}{P(i)}\right)\ ]$$

where, $P(i)$ means the symbol i probability which Expressed in bits. So, for images with gay level of 256 (0 to 255), the maximum entropy equal 8 and it is referred to an ideal case of randomness. In general, the entropy of practical image is less than the maximum entropy.

In encryption process, the entropy of the encrypted image should be ideally equal to 8. When the entropy of it is less than 8, it confirmed degree predictability.

To resist the entropy attacking, the entropy of the encrypted image should be close to the maximum entropy value (Song and Qiao, 2015)

Peak Signal-to-Noise Ratio (PSNR): Peak Signal-to-Noise Ratio (PSNR) can be used to evaluate the encryption scheme strength by indicating the of pixel's value between the original image and the encrypted image. It can calculated by using the following equation:

$$PSNR = 10 * \log_{10}\left[\frac{M * N * 255^2}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(\ O(i,j) - E(i,j))^2}\right]$$

where, O and E are the original and the encrypted image respectively, (i, j) is the coordinate of the pixel and M, N are the image size.

Lower PSNR means higher encryption effectively (Gorji *et al*., 2015)

Measurement based on the value changing: Plain-image pixels values change after image encryption as compared to their original values before encryption. Such change may be irregular. This means that the higher the change in pixels values, the more effective will be the image encryption and hence the encryption quality. So the encryption quality may be expressed in terms of the total changes in pixels values between the plain-image and the cipher-image. Ahmed and Ahmad (2012) proposed a measure for encryption quality that is expressed as the deviation between the original and encrypted image. This method is determined as follows:

Let P, C denote the original image (plain-image) and the encrypted image (cipher-image) respectively, each of size W×H pixels with L grey levels. P(x, y), C (x, y)∈{0,..., L −1} are the grey levels of the images P, C at position (x, y), 0 <x< W–1, 0 <y < H–1. We will define HL(P) as the number of occurrence for each grey level L in the original image (plain-image) and HL(C) as the number of occurrence for each grey level L in the encrypted image (cipher-image). The encryption quality represents the average number of changes to each grey level L and it can be expressed mathematically as:

$$EQ = \frac{\sum_0^{255}|H_L(C) - H_L(P)}{256}$$

Another measurement is proposed by Luo (Jolfaei and Mirghadri, 2010) by computing the relative error, which for an image of H×W is defined as:

$$ARE = \frac{1}{H*W}\sum_{i=0}^{H-1}\sum_{j=0}^{W-1}\frac{|P(i,j)-C(i,j)|}{|P(i,j)|}$$

Which gives the average relative error of a pixel (Jolfaei and Mirghadri, 2010)

The NovelChaotic system and encryption algorithm: Many chaotic systems are proposed to be used in encryption algorithms like Rössler, Chua, Lorenz and Nien. Among these systems we will focus on the systems that are used in the proposed system which are Chua and Lorenz systems. The differential equations of these systems are:

Chua system:

$$\begin{aligned}\dot{x} &= a(y - x - h(x))\\ \dot{y} &= x - y + z\\ \dot{z} &= -by - cz\end{aligned} \quad (6)$$

With, h(x) = m1+0.5(m0- m1)(|x+1)(|x-1|)
Where a = 10; b = 14:78; c = 0.0385; m0 = -1.27; m1 = -0.68

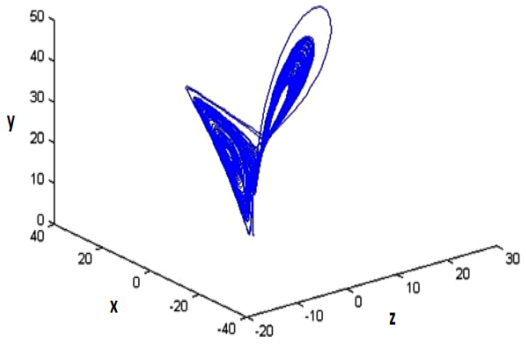


Fig. 1: Trajectory of the novel CL chaotic system

Lorenz system:

$$\begin{aligned}\dot{x} &= a(y + x)\\ \dot{y} &= x(c - z) - y\\ \dot{z} &= xy - bz\end{aligned} \quad (7)$$

