Journal of Applied Sciences Research, 7(4): 392-399, 2011
ISSN 1995-0748
This is a refereed journal and all articles are professionally screened and reviewed

ORIGINAL ARTICLES

Image Encryption Based on Synchronized Communication Chaotic Circuit

[1]Qais H. Alsafasfeh and [2]Abdel Ilah Alshbatat

[1]PhD, Tafila Technical University, Electrical Engineering Department, Tafila- Jordan 66110 P.O.Box 179,
[2]PhD, Tafila Technical University, Electrical Engineering Department, Tafila- Jordan 66110 P.O.Box 179,

ABSTRACT

The chaotic behavior of the circuit closely matches the results predicted by numerical experiments. In this paper we using the concept of synchronized chaotic systems, two possible approaches to Image encryption are demonstrated with the Cuomo circuit implemented in both the transmitter and receiver. This scheme employs the two similar circuits exhibiting chaotic behavior were assembled. Each circuit, when sharing a driving signal, produced the same chaos, and behaved exactly similar. An image was then added to the chaos of one circuit, and the chaos was extracted from the Image in the next circuit, allowing an encrypted image to be sent.

Key words: Lorenz equations, Chaos, Cuomo Circuit

Introduction

Chaos, up to a few years ago, was just an interesting field to researchers who studied the behavior of nonlinear dynamical systems of certain mathematical structure. Chaotic systems are frequently viewed in phase space, which is a region of space where the current state of the system perpetually exists (Carroll, 1997). Many physical systems, particularly those studied in introductory physics classes, exhibit linear dynamics: they behave in a completely predictable and deterministic way (Wang,2008). Given the system and initial conditions their behavior is quite routine and, to a degree, uninteresting. Newtonian mechanics is a prime example of such a system. However, the world of nonlinear systems gives rise to a fairly new concept in math and physics: chaos is the term given to the seemingly random results emerging from a physical system (Gao, 2006). Chaos often appears to be periodic, but is, in fact, not; chaos is in essence 'controlled' randomness. It is difficult if not entirely impossible to make accurate long term predictions about chaos. The solutions exhibit an extreme sensitivity to initial conditions (Cuomo, 1993).

Chaotic systems are nonlinear systems which are well defined mathematically and contain no random variables. It would seem that a definite prediction of the model could be found in these systems. However, solutions tend to not follow a set pattern, as the well defined system would imply(Carroll, 1997).

2. *The Chaos-Based Encryption*:

Image encryption algorithms were proposed in the literature to meet the demand for fast and highly secure image transmission. Unfortunately, traditional image encryption methods were reported with low-level efficiency (Cuomo, 1993). . The chaos-based image encryption provides an efficient solution for this problem. . The first chaotic encryption algorithm was proposed by Matthews in 1989 (Gao ,2006). Recently, there have been varieties of work based on chaotic encryption scheme such as (Fu 2007, Zhang, 2005, Bu, 2004, Wang, 2008 and Ahmed, 2007). These methods have high-level efficiency but have small key space, weak security, and high computational complexity. To overcome these drawbacks, an encryption algorithm based on Cuomo circuit is proposed in this paper.

Corresponding Author: Qais H. Alsafasfeh,Tafila Technical University, Electrical Engineering Department, Tafila - Jordan 66110 P.O.Box 179.
Email: qsafasfeh@ttu.edu.jo, qshashim@yahoo.com

3. *Lorenz System:*

The Lorenz equations are a fairly simple model in which to study chaos.

$$\begin{aligned}\dot{x} &= \sigma(y - x)\\ \dot{y} &= rx - y - xz\\ \dot{z} &= xy - bz\end{aligned} \tag{1}$$

The arbitrary parameters $\sigma,r,b > 0$ and for this example are $\sigma = 10$, $r = 28$, $b = 8/3$. This system of differential equations is then solved numerically using RungeKutta .The system is deceptively simple; it is merely a set of 3 ordinary differential equations. However, chaos emerges from the set of Lorenz equations (Cuomo, 1993).

