Novel Encryption Method Based on a new 4D Chaotic System for Data Transmission with Electronic Circuit

M. Messadi
L2EI Laboratory
MSB University,
Jijel, Algeria

T. Belguebli, H. Mekhloufi
Electronics departement,
Constantine 1University,
Constantine, Algeria

H. Hamiche
L2CSP Laboratory
MMTOUniversity
Tizi-Ouzzou Algeria

K. Kemih
L2EI Laboratory
MSB University,
Jijel, Algeria

***Abstract*—This paper studies the problem of synchronization of a new 4D chaotic systems using passive control and its application to the design of a new approach for the information encryption. The basic principle of the cryptosystem is simple; At the transmitter, the message is injected into the dynamics of the chaotic system. At the receiver, the message is recovered by a chaotic demodulation after synchronization by the passive control. The electronic circuit is detailed using the Multisim software to demonstrate the feasibility of the proposed approach.**

Keywords—Passive control, chaotic system, secure communication, electronics circuit.

I. INTRODUCTION

Encryption is a commonly used method of protecting information. For example, when giving orders for financial transfers over the internet, we do not necessarily want a third party to intercept the message and modify the recipient of the transfer. More generally, encryption is used for all sensitive activities such as financial transactions, it is the process which makes it possible to make a secret message incomprehensible by people other than the recipient [1]. The idea of using chaos in communication systems was inspired by the discovery of Pecora-Carroll [2] in 1990. They showed that two identical chaotic systems with different initial conditions can possibly synchronize if they are suitably coupled, that is, under certain conditions. The development of communication systems using chaos therefore began with very simple synchronization schemes of electronic circuits, aimed at the simultaneous encryption and reconstruction of an information signal [3-8].

In communication systems, synchronization is a very important key for successful transmission. The role of synchronization is to try to estimate some of the states of the dynamic system or sometimes unknown inputs. This means that two chaotic signals will be said to be synchronized if they are asymptotically identical when time tends to infinity. Sensitivity to initial conditions is a fundamental characteristic of chaotic systems, which makes chaotic synchronization seem difficult to achieve and presents more constraints. In the literature, there are several synchronization methods, synchronization by impulsive control [9], observer-based synchronization [10] and many other approaches [11-15]

In the context of this article, we are interested in the encryption of information by chaos, more precisely, in the synchronization of chaotic systems for application in the encryption of information. The basic principle of the cryptosystem is simple, at the transmitter part, the message is injected into the dynamics of the chaotic system. At the receiver, the message is restored by a chaotic demodulation after synchronization by the passive command. In order to show the feasibility of the proposed approach, a circuit of the crypto system is produced by Multisim software.

The work is organized as follows: In Section 2, some recalls of the passive control are given. A new result for the synchronization of the new 4D system based on the passive control is given in Section 3. Section 4 is devoted to give the application of the proposed synchronization method in order to encrypt the information. In Section 6, we expose the schematics of the proposed cryptosystem under Multisim software. Finally, in Section 7 we give some concluding remarks.

II. PASSIVITY BASED CONTROL

Consider the following nonlinear system

$$\begin{aligned} \dot{x}(t) &= f\big(x(t), u(t)\big) \\ y(t) &= h\big(x(t)\big) \end{aligned} \tag{1}$$

u(t) is the input vector and *y(t)* is the output vector..

Definition1 [16-17]

System (1) is said to be at "phase minimum" if the dynamic zero is asymptotically stable.

Definition2 [16-17]

System (1) is passive if there is a real constantβ such that for $\forall t \geq 0$, The following inequality is checked:

$\int_0^t u^T(\tau)\, y(\tau) \geq \beta$and

$$\int_0^t u^T(\tau)\, y(\tau)\, dt + \beta \geq \int_0^t \rho y^T(\tau)\, y(\tau)\, d\tau \tag{2}$$

The physical meaning of this definition is that the increase in storage energy in a passive non-linear system is due to an external source.

