Masking System Design for Gray-Level Images Using Finite Time Synchronization of two Chaotic Lorenz Systems

Julio C. Rolón Garrido, Leonardo Acho Zuppa[1], and Víctor Hernández Rosas
Centro de Investigación y Desarrollo de Tecnología Digital (CITEDI-IPN)
Tijuana B.C., México
Correspondence: CITEDI-IPN 2498 Roll Dr. #757, Otay Mesa, San Diego, California, 92154, USA

Tel.: +(52-664) 623-13-44 ext. 82832
Fax : +(52-664) 623-13-88

Abstract: - The present paper describes the design of a chaotic masking system with application to the encryption – decryption of gray-level images using finite time synchronization of two chaotic Lorenz systems. The discrete implementation was realized using the Euler's approximation of the masking system design proposed in the continuous time domain. Lyapunov theory is invoked to prove finite time convergence for the synchronization algorithm; *MSE* (Mean Square Error) and *PSNR* (Peak of the Signal-to-Noise) criteria were employed to evaluate potential degradation of the image quality because of the encryption-decryption process.

Key-Words: - Finite time convergence, Synchronization, Lorenz systems, Masking systems.

1. Introduction

The design of systems with finite time convergence has been studied, among others, in [2], [7], and [9]. More recently, the synchronization problem has been of great interest, see for example, [3], [4], [5], [6] and references there in; however, none of them has considered the problem of masking systems design based on finite-time synchronization algorithm of two chaotic Lorenz systems. The objective of this paper is to present a masking system design with application to the encryption – decryption of gray-level images using the finite time synchronization of two chaotic Lorenz systems presented in [1]. The finite time synchronization of two chaotic Lorenz systems was possible by adding two relay terms to the synchronization problem formulation given in [5]. We used this formulation in combination with the masking system design given in [10], which proved to be applicable with our synchronization formulation (in [10] a different synchronization algorithm is proposed). The resultant masking system was then transformed to a discrete version using Euler's method and utilized to encrypt and decrypt gray-level images. Simulation results are shown to support our main result.

2. Problem Formulation

The Lorenz system is given by

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

where *σ, r*, and *b* are constant parameters. With *σ=16*, *r=45.6* and *b=4*, the Lorenz system presents chaotic behavior [1].

The system (1) is referred as the transmitter, where *x(t)* is the transmitted signal used by the receiver system given by

$$\begin{aligned} \dot{x}_r &= \sigma(y_r - x_r) + k_1 \sigma sign(x - x_r) \\ \dot{y}_r &= rx - y_r - xz_r + sign(x - x_r) \\ \dot{z}_r &= xy_r - bz_r \end{aligned} \tag{2}$$

where k_1 is a positive constant, and

$$sign(z) = \begin{cases} 1, & if\ z > 0 \\ 0, & if\ z = 0 \\ -1, & if\ z < 0 \end{cases}$$

The above dynamic system is a modification of the receiver system proposed in [5] but the relay terms. These relay terms provide finite time convergence

[1] This work was partially supported by the Mexican Council for Science and Technology (CONACyT).

[1]. The receiver system only uses the transmitted signal *x(t)* as its input.

Let us define the state errors between the transmitter and the receiver systems as

$$e_1 = x - x_r,\ e_2 = y - y_r,\ e_3 = z - z_r \qquad (3)$$

Subtracting (2) from (1) and using (3) we have

$$\begin{aligned} \dot{e}_1 &= \sigma(e_2 - e_1) - k_1\sigma\, sign\ (e_1) \\ \dot{e}_2 &= -e_2 - xe_3 - sign\ (e_1) \\ \dot{e}_3 &= xe_2 - be_3 \end{aligned} \qquad (4)$$