4. *Chaos in Circuits*:

Another physical system which can be easily exploited to create chaos is electronic circuits. Circuits can be easily constructed, consisting mainly of readily available and cheap parts. In fact, one only needs several op amps, resistors and capacitors to create chaos in the voltage output of the circuit.

Now two nearly identical Lorenz circuits are studied; one acts as the transmitter and the other as the receiver. The transmitter parameters are such that the circuit is in the Lorenz chaotic regime. The transmitter signal $x(t)$ is fed into the receiver into certain way, with the result that the receiver quickly synchronizes to the transmitter, starting from any initial conditions (Cuomo,1993).

A direct implementation of (1) with an electronic circuit. An appropriate transformation this new scaling the Lorenz equations are transformed to

$$\begin{aligned}\dot{u} &= \sigma(v - u)\\ \dot{v} &= ru - v - 20u\,w\\ \dot{w} &= 5u\,v - bw\end{aligned} \tag{2}$$

this system. which we refer to as transmitter, can be more easily implemented with an electronic circuit because the stale variables all have similar dynamic range and circuit voltages remain well within the range of typical power supply limits.

An analog circuit implementation of the circuit in the equations in (2) is shown in Figure 1(Gao,2006 and Fu., 2007).

By applying standard node analysis techniques to the circuit of Figure 1, a set of state equations that govern the dynamical behavior of the circuit can be obtained. This set of equations is given by

$$\begin{aligned}\dot{u} &= \frac{1}{R_5C_1}\left[\frac{R_4}{R_1}v - \frac{R_3}{R_3 + R_2}\left(1 + \frac{R_4}{R_1}\right)\right]\\ \dot{v} &= \frac{1}{R_{15}C_2}\left[\frac{R_4}{R_4 + R_4}\left(1 + \frac{R_{12}}{R_8} + \frac{R_{12}}{R_9}\right)\left(1 + \frac{R_7}{R_6}\right)u - \frac{R_{12}}{R_8}v - \frac{R_{12}}{R_9}uw\right]\\ \dot{w} &= \frac{1}{R_{20}C_3}\left[\frac{R_{19}}{R_{16}}uv - \frac{R_{18}}{R_{17} + R_{18}}\left(1 + \frac{R_{19}}{R_{16}}\right)w\right]\end{aligned} \tag{3}$$

to find the value of all parameters of the above circuit we will take $\sigma = 10$, $r = 20$, $b = 2$ and compare between Eq. 2 and 3 and make scaling for R_5, R_{15}, R_{20} by 20000 then the value of the parameters is:

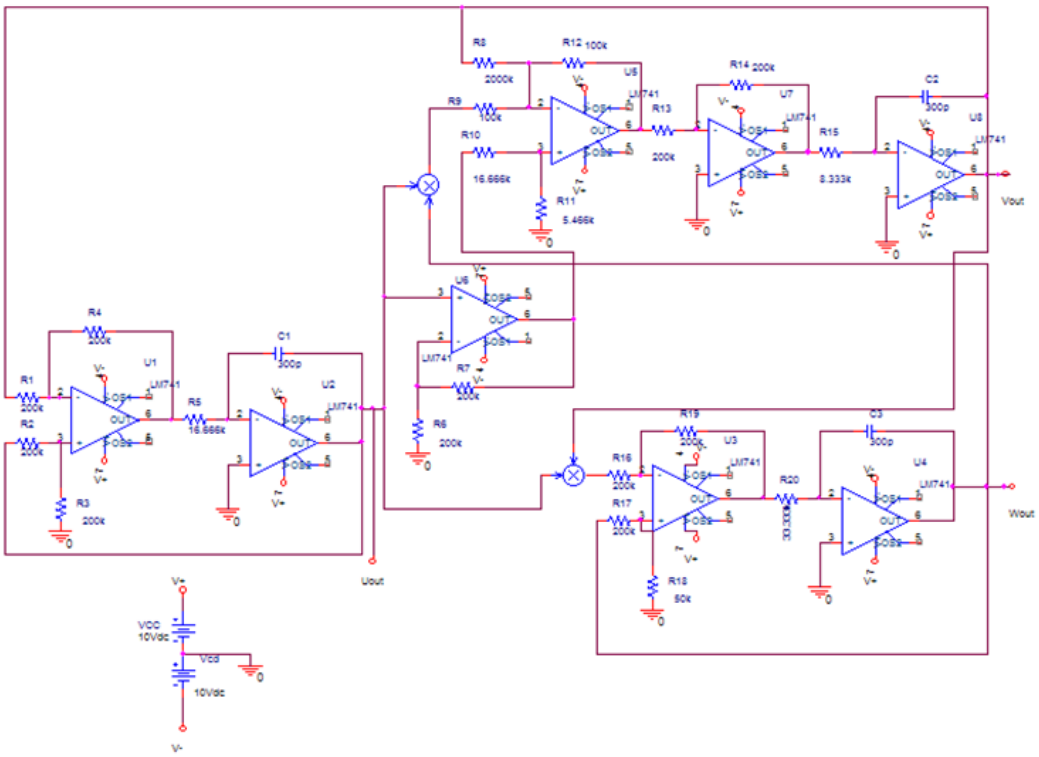

Fig. 1: Synchronizing chaotic transmitter circuit.

$$R_1, R_2, R_3, R_4, R_6, R_7, R_{13}, R_{14}, R_{16}, R_{17}, R_{19} = 200k\Omega, R_{12} = R_9 = 100k\Omega, R_8 = R_{17} = 2000\Omega$$
$$, R_5 = R_{10} = 16.666k\Omega, , R_{18} = 50k\Omega, , R_{11} = 5.466k\Omega, , R_{15} = 8.333k\Omega, C_1 = C_2 = C_3 = 300\,pF$$

to illustrate the chaotic behavior of the transmitter circuit, Figure 2 shows a sample function corresponding to the circuit waveform u(t). Figure 3, 4 shows the circuit's chaotic attractor projected onto the uv-plane and uw-plane, respectively. A full-dimensional response system that will synchronize to the chaotic signals at the transmitter (4) is given by

$$\begin{aligned} \dot{u}_r &= \sigma(v_r - u_r) \\ \dot{v}_r &= r u_r - v_r - 20 u_r w_r \\ \dot{w}_r &= 5 u_r v_r - b w_r \end{aligned} \tag{4}$$

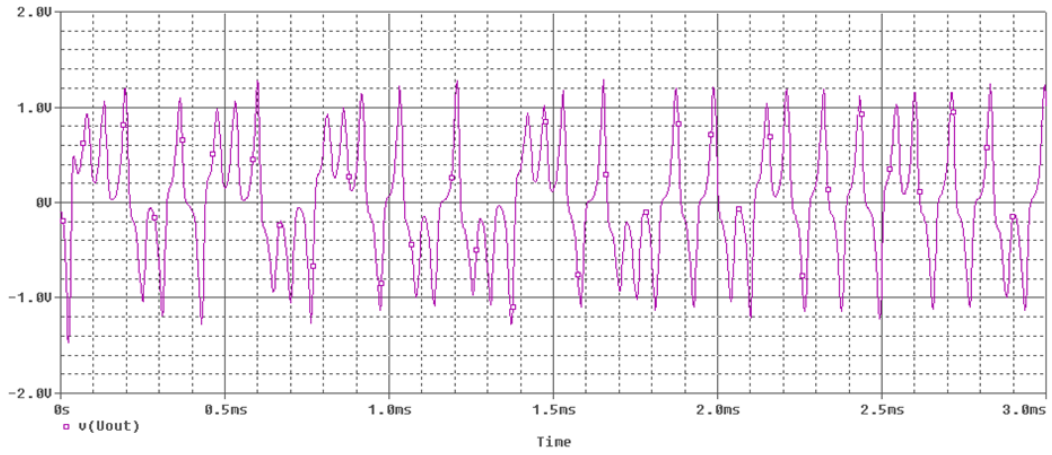

Fig. 2: Time series of u(t) waveforms generated.