System (1) can be represented in the ordinary form [25]

$$\begin{aligned} :\dot{x} &= f(z) + g(z,y)y \\ \dot{y} &= l(z,y) + k(z,y)u \end{aligned} \tag{3}$$

If System (1) is at minimum phase, the nonlinear system (3) may be equivalent to a passive system and asymptotically stabilized at equilibrium points by a closed-loop control of the following form [16-17] :

$$u = k(z,y)^{-1}\left[-l(z,y) - \frac{\partial W(z)}{\partial z} g(z) - \gamma y + \eta\right] \quad (4)$$

Where $W(z)$ is Lyapunov's function of $f_0(z)$, γ is a positive value and η is an external signal connected to the reference input.

III. SYNCHRONIZATION OF THE CHAOTIC 4D SYSTEM BY THE PASSIVE CONTROL

In this section we will apply the passive command for synchronizing the 4D chaotic system.

The master system is described by [19]:

$$\begin{aligned} \dot{x}_1 &= ax_1 - x_2x_3 + x_4 \\ \dot{x}_2 &= -bx_2 + x_1x_3 \\ \dot{x}_3 &= -cx_3 + x_1^2 \\ \dot{x}_4 &= -dx_1 \end{aligned} \quad (5)$$

And the slave system:

$$\begin{aligned} \dot{y}_1 &= ay_1 - y_2y_3 + y_4 + u_1 \\ \dot{y}_2 &= -by_2 + x_1x_3 \\ \dot{y}_3 &= -cx_3 + x_1{}^2 + u_2 \\ \dot{y}_4 &= -dx_1 + u_3 \end{aligned} \quad (6)$$

we assume that:

$$e = (e_1, e_2, e_3, e_4)^T = (y_1 - x_1, y_2 - x_2, y_3 - x_3, y_4 - x_4)^T \quad (7)$$

We get the equations for the synchronization error, as follows:

$$\begin{aligned} \dot{e}_1 &= ae_1 - (y_2y_3 - x_2x_3) + e_4 + u_1 \\ \dot{e}_2 &= -be_2 + (y_1y_3 - x_1x_3) \\ \dot{e}_3 &= -ce_3 + (y_1^2 - x_1^2) + u_2 \\ \dot{e}_4 &= -de_1 + u3 \end{aligned} \quad (8)$$

After simplification, we get:

$$\begin{aligned} \dot{e}_1 &= ae_1 - e_2e_3 - x_2e_3 - e_2x_3 + e4 + u_1 \\ \dot{e}_2 &= -be_2 + e_1e_3 + e_1x_3 + e_3 \\ \dot{e}_3 &= -c\, e_3 + e_1^2 + 2\, e_1x_1 + u_2 \\ \dot{e}_4 &= -d\, e_1 + u_3 \end{aligned} \quad (9)$$

We start by rewriting the system in the form of a passive system (3), for that, we choose:

$$z_1 = e_2 \;\; y_1 = e_1 \; y_2 = e_3 \; y_3 = e_4$$

Which allows us to get:

$$f(z) = \begin{bmatrix} -bz_1 \end{bmatrix} \quad g(z,y) = [\, y_2, x_3 x_1 \, 0 \,]$$

$$l(z,y) = \begin{vmatrix} ay1 + y3 - z1y2 - z1x3 - x3y2 \\ -cy2 + y_1^2 + 2y1x1 \\ -dy1 \end{vmatrix}$$

$$k(z,y) = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix}$$

we take: $V(z,y) = W(z) + \frac{1}{2}y^2 \quad (10)$

Where *W(z)* is a Lyapunov function, with W(0)=0 :

$$W(z) = \frac{1}{2}z_1^2 \quad (11)$$

The calculation of the derivative of the Lyapunov function as a function of time is as follows:

$$\frac{dW(z)}{dt} = -bz_1^2 \le 0 .$$

The dynamic zero of the synchronization error is stable in the sense of Lyapunov.