where, a = 10, c = 24, b = 8/3,

The proposed chaotic system is hybrid system generated by mixing bands of Chua and Lorenz chaotic systems, so we will call it CL system. The new CL chaotic system has a new chaotic trajectory and improved randomness and it will be proved by 0-1 test and the FIPS PUB 140-1 statistical tests. The differential equations of the CL system are defined as:

$$\begin{aligned}\dot{x} &= a(y - x - (m1 + 0.5(m0 - m1)(|x + 1|)(|x - 1|)))\\ \dot{y} &= x(c - z) - y\\ \dot{z} &= xy - bz\end{aligned} \quad (8)$$

where, a = 10, b = 8/3, c = 24, m0 = -1.27; m1 = -0.68

In Eq. (8) above, $\dot{x}$ is taken from Chau system while $\dot{y}$ and $\dot{z}$ are taken from Lorenz system.

Figure 1 shows the trajectory of the proposed system. It can be seen that this trajectory has a strange shape which refer to a chaotic behavior.

The encryption algorithm based on novel CL chaotic system is as follows:

- Set the initial conditions X_0, Y_0, Z_0 and the parameters for CL chaotic system.
- Decompose the RGB image A into three level matrices which are A1, A2 and A3 with the same dimension.
- Determine the dimension of matrix A1 and retrieve x, y, z of the same dimension and create chaotic encryption keys using:
  $X_k = 10^{10} * X \bmod 256, Y_k = 10^{10} * Y \bmod 256, Z_k = 10^{10} * Z \bmod 256$
- Implement the encryption key on the digital image by:

  $A1 = A_{k1}$ XOR X_k, $A2 = A_{k2}$ XOR Y_k, $A3 = A_{k3}$ XOR Z_k

The decryption process has the same steps as in the encryption process.

RESULTS AND DISCUSSION

The results are divided into two parts, first testing the novel CL system presented in section III to verify its chaotic and randomness behavior. Then testing the encryption system based on CL system. After implementing the 0-1 test to the CL system, we have obtained the following results x = 0.9987, y = 0.9983; z = 0.9983. According to the test, all system variables produce numbers very closed to one, then it is a chaotic system and the chaotic behavior can be obtained from anyone of its outputs. Table 2 shows the result of implementing of the FIPS PUB 140-1 statistical tests to check the system randomness. The results obtained in the table strongly prove that CL chaotic system fulfills the randomness requirements needed for reliable encryption algorithm.

Table 2: The result of FIPS PUB 140-1 tests

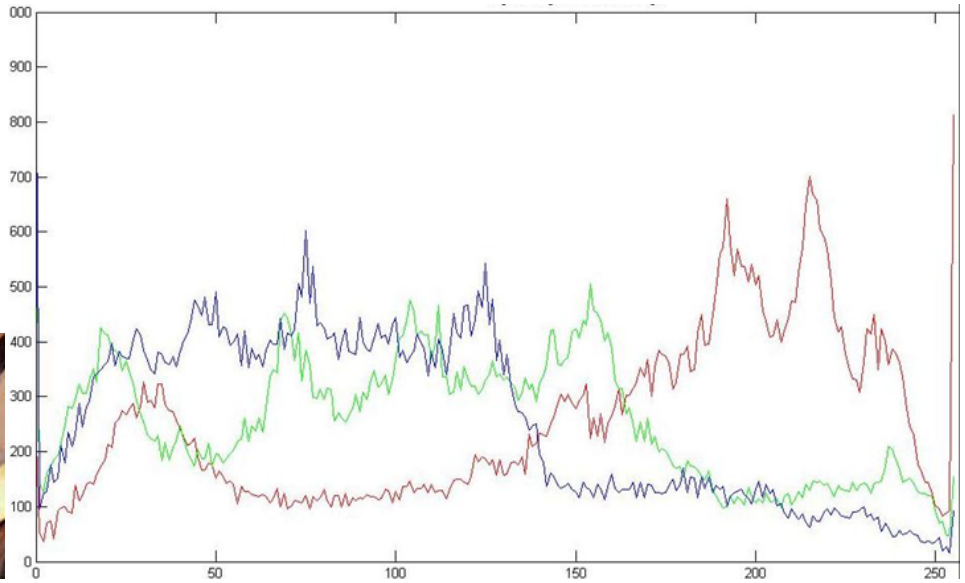
X_k						
Monobit Test	9961					
Poker Test	19.41					
Test	1	2	3	4	5	6
Ones	2470	1286	617	322	143	163
Zeros	2510	1241	628	328	147	146
Long	0					
Y_k						
Monobit Test	9983					
Poker Test	14.73					
Run Test	1	2	3	4	5	6
Ones	2470	1226	632	317	150	169
Zeros	2449	1267	610	318	162	157
Long	0					
Z_k						
Monobit Test	10013					
Poker Test	10.13					
Run Test	1	2	3	4	5	6
Ones	2518	1214	631	317	153	158
Zeros	2458	1288	616	322	162	145
Long	0					