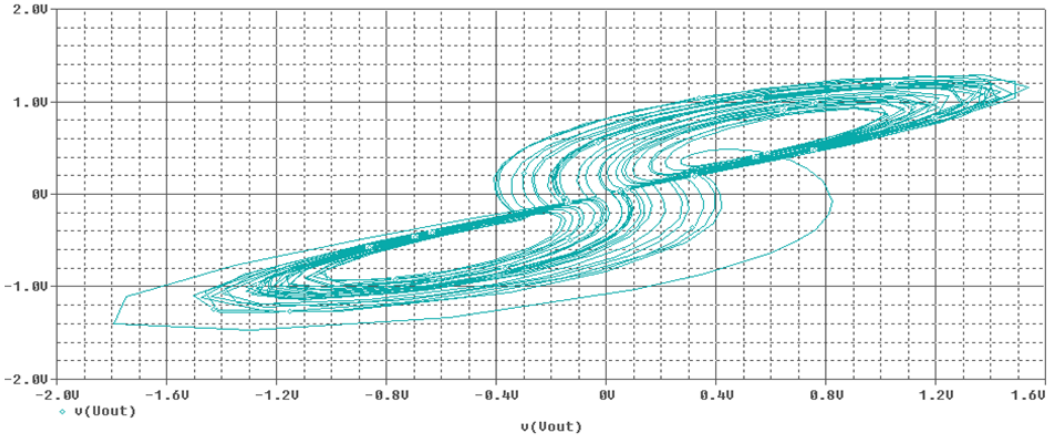

Fig. 3: Chaotic attractor projected onto uv-plane.

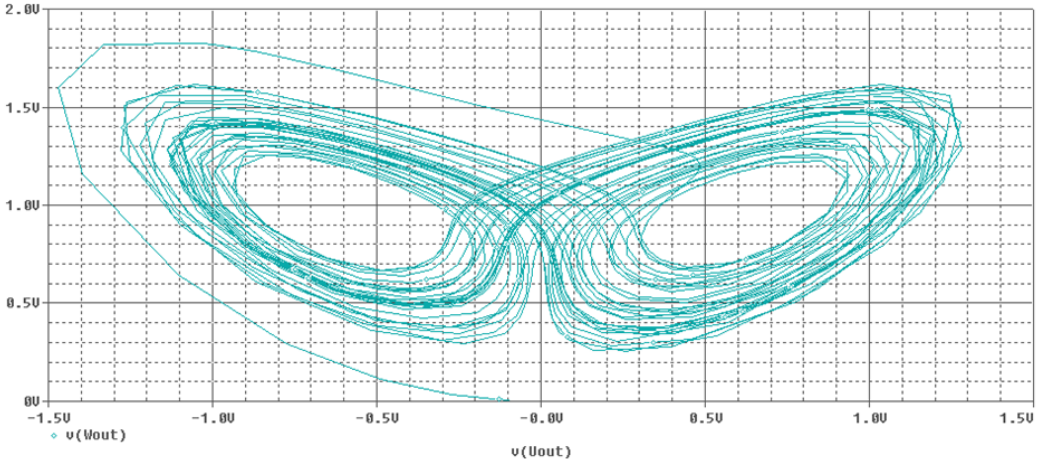

Fig. 4: Chaotic attractor projected onto uw-plane.

An electronic implementation of the receiver equations (3) is shown in Figure 5.