The derivative $\frac{dW(z)}{dt}$ along the dynamics of the error system (9) is given as follows :

$$\frac{dV(z,y)}{dt} = \frac{\partial W(z)}{\partial z} \times \dot{z} + y \times \dot{y}$$

$$= \frac{\partial W(z)}{\partial z} f(z) + \frac{\partial W(z)}{\partial z} g(z,y)y + l(z,y)y + k(z,y)uy \quad (13)$$

Since. : $$\frac{dW(z)}{dz} f(z) \le 0 \quad (14)$$

Then equation (13) becomes:

$$\frac{dV(z,y)}{dt} \le \frac{\partial W(z)}{\partial z} g(z,g)y + (l(z,y) + k(z,y)u)y \quad (15)$$

Closed-loop control is selected in the form :

$$u = k^{-1}(z,y)\left[-l^{-1}(z,y) - \frac{\partial W(z)}{\partial z} g(z,y) - \gamma_{12}y + \upsilon\right] \quad (16)$$

If we consider (16), we find :

$$\text{u=} \begin{vmatrix} -(ae_1 + e_4 - e_2e_3 - x_3e_3) - \gamma e_1 - e_2(e_3 + x_3) \\ -(ce_3 + e_1^2 + 2x_1e_1) - \gamma e_3 - e_2\, x_1 \\ -(de_1) \qquad -\gamma e_4 \end{vmatrix}$$

Where γ is a positive constant. When substituting (16) into (15), we get:

$$\frac{\partial V(z,y)}{\partial t} \le -\gamma_{12}y^2 + \upsilon y \quad (17)$$

Integrating (17) gives us:

$$V(z,y) - V(z_0,y_0) \le \int_0^t -\gamma_{12}y^2(\tau)d\tau + \int_0^t \upsilon(\tau)y(\tau)d\tau \quad (18)$$

$$V(z,y) \ge 0 \text{ and } \rho = V(z_0,y_0)$$

$$\int_0^t \upsilon(\tau)y(\tau)d\tau + \rho \ge V(z,y) + \int_0^t \gamma_{12}y^2(\tau)d\tau \ge V(z,y) \quad (19)$$

The relation (19) satisfies the definition of passivity given by the equation (2), so the synchronization error system (9) is strictly passive. The evolution of the state variables of the master and slave systems as well as the error are shown in the Fig. 1. As we can see it is clear that the transmitter synchronizes quickly with the receiver.

IV. APPLICATION OF SYNCHRONIZATION FOR INFORMATION ENCRYPTION

In this part, we will use this synchronization method in the field of cryptography, by developing an encryption method, which is based on the inclusion of an information signal in the transmitting system. In the receiver, we will also use a method for recovering this signal. A simulation of the transmission of a sinusoidal signal will be tackled in order to test the performance of these proposed methods for the encryption and decryption of the information signal.

*1) **Design of the transmitter***

At the sender's level, the message is injected into the dynamics of the chaotic system while maintaining the chaotic behavior. Thus the sender system is governed by the following equations:

$$\begin{aligned}\dot{x}_1 &= ax_1 - x_2x_3 + x_4\\ \dot{x}_2 &= -bx_2 + x_1x_3 + cs(t)\\ \dot{x}_3 &= -cx_3 + x_1^2\\ \dot{x}_4 &= -dx_1\end{aligned} \qquad (20)$$

Starting from (20), we can schematize the transmitter system in Simulink as shown in Fig. 1 .

*2) **Receiver design***

No changes will be made to the receiving system, so it is always governed by the same equations below:

$$\begin{aligned}\dot{y}_1 &= ay_1 - y_2y_3 + y_4 + u_1\\ \dot{y}_2 &= -by_2 + y_1y_3\\ \dot{y}_3 &= -cy_3 + y_1^{\,2} + u2\\ \dot{y}_4 &= -dy_1 + u_3\end{aligned} \qquad (21)$$

To restore the message transmitted by inclusion at the receiver, we will use chaotic demodulation [18].

$$\begin{cases}\dfrac{d^{\alpha}Q}{dt^{\alpha}} = -\varsigma K\left(a(y_s - U_m) + \varsigma\hat{m}(t)\right)\\ \hat{m}(t) = \varsigma K U_m(t) + Q\end{cases} \qquad (22)$$

$\hat{m}(t)$ the reconstructed signal

From Fig.2, we can see that the message is well recovered.