To evaluate the performance of the encryption algorithm it is tested with Lina image. Figure 2 shows the results of implementing the algorithm using CL system. The figure shows the encrypted and decrypted image when the same initial conditions are used (in both Tx and Rx sides) and the decrypted image when atiny difference in any of initial conditions or parameters (when intruder tries to attack the transmission) with the corresponding histograms. The parameters of CL system are a = 10, b = 8/3, c = 24, m0 = -1.27; m1 = -0.68.

In Fig. 2, it is very clear that the novel chaotic system has high sensitivity to the initial conditions and to the system parameters as well to any chaotic system. So any attacker use different systems, initial conditions or parameters even with a very little difference, it is impossible to achieve correct decryption process and obtain the original data before encryption.

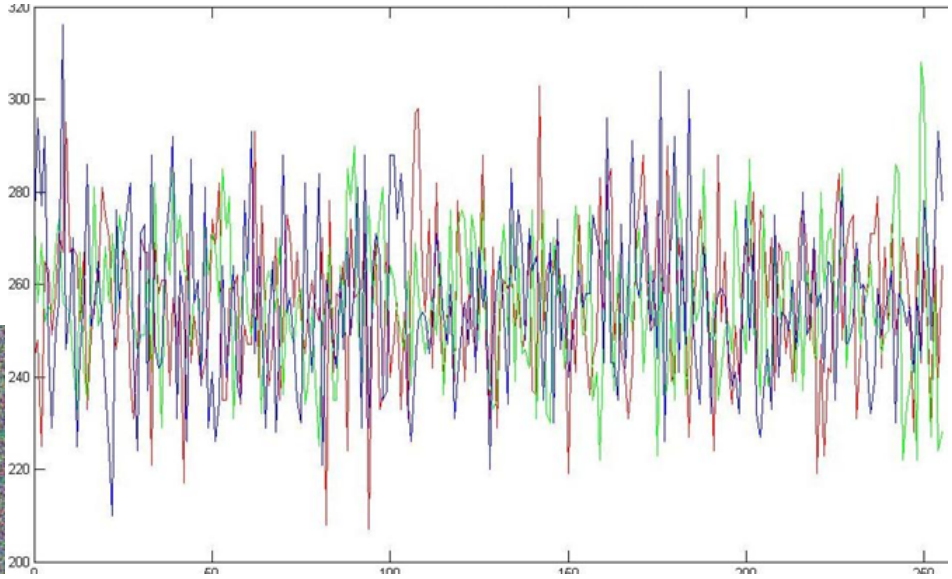
The tests images that are used in the system performance evaluation are in size of 256*256 and shown in Fig. 3.