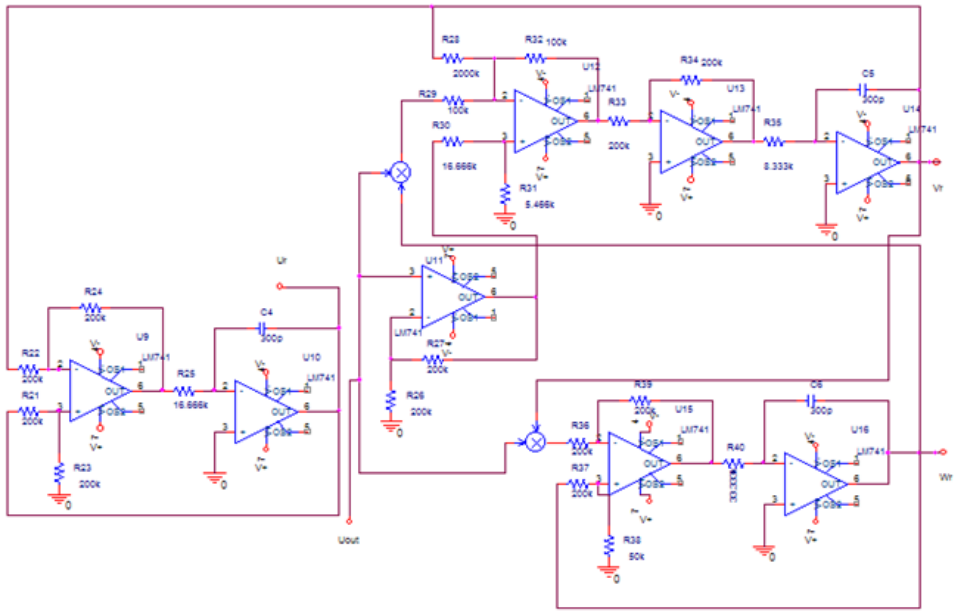

Fig. 5: Synchronizing chaotic receiver circuit.

The practical advantage of this similarity is that the transmitter and receiver circuits can be built in an identical way, which helps to achieve perfect synchronization between the transmitter and receiver illustrate the synchronization performance of the receiver circuit. In Figure 6 a plot of the actual circuit outputs u(t) versus $u_r(t)$ is shown. Figure 7 shows a similar plot for the circuit outputs v(t) and $v_r(t)$. The 45° lines indicate that nearly perfect synchronization is achieved and maintained between the transmitter and receiver (Gao, H.,2006).

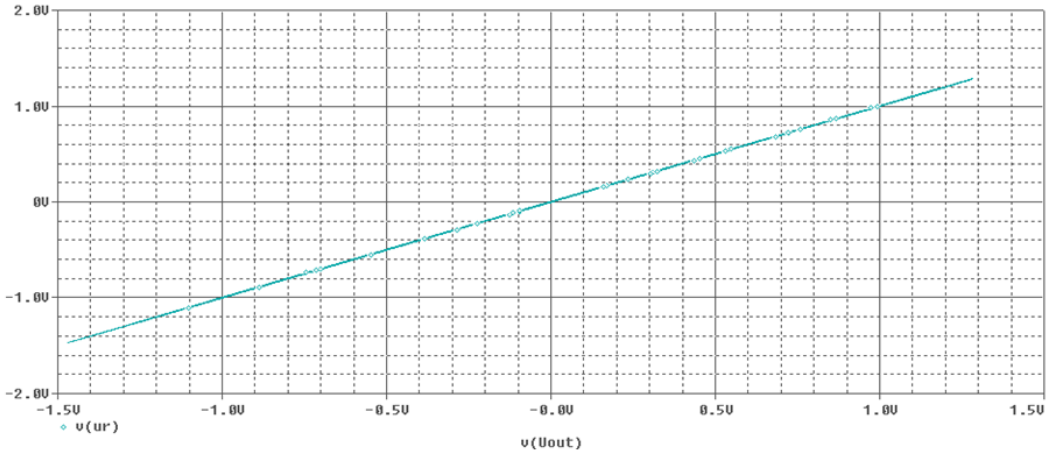

Fig. 6: Synchronization of transmitter and receiver signals.

5. Encryption Based Cuomo Chaotic Circuit:

Since each circuit is able to reproduce the same signal, chaos begins to have practical applications. A secret signal can be embedded with the chaos of one circuit. The result in signal appears to be only chaos and noise, and is useless. With the synchronizing circuit producing the same signal, however, the chaos can be extracted from the image, leaving only the secret signal. Thus, chaos can be used as a form of encryption encoding.

The image encryption is based on the proposed Cuomo chaotic circuit. Generated elements have been stored within the chaotic matrix of size the same as the original image's size. As with the other algorithms that made use of the XOR operation to encrypt, decryption is a simple matter of recreating the matrix of chaotic elements and XORing it with the encrypted image matrix. The actual procedure for encryption that this paper proposed is:

Step 1: Set the key (initial condition and parameters $(\delta, \beta, r, y_o, x_o, z_o)$ in the acceptable intervals.