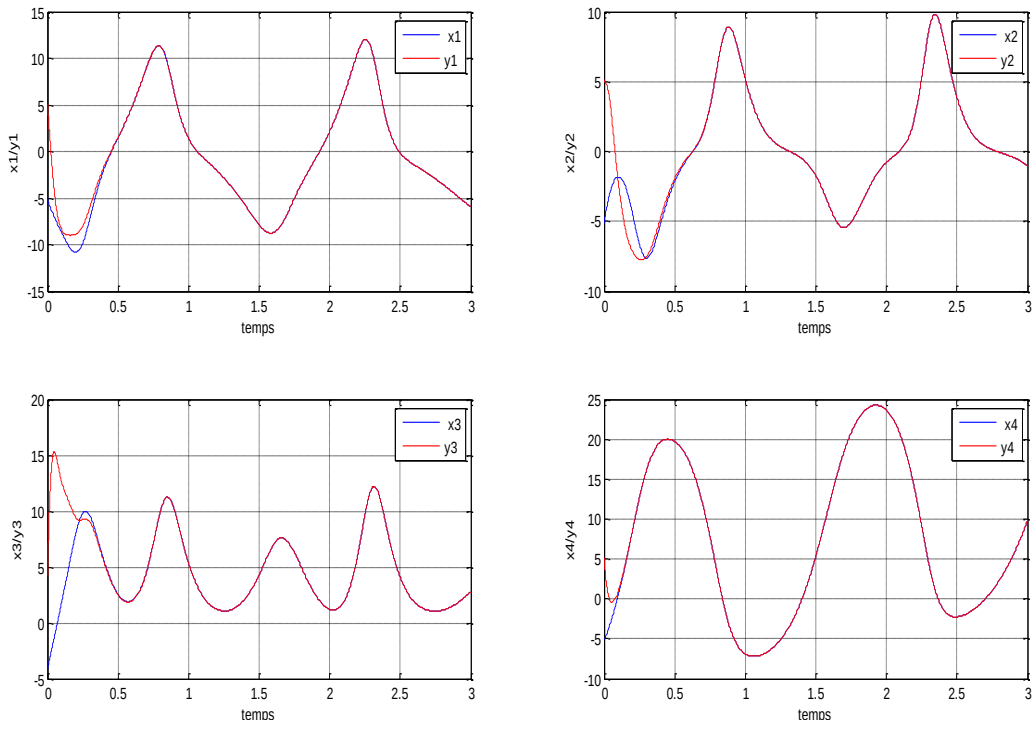

Fig. 1 Synchronization results between transmitter and receiver

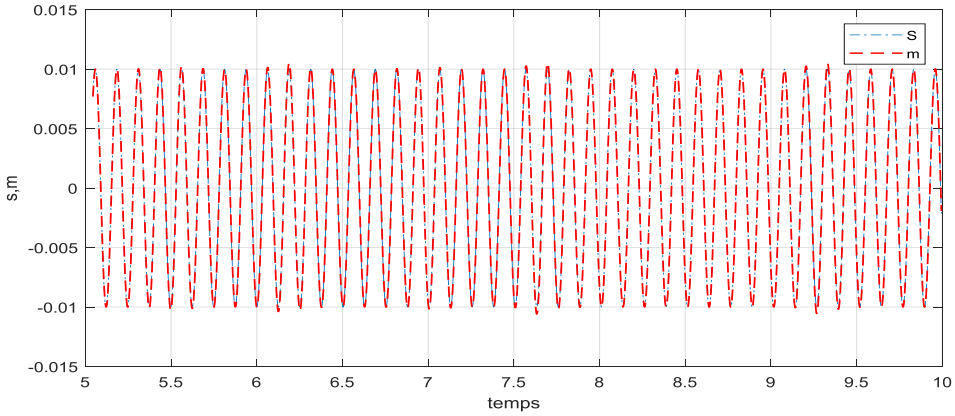

Fig. 2: The transmitted message and the reconstructed message.