The synchronization problem can be stated using the error dynamics (4) and it is equivalent to asymptotically stabilizing this error dynamics. The finite time synchronization problem consists in that for any initial conditions *e₁(0), e₂(0)* and *e₃(0),* the solution of the system (4) *e₁(t), e₂(t)* and *e₃(t),* reach the origin ($e_1=e_2=e_3=0$) as *t* tends to infinity, and, besides

$$\lim_{t\to t_s}\|e_1(t)\| = 0,$$

where t_s is the settling time. This settling time t_s is a function of the initial conditions (see [7]). In [9], Theorem 2, it is shown that a system converges in finite time almost everywhere with respect to a Lebesgue measure zero (*a.e.*) if, given a Lyapunov function *V,* its time derivative along the trajectories of the system is bounded by a negative number (i.e, $\dot{V} \le -k \quad a.e.,$ with *k>0*). Global finite time convergence (*a.e.*) is concluded if the Lyapunov function *V* is proper and $\dot{V} \le -k \quad a.e.$ (see [9]).

To prove finite time convergence *a.e* for the system (4), the next Lyapunov function is proposed (a proper one):

$$V = \frac{1}{2}\left(\frac{1}{\sigma}e_1^2 + e_2^2 + e_3^2\right) + \frac{1}{\sigma}|e_1|$$

where its time derivative along the trajectories of the system (4) yields:

$$\begin{aligned} \dot{V} &= \frac{1}{\sigma}e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3 + \frac{1}{\sigma}sign(e_1)\dot{e}_1 \\ &= -e_1^2 + e_1e_2 - e_2^2 - be_3^2 - |e_1| - k_1 - k_1|e_1| \\ &= -(e_1 - \frac{1}{2}e_2)^2 - \frac{3}{4}e_2^2 - be_3^2 - |e_1| - k_1 - k_1|e_1| \\ &\le -k_1 \quad a.e. \end{aligned}$$

Such that with $k_1>0$, the finite time synchronization problem is solved after Theorem 2 in [9] is invoked. When *e₁(t)* reach the value of zero, the final error dynamics is asymptotically stable. This fact follows because when *e₁(t)=0,* we obtain the same error dynamics that in [5] (of course, after using *e₁(t)*=0) that proves, that the origin, is asymptotically stable.

To estimate the settling time, we can integrate the expression obtained above,

$$\dot{V} \le -k_1 \qquad (5)$$

Integrating (5) from *0* to t_s, we obtain

$$-V(0) \le V(t_s) - V(0) \le -k_1 t_s$$

which means that

$$\begin{aligned} t_s &\le \frac{V(0)}{k_1} \\ &= \frac{1}{k_1}\left[\frac{1}{2}\left(\frac{1}{\sigma}e_1^2(0) + e_2^2(0) + e_3^2(0)\right) + \frac{1}{\sigma}|e(0)|\right] \end{aligned}$$

Remark 1.- Certainly, it is difficult to know the exact settling time t_s because the initial conditions of the transmitter are unknown and so are *e₁(0), e₂(0),* and *e₃(0)*. However, we can use some approximation to face this difficulty. The tri-dimensional phase portrait of the Lorenz system has an attractor surrounding the origin. This attractor can be enclosed by some sphere and we can use this sphere to bound the initial conditions of the transmitter for a proper operation; i.e., to preserve chaotic behavior of the transmitter for all *t>0*. ♦

3. Simulation Results

The systems (1) and (2) were programmed using MatLab. Fig.1 shows the state variables of the transmitter and the receiver. The initial conditions were *x(0)=5, y(0)=-10, z(0)=15,* $x_r(0)=-5$, $y_r(0)=10$, and $z_r(0)=-15$, and we selected $k_1=1$. Fig. 2 shows the error dynamics.

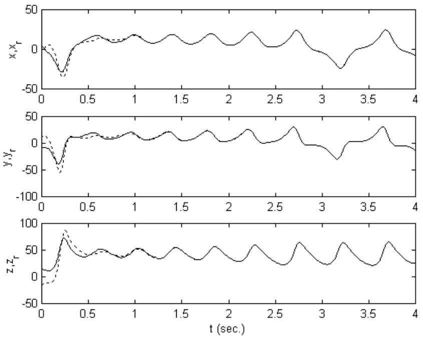

Fig.1 State variables of the transmitter (continuous lines) and the receiver (dotted lines).