As explained before, the CL system is used for encryption process by changing the values of the image's pixels. Then, the tests' results are evaluated after the CL implementation on these images and



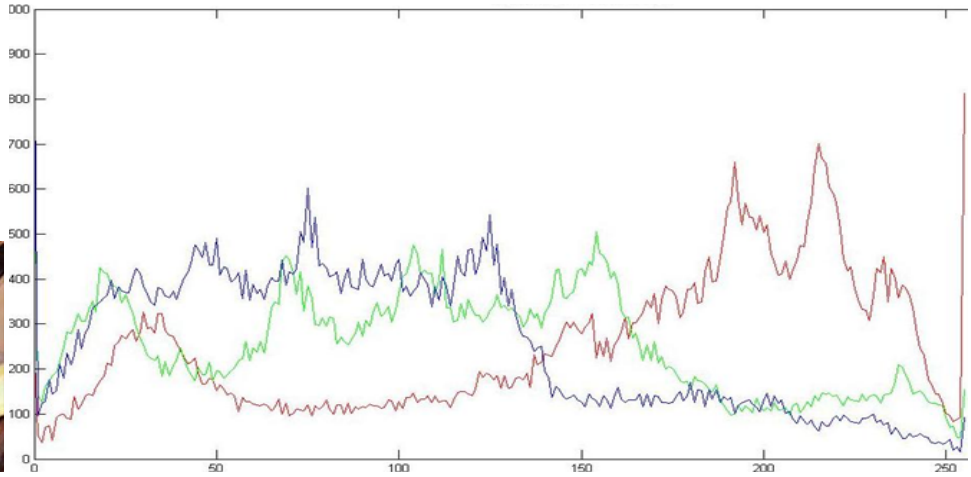
(a) Original image

Histogram of the original image

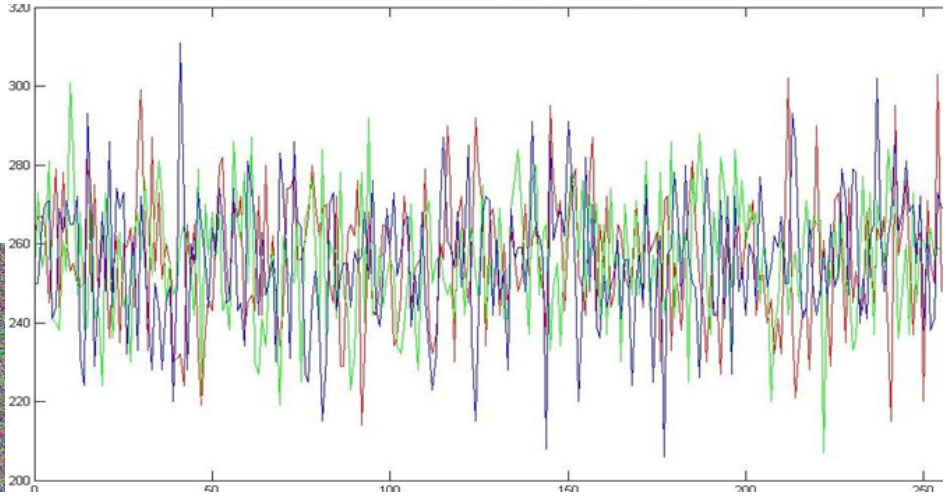


(b) Image after encryption with $x_0 = y_0 = z_0 = 0.1$

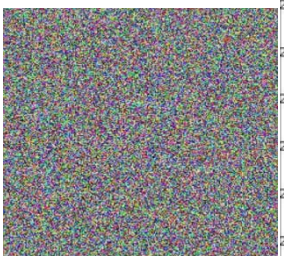
Histogram of the encrypted image

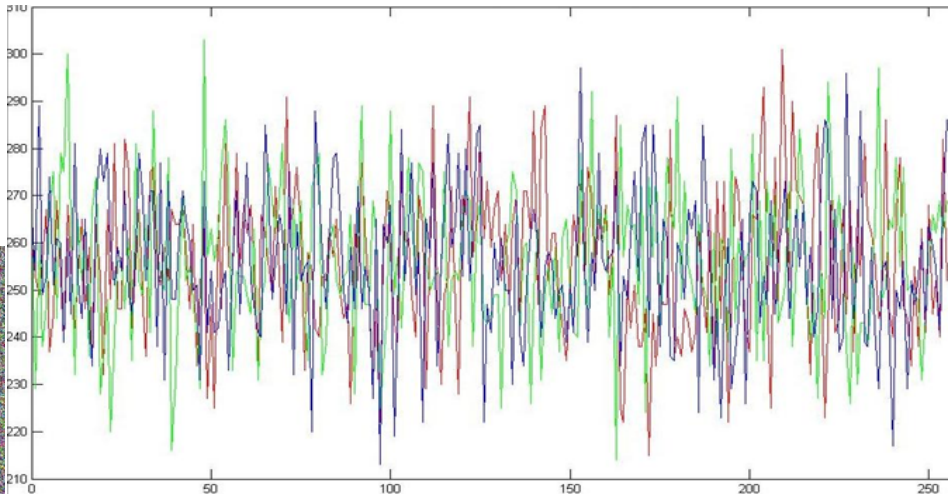


(c) Decrypted image using the same initial conditions and parameters Histogram of decrypted image



(d) Decrypted image when x_0 becomes 0.1000001 Histogram of decrypted image





(e) Decrypted image when a becomes 10.000001 Histogram of decrypted image

Fig. 2: Lina test image and its histogram with correct and incorrect decryption process

(a) Lena (b) Barbara (c) Baboon

(d) Peppers (e) Cube (f) Airplane

Fig. 3: Tests' images for CL system evaluation performance

Table 3: CL and traditional system evaluation performance tests results

Image name	Original entropy	Test type	Lorenz	Ross.	Nien	Chua	CL
Lena	7.7909	EQ	131.1404	131.14626	131.1514	131.146	131.147
		ARE	187.6016	188.29427	187.5443	188.26	188.055
		Corr.	-0.00203	-0.003873	0.000474	-0.003	0.0036
		Entropy	7.999113	7.9990752	7.998964	7.99914	7.99913
		ID	45082.67	45620.667	44051.33	44996	46537.3
		Md	47614.83	47802	47600.67	47777.7	47743.5
		PSNR	8.591016	8.5811673	8.600318	8.58492	8.60403
Barbara	7.6456	EQ	108.5162	108.51456	108.5158	108.507	108.512
		ARE	161.7995	162.0651	162.5365	162.57	163.078
		Corr.	-3.62E-05	-1.69E-03	-0.0005	-0.0041	-0.0007
		Entropy	7.999091	7.9990441	7.999078	7.99912	7.999