Step 2: Generate the first mask with the same size of image.
Step 3: Perform the XOR between the chaotic mask and original image.
Step 4: If the image is not encrypted generate the second mask with the same size of image.
Step 5: Perform the XOR between the chaotic mask and image in step 3.
Step 6: If the image is not encrypted generate the third mask with the same size of image.
Step 7: Perform the XOR between the chaotic mask and image in step 5.
Step 8: Pass the encrypted image
Step 9: Pass the encryption key.
Step 10: End

6. Experimental Results:

Experimental results and performance analysis of the proposed image encryption scheme are shown in this section using Lena image. An 8-bit Lena image of size 256x256 is shown in Figure 8 (a) while Figure 8 (b) shows the encrypted image. The encryption initial parameters were set as $(\alpha, \beta, \gamma, \tau, x_o)$ = (1.47, 5, 4.876545676545671, 2.3) with initial conditions for each generated mask as (x_{10}, x_{20}, x_{30}) =

(0.987654321012345, 0.345645477457451, 0.34564547745745). As shown in Figure 8 (b), the encrypted image is rough-and-tumble and unrecognizable. As Figure 8(c) shows, the decrypted image using the same encryption key is an exact version of the original Lena image. Figure 8 (d) shows the error between the original image and decrypted image, which is zero.

Fig. 8: (a) original Image (b) encrypted Image, (c) Decrypted Image (f) error between original and encrypted image.

Statistical analysis has been performed on the proposed image encryption algorithm, demonstrating its superior confusion and diffusion properties which strongly resist statistical attacks. This is shown by a test on the histograms of the enciphered images and on the correlations of adjacent pixels in the ciphered image.

1. Histogram of the encrypted image: the histogram of the encrypted image is fairly uniform and is significantly different from that of the original image that is the encrypted image is unrecognizable as shown in Figure 9.

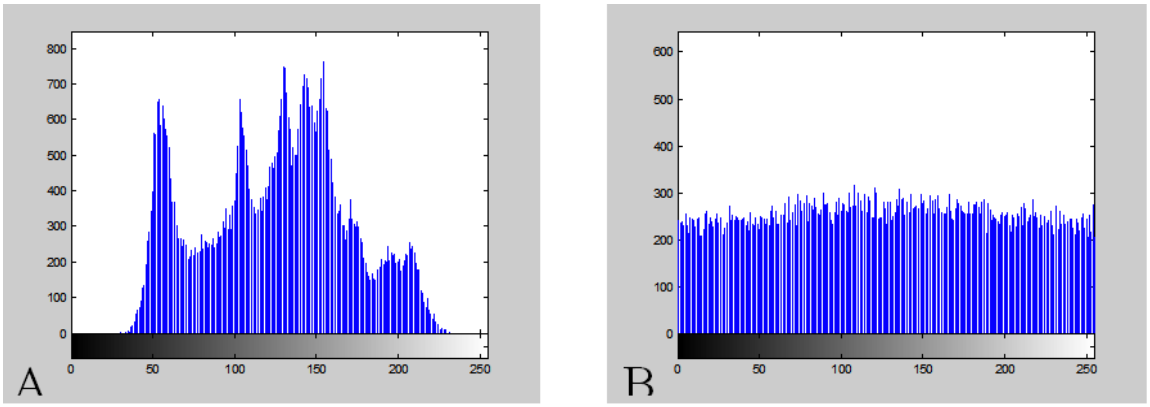

Fig. 9: Histogram of Original Image and Encrypted.

2. The correlation between two vertically adjacent pixels: Two horizontally adjacent pixels and two diagonally adjacent pixels can be found using Eq. 4:

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

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

$$\text{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \quad (6)$$

$$g_{xy} = \frac{\text{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

where E(x) is the expected value and N is the number of pixels. Figure 10 shows the correlation results of the adjacent pixels of the original and encrypted image. As Table 1 shows, the encrypted image has very small or negative correlation. This is a positive indicative of the robustness of the proposed encryption method.