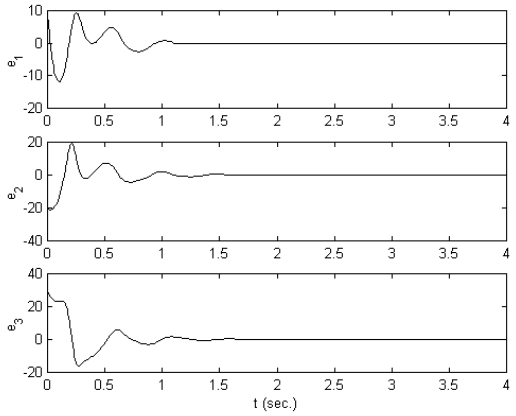

Fig. 2 State variables of the error dynamic.

4. Masking System Design

Following the masking system design presented in [10], we implemented the secure-communication system shown in Fig.3. This masking system is similar to the example given in section three of [10] except by the finite time synchronization part. The function *ϕ(y,s)* is called the encryption function where *s(t)* is the information signal, $s_e(t)$ is a transmitted signal, and $\psi(y_r,s_e)$ is the decryption function (for more details on these functions, see [10]). The encrypted and decrypted functions are such that:

a) ϕ is continuous in its argument and
b) For every fixed pair of *(x,s)*, ψ is continuous in its first argument and $\psi(x,\phi(x,s))=s$.

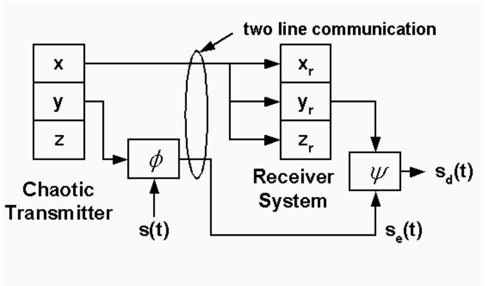

Fig.3 Masking system with two line communication.

For the purpose of numerical simulations, we select the following encryption and decryption functions (as in [10])

$$\phi(y,s) = 0.1(y^2 + (1+y^2)s)$$

$$\psi(y_r,\phi) = -\frac{y_r^{\,2}}{(1+y_r^2)} + 10\frac{\phi}{(1+y_r^2)}$$

The terms 0.1 and 10 were added to avoid high scale transmitted signals. We implemented the system in Fig.3 with Simnon where the simulation results obtained are shown in Fig.4. The initial conditions for the chaotic transmitter and the receiver system were the same than the used in section three.

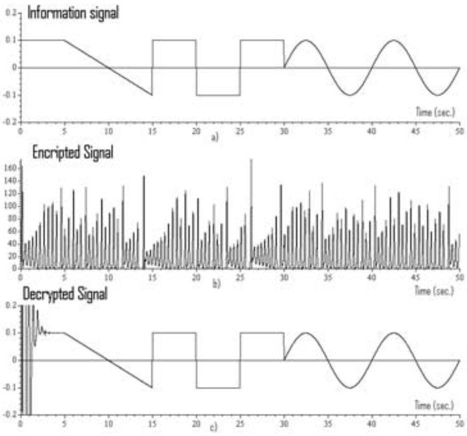

Fig.4 Simulation result.

5. Masking System Design for Gray-Level Images

We treat the system in Fig.3 to develop an algorithm to encrypt and decrypt gray-level images.

It is assumed that we have a gray-scale image as a two-dimensional array *A* where each element of the array *A* gives the intensity value of the image element (pixel), and the location of each pixel in the image is given by the coordinates of each element in *A*. It is also assumed that the value of “0” corresponds to a black intensity pixel and a “1” corresponds to a white intensity pixel; so, the 256 gray-levels are confined between these values. For the encrypted image, values out of this range ([0 1]) are assumed to be admissible.