		ID	51897.33	52825.333	49641.33	50287.3	49682
		Md	41183.83	41235.333	41356.33	41364.3	41495.2
		PSNR	8.852987	8.8353576	8.829191	8.82354	8.82881
Baboon	7.7545	EQ	125.3861	125.38245	125.3857	125.385	125.384
		ARE	142.2422	142.29167	142.026	142.003	142.18
		Corr.	1.36E-05	-0.001986	-7.14E-05	-0.0026	-0.002
		Entropy	7.998976	7.9990751	7.999064	7.99905	7.99917
		ID	50584.67	50442.667	47118.67	50691.3	50430
		Md	36150	36184.5	36097.5	36101.7	36142
		PSNR	8.794992	8.792838	8.806537	8.78922	8.79186
Cube	4.6606	EQ	60.83959	60.76093	60.83389	60.7351	60.6638
		ARE	819.4141	819.28385	819.638	819.628	820.008
		Corr.	0.002559	0.0007121	0.000617	8.9E-05	-0.0009
		Entropy	7.999374	7.999421	7.999464	7.99948	7.99951
		ID	47312	46994.667	44516	47549.3	43292.7
		Md	167653	167613.83	167706.7	167702	167797
		PSNR	5.758049	5.7497712	5.748341	5.75021	5.74282
Peppers	7.6629	EQ	102.9658	102.95813	102.8966	102.933	102.942
		ARE	199.4219	200.46875	199.9089	199.096	200.69
		Corr.	0.002789	0.0004242	-0.00024	-0.0026	0.00053
		Entropy	7.998906	7.9991012	7.99909	7.99896	7.99909
		ID	43395.33	44042.667	42976	45894.7	41578
		Md	49645.33	49916.667	49765.83	49560.8	49969.8
		PSNR	8.137196	8.1221491	8.120093	8.12462	8.11834
Airplane	6.6587	EQ	180.9754	180.97644	180.9817	180.994	180.994
		ARE	284.9349	285.27344	284.2266	284.964	285.276
		Corr.	0.002456	-0.004645	0.000766	-0.0042	0.001969
		Entropy	7.999046	7.9991529	7.998976	7.99882	7.99893
		ID	41118.67	43359.333	41702.67	43308	42154.67
		Md	72710.33	72807	72546.83	72734.5	72821.67
		PSNR	7.975817	7.9608048	7.983654	7.96419	7.985018

compared with the traditional systems implementation's results as shown in Table 3.