V. THE SCHEMATICS OF THE CRYPTO SYSTEM UNDER MULTISIM SOFTWARE

To design the analog secure communication circuit, only common electronic components are used such as resistors, capacitors, diodes, multipliers, and operational amplifiers.

The analog circuit of the complete system is provided in Fig.4, Fig.5, Fig.6 and Fig.7. The oscilloscope traces of the proposed circuit are shown in Fig.8, Fig.9 Fig.10 and Fig.11. Comparing the different results shown in Fig.1 and Fig.2, a good qualitative agreement between the numerical simulations with Matlab and the electrical simulations with Multisim Software is observed.

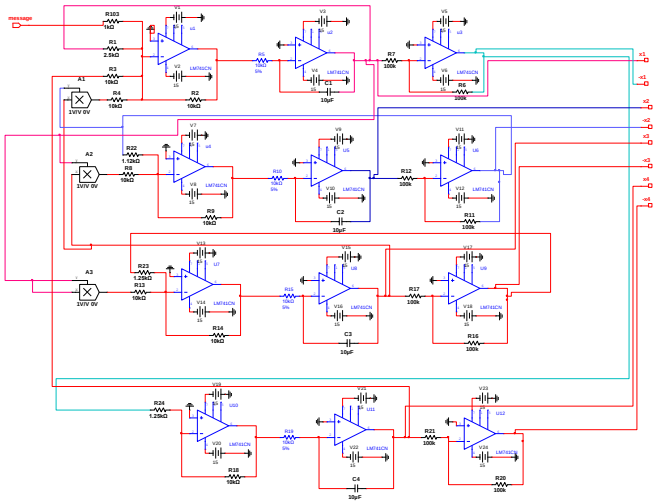

Fig.3 theTransmitter circuit.

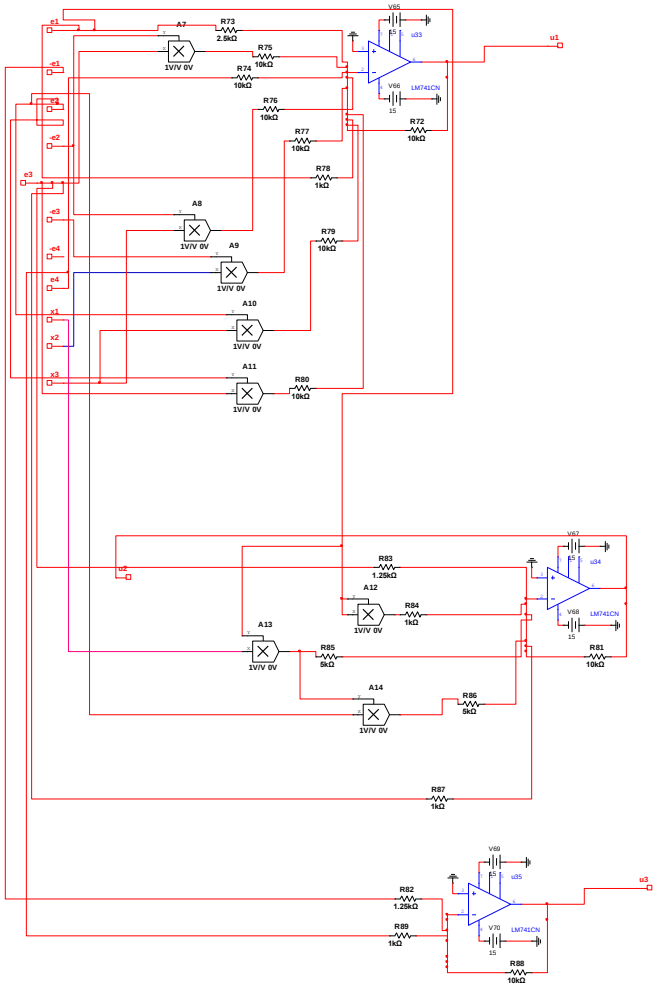

Fig. 4: Passive control circuit.