The discrete algorithm proposed is based on the discretization of the chaotic transmitter and receiver systems given in equations (1) and (2), respectively. Because the receiver system contains terms that are no differentiable, the Euler’s method is used to give us the following discrete version of these dynamics:

$$\begin{aligned} x(k+1) &= x(k) + h[\sigma(y(k)-x(k))] \\ y(k+1) &= y(k) + h[rx(k) - y(k) - x(k)z(k)] \\ z(k+1) &= z(k) + h[x(k)y(k) - bz(k)] \end{aligned} \tag{6}$$

and

$$\begin{aligned} x_r(k+1) &= x_r(k) + h[\sigma(y_r(k)-x_r(k)) + k_1\sigma sign(x(k)-x_r(k))] \\ y_r(k+1) &= y_r(k) + h[rx(k) - y_r(k) - x(k)z_r(k) + sign(x(k)-x_r(k))] \\ z_r(k+1) &= z_r(k) + h[x(k)y_r(k) - bz_r(k)] \end{aligned} \tag{7}$$

where *h* is a constant value called the integration step. One possibility to select a value for *h* is such that the dynamic in (6) preserves its chaotic behavior. Fig.5 shows simulation results of the system (6) with *h=0.01*; this value of *h* is preserved hereafter.

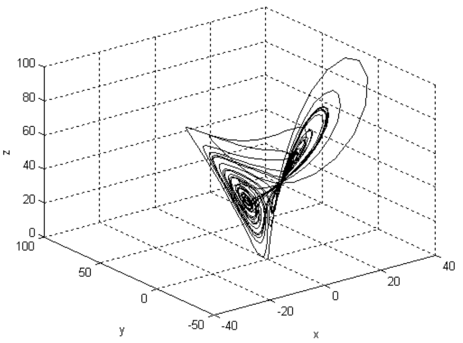

Fig. 5 Lorenz’s chaos plot with initial conditions x(0)=0.1,y(0)=0.1, and z(0)=0.

Remark 2.- The relay terms in the discrete receiver system (7) can produce some numerical problems that may affect the performance of digital processors due to chattering, but this problem can be diluted using some smooth approximation of the *sign* function, like

$$sign\,(x) \approx \frac{x}{|x|+\varepsilon} \qquad (8)$$

with ε a positive constant sufficiently small. This smooth approximation of the “signum” function also helps to avoid the high frequency contents of the relay terms.♦

Remark 3.- Stability analysis in discrete time domain can be done straightforwardly using the discrete time version of the Lypunov function, where the stability requirement is in function of *h*. ♦

Using (8) in (7) with $\varepsilon=0.01$, and $k_1=1/\sigma$, the discrete error dynamics is shown in Fig. 7. In contrast, Fig. 6 shows the discrete dynamic error using (7) without the relay terms. Hereafter we use (8) in (7) with $\varepsilon=0.01$, and $k_1=1/\sigma$.

For the purpose of illustration, we selected the following encryption and decryption functions:

$$\phi(y(k),s(k)) = \frac{1}{2200}(y^2(k)+(1+y^2(k))s(k)) \qquad (9)$$

$$\psi(y_r(k),\phi(k)) = -\frac{y_r^{\,2}(k)}{(1+y_r^2(k))} + 2200\,\frac{\phi(k)}{(1+y_r^2(k))} \qquad (10)$$

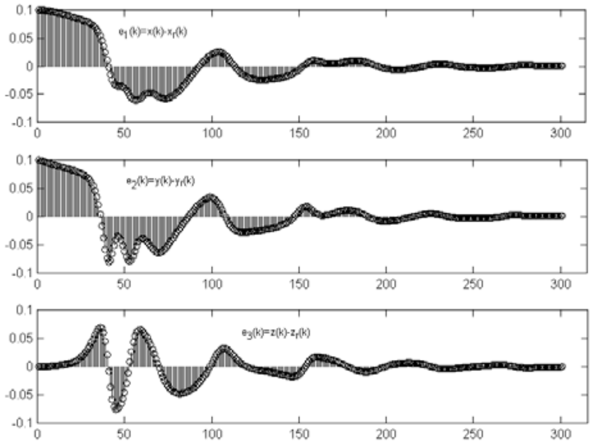

Fig. 6 Discrete error dynamic without the relay terms.