According to the tests results in Table 3, it could be notice that:

- In all cases, The CL performance is either very near from the best test result of the traditional system or it has the better result.
- The CL performance is the best system for image pixel's value changing when the image is more regular, which is mean that the system is almost has the highest randomness behavior between all chaotic systems.

CONCLUSION

A novel chaotic system designed by mixing two chaotic systems is proposed in this study. The system has been tested using 0-1 test and FIPS PUB 140-1 statistical tests to test its chaotic characteristics and to check its randomness characteristics. The encryption key generated from the proposed system is used for digital RGB image encryption by using the XOR logic. If an intruder stole the encrypted image, it is impossible to reconstruct the original image because the CL system is unpredictable and has higher sensitivity to the initial conditions and the variable (parameter) values.

REFRENCES

Ahmad, J. and F. Ahmed, 2012. Efficiency analysis and security evaluation of image encryption schemes. Int. J. Vid. Image Process. Netw. Secur., 12(4): 18-31.

Aziz, M.M. and M.N. Faraj, 2012. Numerical and chaotic analysis of CHUA'S circuit. J. Emerg. Trends Comput. Inform. Sci., 3(5): 783-791.

Cuomo, K.M., A.V. Oppenheim and S.H. Strogatz, 1993. Synchronization of lorenz-based chaotic circuits with applications to communication. IEEE T. Circuits-II, 40(10): 626-633.

Dawes, J.H.P. and M.C. Freeland, 2008. The '0-1 Test for Chaos' and Strange Nonchaotic Attractors. Centre for Mathematical Sciences, Wilberforce Road, Cambridge, pp: 1-6.

FIPS (F.I.P.S.), 2002. Security Requirements for Cryptographic Modules. FIPS PUB 140-2.

Gorji, R.B., M.H. Shirvani and F.R. Mooziraji, 2015. A new image encryption method using chaotic map. J. Multidisc. Eng. Sci. Technol., 2(2): 251-256.

Gottwald, G.A. and I. Melbourne, 2009. On the implementation of the 0-1 test for chaos. SIAM J. Appl. Dynam. Syst., 8(2009): 129-145.

Jolfaei, A. and A. Mirghadri, 2010. A new approach to measure quality of image encryption. Int. J. Comput. Netw. Secur., 2(8): 38-43.

Merah, L., A. Ali-Pacha, N.H. Said and M. Mamat, 2013. Design and FPGA implementation of lorenz chaotic system for information security issues. Appl. Math. Sci., 7(5): 237-246.

Moghtadaei, M. and M.R. Hashemi Golpayegani, 2012. Complex dynamic behaviors of the complex Lorenz system. Sci. Iran., 19(3): 733-738.

Nien, H.H., C.K. Huang, S.K. Changchien, H.W. Shieh, C.T. Chen and Y.Y. Tuan, 2007. Digital color image encoding and decoding using a novel chaotic random generator. Chaos Soliton. Fract., 32(3): 1070-1080.

Sambas, A., W.S. Mada Sanjaya and H. Tussadiyah, 2012. Unidirectional chaotic synchronization of rossler circuit and its application for secure communication. WSEAS T. Syst., 9(11): 506-515.

Song, C. and Y. Qiao, 2015. A novel image encryption algorithm based on DNA encoding and spatiotemporal chaos. Entropy, 17(10): 6954-6968.

Sprott, J.C., 2015. New chaotic regimes in the lorenz and chen systems. Int. J. Bifurcat. Chaos, 25(2).

Vaidyanathan, S., 2011. Hybrid synchronization of liu and lü chaotic systems via adaptive control. Int. J. Adv. Inform. Technol., 1(6): 13-32.