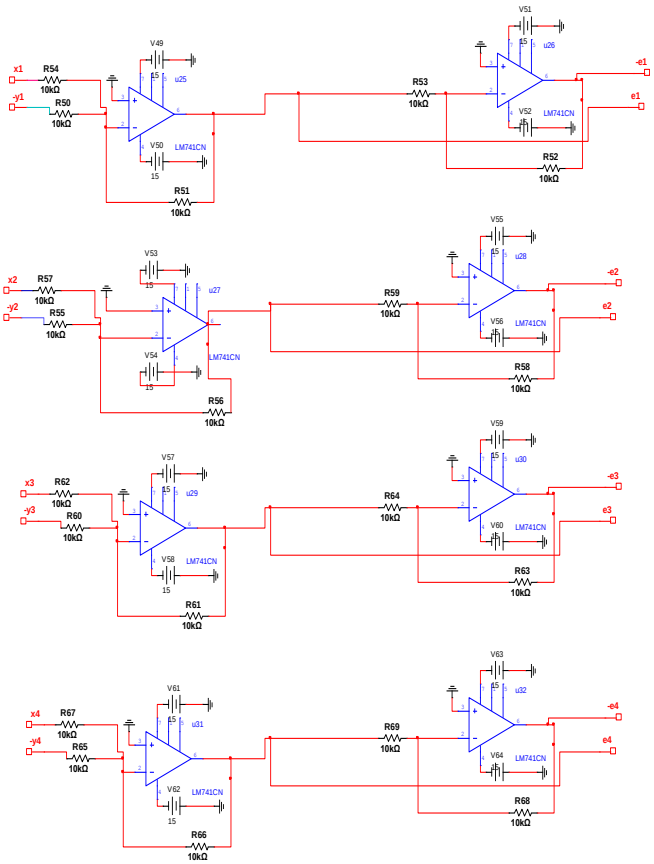

Fig.5: Synchronization error circuit.

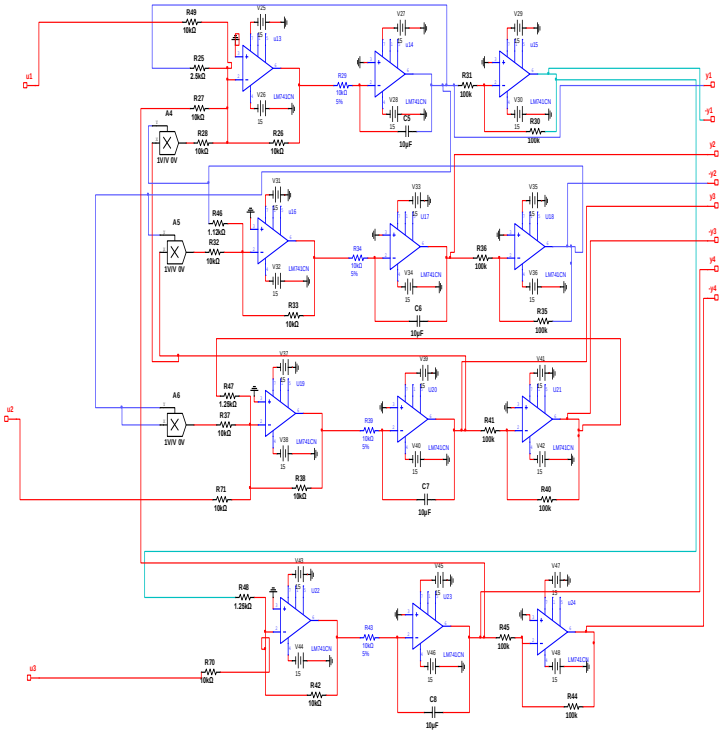

Fig.6: Receiver circuit with control.