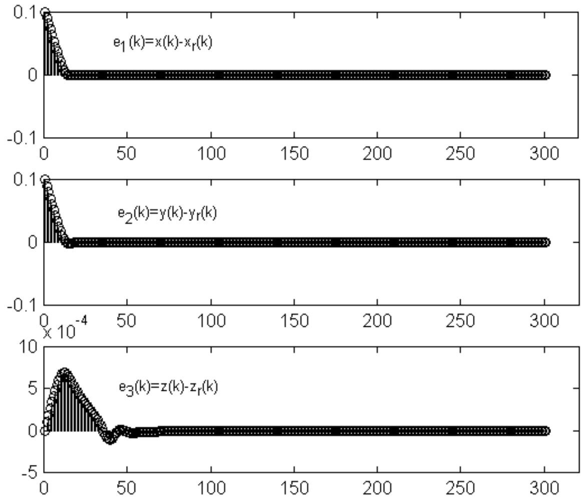

Fig. 7 Discrete error dynamic using the relay terms with the approximation (8).

Where the signal *s(k)* is obtained using the image information in *A* and the algorithm presented in Fig.8, where *M* is the number of columns of *A* and *N* is the number of rows of *A*.

```
k=1
For i=1 to N
    For j=1 to M
        s(k)=A(i,j)
        k=k+1
    Next j
Next i
```

Fig. 8 Algorithm to produce the information signal *s(k)*.

Using the masking system described in Fig.3 in its discrete version (i.e., with equations (6), (7) and (8)), and (9) and (10) with the test image shown in Fig.9, the encrypted image obtained is shown in Fig.10 meanwhile the decrypted image is displayed in Fig.11. The initial conditions used were $x(0)=0.1$, $y(0)=0.1$, $z(0)=0$, and $x_r(0)=y_r(0)=z_r(0)=0$.

Having obtained a decrypted image (Fig. 11), it is of interest to determine if any degradation of $s(k)$ is introduced because of the encryption – decryption process. It is expected that given the characteristics of finite time synchronization, some error will occur in the decrypted image, mainly at the upper left portion of the image, since it is the first part of the signal to be processed. Original (Fig. 9) and decrypted (Fig. 11) images were compared, and the resulting error image (with an intensity gain of 500) was produced (see Fig. 12). Fig. 12 shows that in effect, only some pixels of the first row of the image are somewhat affected. The quality of reconstruction has an $MSE=2.4815x10^{-7}$ and a $PSNR=114.18$ dB. From the result, given the very high resulting PSNR, we can conclude perfect reconstruction is achieved.

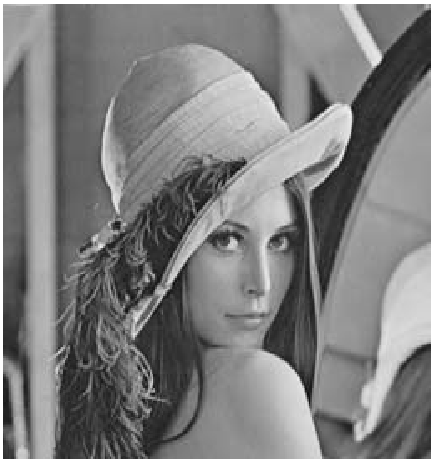

Fig. 9 Test gray-level image.

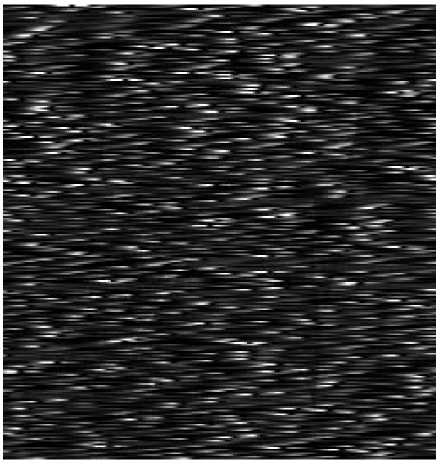

Fig. 10 Encrypted image.