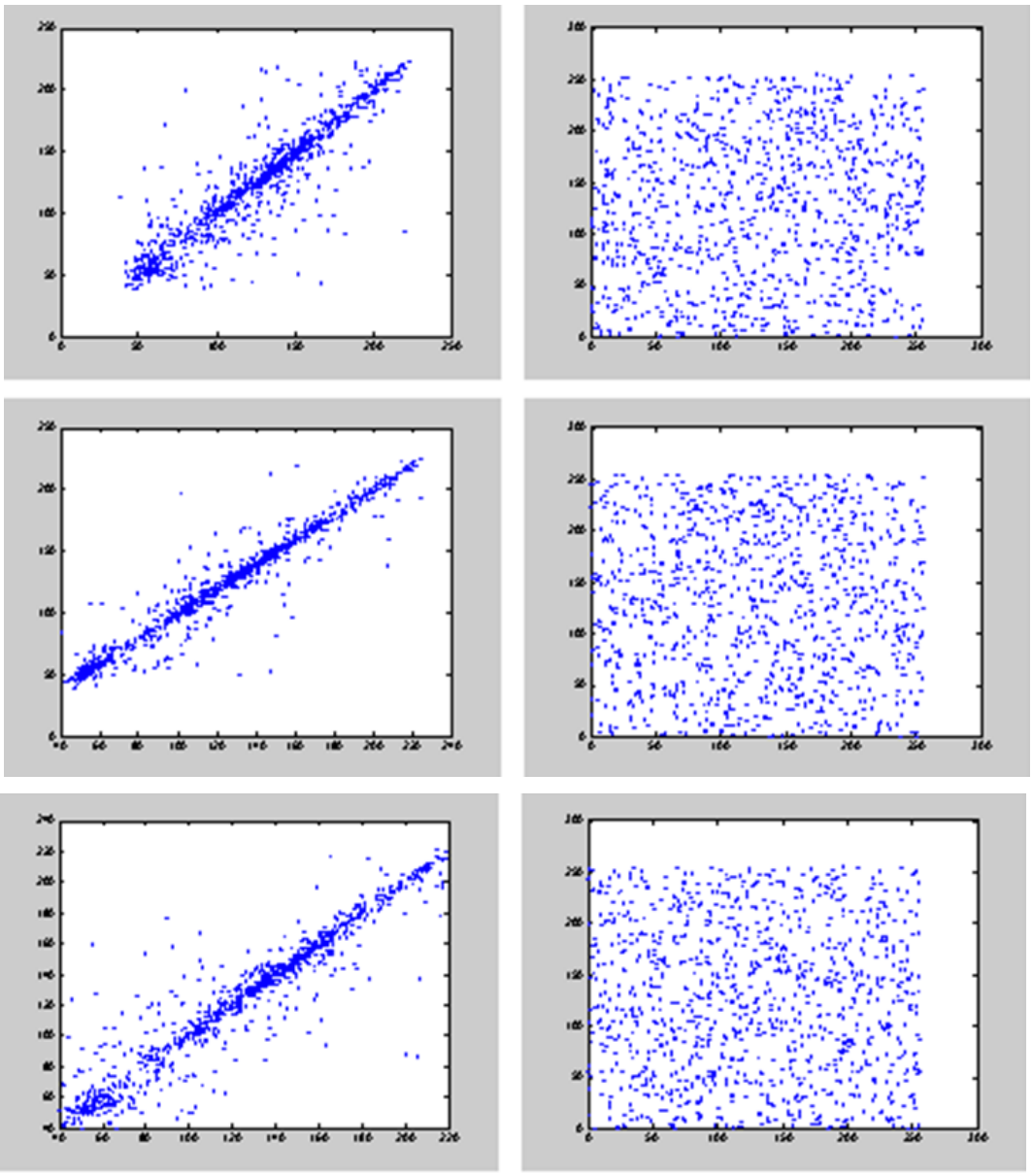

Fig.10: Correlations of two diagonal, horizontally and vertical adjacent pixels in the Plain Image and in the cipher-image.

Table 1: Correlation between adjacent pixels in the original and encrypted image.