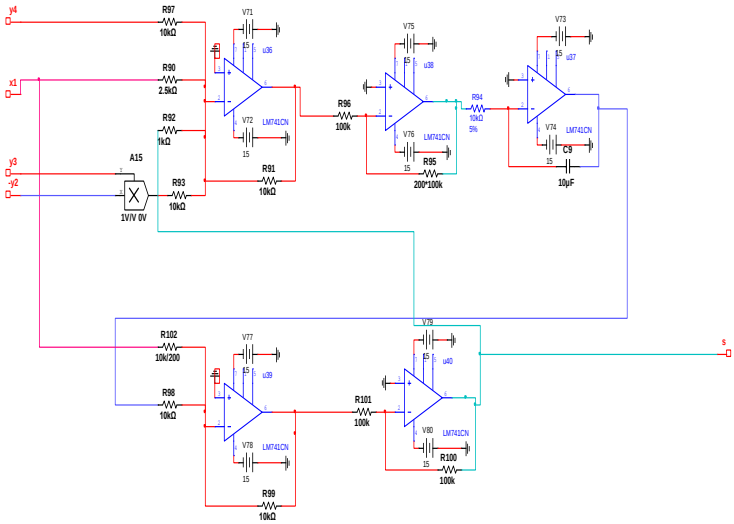

Fig.7: Chaotic demodulation circuit.

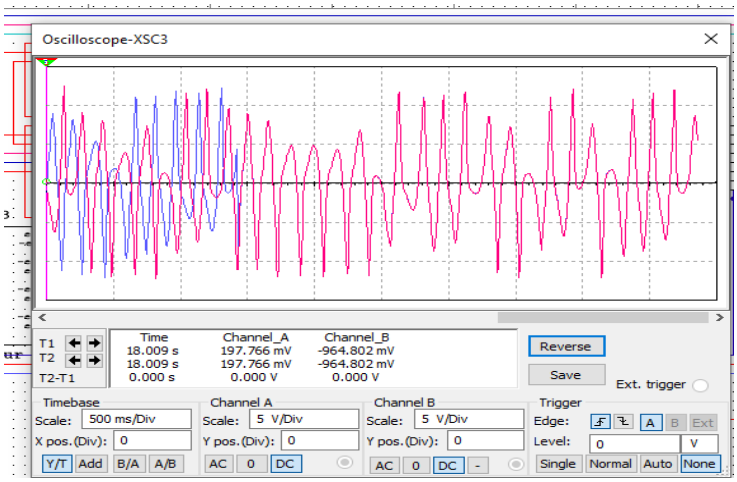

Figure 8: Status synchronization (x_1) and slave (y_1)

Fig.9: Status synchronization (x_2) and (y_2)

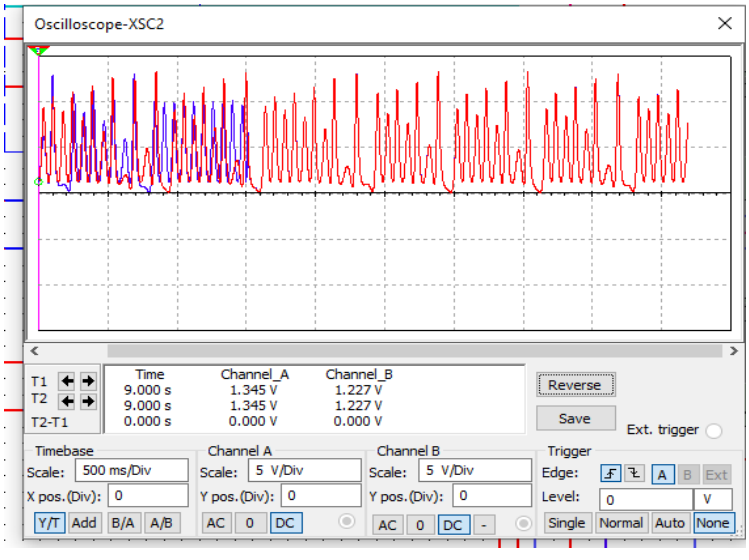

Fig. 10: Status synchronization (x_3) and slave (y_3)