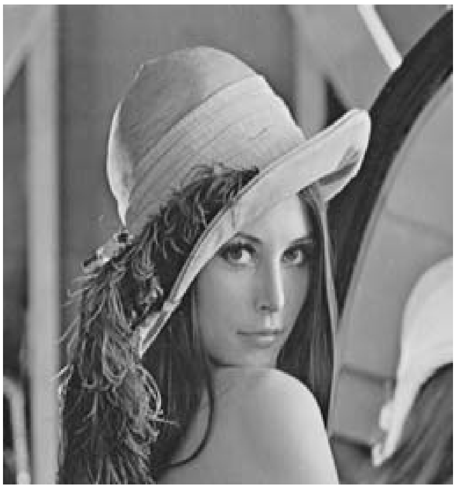

Fig. 11 Decrypted image.

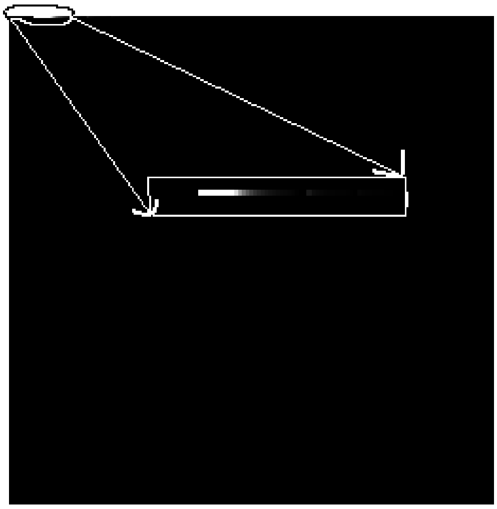

Fig.12 Error image with a gain intensity of 500.

Now, we corrupted the signals in both communication lines of Fig. 3 with an uncorrelated noise of normal distribution with mean zero and variance 0.011719 (the equivalent to a variation of three levels in the gray scale). Fig. 13 shows the decrypted image. In this case, the quality of reconstruction has an *MSE=20.197* and a *PSNR=35.0 dB*.

Fig. 13 shows the poor tolerance to noise of the scheme proposed in Fig. 3. However, in practical telecommunications applications, the perturbation situation shown here is very unlikely to occur, since in modern digital communication systems, channel coding techniques are always introduced between transmitter and receiver to achieve very robust communication channels.

A final numerical experiment was done by adding *salt and pepper* noise with 0.05 noise density to the encrypted image in Fig. 10 (see Fig. 14). The decrypted image obtained is illustrated in Fig. 15.

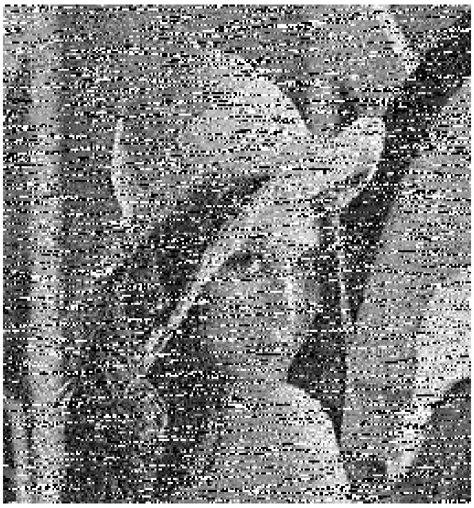

Fig. 13 Decrypted image.

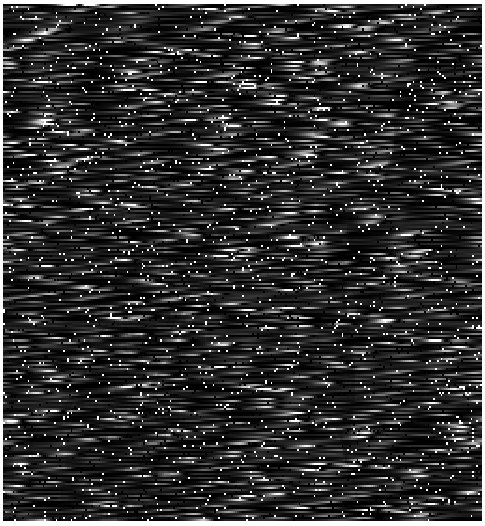

Fig. 14 Encrypted image with *salt and pepper* noise.