	Plain image	Ciphered image
Horizontal	0.9681	0.0847
Vertical	0.9434	-0.0274
Diagonal	0.9238	-0.0174

3. Information Entropy: A higher value of information entropy indicates a fairly uniform histogram. Ideally, entropy of an encrypted image should be 8 to prevent attackers from obtaining much image information through entropy analysis (Wang, L.,2008). The entropy of the encrypted Lena image is 7.9952 which mean that information leakage in the encryption process is negligible and the encryption system is secure against the entropy attack.

4. Differential Analysis: the attacker may make a slight change such as modifying only one pixel of the encrypted image and then observing the change of the result (Ahmed, H.E.2007). Two common measures can be used for the differential analysis: the number of pixels change rate (NPCR) and the unified average changing intensity (UACI) as defined by 5 and 6. Let us take two encrypted images, *C1* and *C2* each of size W-by-H, whose corresponding original images have only one-pixel difference. A 2-D array *D* is

   defined as: if $C_1(i,j) = C_2(i,j)$ then $D(i,j) = 1$, otherwise $D(i,j) = 0$, then

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \tag{5}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\% \tag{6}$$

The obtained NPCR for the encrypted Lena image is found it to be over 99% and UACI is 2.5% showing robustness of the proposed encryption scheme.

For a secure image cipher, the key space should be large enough to make the brute force attack infeasible. The key of the new algorithm consists of three floating-point numbers. If we use the first 15 digits of a floating-point number, then there are 15 + 15 + 15 = 75 uncertain digits. So the possible key number is 10^{45}.An image cipher with such a long key space is sufficient for reliable practical use.

Apart from the security consideration, running speed of the algorithm is also an important aspect for a good encryption algorithm. We have measured the encryption/decryption rate of on 256 grey-scale images of size 256 x 256 by using the proposed image encryption scheme. The time analysis has been done on Pentium-4 with 512 MB RAM computer, the average encryption/decryption time is 0.4 s.

7. Conclusions:

In this paper, Lorenz system and Cuomo circuit implementation is used for image encryption. The transmitter circuit is exploited in order to send encrypted image that is almost impossible to decode without the driving signal and the appropriate receiver circuit. The receiver circuit is exploited to decode the encrypted image and recover the original image. Results indicate that the proposed scheme is a simple yet very secure system.

REFERENCES

Ahmed, H.E., H.M. Kalash and O.S. Allah, 2007. Encryption efficiency analysis and security evaluation of rc6 block cipher for digital images, International Journal of Computer, Information, and Systems Science, and Engineering, 1(1): 33-39.

Atkinson, K.E., 1989. An introduction to numerical analysis, John Wiley & Sons.

Bu, S. and B.H. Wang, 2004. Improving the security of chaotic encryption by using a simple modulating method, Chaos, Solitons and Fractals, 19(4): 919-924.

Carroll, T.L. and L.M. Pecora, 1990. Synchronization in chaotic systems, Phys. Rev. Letter, 64(8): 821-824.

Cuomo, K.M. and V. Alan, 1993. Circuit implementation of synchronized chaos with applications to communications, Physical Review Letters, 71(1): 65-68.

Cuomo, K.M., A.V. Oppenheim and S.H. Strogatz, 1993. Synchronization of lorenz-based chaotic circuits with applications to communications, IEEE transactions on circuits and systems-II: analog and digital signal processing, 40(10): 626-633.

Fu, C., Z.C. Zhang and Y.Y. Cao, 2007. An improved image encryption algorithm based on chaotic maps, Third International Conference on Natural Computation, ICNC 2007: 24-27.

Gao, H.,Y. Zhang, S. Liang and D. Li, 2006. A new chaotic algorithm for image encryption, Chaos, Solitons and Fractals, 29: 393-399.

Wang, L., Q. Ye, Y. Xiao, Y. Zou and B. Zhang, 2008. An image encryption scheme based on cross chaotic map, Image and Signal Processing, 3: 22-26.

Zhang, L., X. Liao and X. Wang, 2005. An image encryption approach based on chaotic maps, Chaos, Solitons and Fractals, 24(3): 759-765.