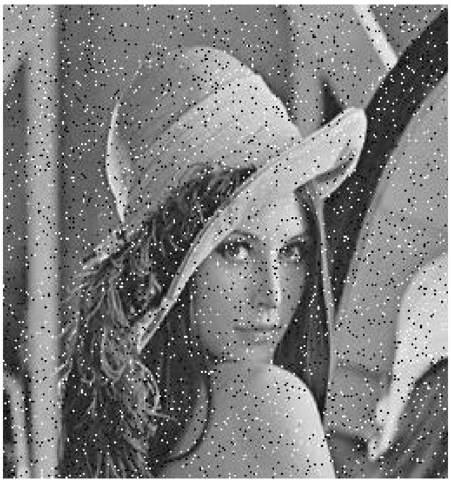

Fig. 15 Decrypted image.

6. Conclusions

In the present paper a masking system design that uses a finite time synchronization algorithm based on chaotic discrete signals, with application to the encryption – decryption of gray-level images is presented. Numerical results show that a very high PSNR is achieved after decrypting the encrypted image, therefore the algorithm can be considered as a perfect reconstruction implementation. Robustness of the proposed algorithm is demonstrated by adding *salt and pepper* noise to the encrypted image and still recovering a good quality decrypted image.

References:

[1] Acho L., Hérnandez C., Aguilar B., Finite Time Synchronization of Lorenz-based Chaotic Systems. *Advances in Systems Theory, Mathematical Methods and Applications*. WSEAS Press, 2002, pp. 155-157.

[2] Bhat S. P. and Bernstein D. S. Finite-Time Stability of Continuous Autonomous Systems, *Siam J. Control Optim.*, Vol.38 No.3, 2000, pp. 751-766.

[3] Chua L. O., Yang T., Zhong G.-Q. and Wu C. W. Adaptive Synchronization of Chua's Oscillators, *Int. Journal of Bifurcation and Chaos*, Vol.6, No.1, 1996, pp. 189-201.

[4] Corron Ned J. and Hahs D. A New Approach to Communications Using Chaotic Signals, *IEEE Trans. on Circuits and Systems-I*, Vol.44, No.5,1997, pp. 373-458.

[5] Cuomo K. M. and Oppenheim A. V. Synchronization of Lorenz-based Chaotic Circuits with Application to Communications, *IEEE Trans. on Circuits and Systems-II*, Vol.40 No.10, 1993, pp. 626-633.

[6] Dedieu H., Kennedy P. M., and Hasler M. Chaos Shift Keying: Modulation and Demodulation of a Chaotic Carrier Using Self-Synchronization Chuas's, *IEEE Trans. on Circuits and Systems-II*, Vol.40 No.10, 1993, pp. 634-642.

[7] Hong Y., Huang J., and Xu Y. On an Output Feedback Finite-Time Stabilization Problem, *IEEE Trans. on Automatic Control*, Vol.46 No.2, 2001, pp. 305-309.

[8] Millerioux M. and Mira C. Finite-Time Global Synchronization for Piecewise Linear Maps, *IEEE Trans. Circuits and Systems I*, Vol. 48, No.1, 2001, pp 111-116.

[9] Paden Brad E. and Sastry Shankar. A Calculus for Computing Filippov's Differential Inclusion with Application to the Variable Structure Control of Robot, *IEEE Trans. on Circuit and Systems,* Vol.Cas-35, No.1, 1987, pp. 73-82.

[10] Zhong-Ping J. A Note on Chaotic Secure Communication Systems, *IEEE Trans. on Circuit and Systems I,* Vol. 49, No.1, 2002, pp. 92-96.