Fig. 11 Superposition of the original signal s(t) and the recovered signal ŝ (t)

VI. Conclusion

In this paper, a new approach for secure communications using passive controller has been presented with a circuit simulation using Multisim. The unknown information is encrypted in the transmitter, by injection method, and using passive control, the synchronization is achieved and the hidden information is reconstructed by chaotic demodulation. To verify the effectiveness of this approach simulation under Simulink and an electronic realization under Multisim have been implemented, the result of the simulation validates our approach.

References

[1] NEMATI, Hamid R. (ed.). *Applied Cryptography for Cyber Security and Defense: Information Encryption and Cyphering: Information Encryption and Cyphering*. IGI Global, 2010.

[2] PECORA, Louis M. et CARROLL, Thomas L. Synchronization in chaotic systems. *Physical review letters*, 1990, vol. 64, no 8, p. 821.

[3] HAMICHE, Hamid, MEGHERBI Ouerdia, KARA Redouane, SADDAOUI Rafik, LAGHROUCHE Mourad, DJENNOUNE, Saïd, A new implementation of an impulsive synchronization of two discrete-time hyperchaotic systems using ArduinoUno boards. *International Journal of Modelling, Identification and Control*, 2017, vol. 28, no 2, p. 177-186.

[4] HAMICHE, Hamid, KASSIM Sarah DJENNOUNE, Saïd., GUERMAH Saïd, BETTAYEB Maamar, Secure data transmission scheme based on fractional-order discrete chaotic system, International Conference on Control, Engineering and Information Technology, 2015, Tlemcen, Algeria.

[5] ZOUAD, Fadia, KEMIH, Karim, et HAMICHE, Hamid. A new secure communication scheme using fractional order delayed chaotic system: design and electronics circuit simulation. *Analog Integrated Circuits and Signal Processing*, 2019, vol. 99, no 3, p. 619-632.

[6] BOURAOUI, H. et KEMIH, K. Observer-based synchronization of a new hybrid chaotic system and its application to secure communications. *Acta Phys. Polonica A*, 2013, vol. 123, p. 259-262.

[7] KEMIH, K., HALIMI, M., GHANES, M., *et al.* An Application of Chaotic Chua's System for Secure Chaotic Communication Based on Sliding Mode observer. In : *AIP Conference Proceedings*. American Institute of Physics, 2011. p. 344-349.

[8] MEGHERBI Ouerdia, GUERMAH Saïd, HAMICHE, DJENOUNE Saïd, A Novel transmission scheme based on impulsive synchronization of two Colpitts chaotic systems, *3rd International Conference on Systems and Control*, ICSC'13, 2013, Algiers, Algeria.

[9] LU, Jun Guo et HILL, David J. Impulsive synchronization of chaotic Lur'e systems by linear static measurement feedback: An LMI approach. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2007, vol. 54, no 8, p. 710-714.

|10] ZHENG, Gang et BOUTAT, Driss. Synchronisation of chaotic systems via reduced observers. *IET Control Theory & Applications*, 2011, vol. 5, no 2, p. 308-314.

[11] WANG, Faqiang et LIU, Chongxin. Synchronization of unified chaotic system based on passive control. *Physica D: Nonlinear Phenomena*, 2007, vol. 225, no 1, p. 55-60.

[12] LI, Chunlai et ZHANG, Jing. Synchronisation of a fractional-order chaotic system using finite-time input-to-state stability. *International Journal of Systems Science*, 2016, vol. 47, no 10, p. 2440-2448.

[13] VAIDYANATHAN, S., VOLOS, Ch K., RAJAGOPAL, K., *et al.* Adaptive Backstepping Controller Design for the Anti-Synchronization of Identical WINDMI Chaotic Systems with Unknown Parameters and its SPICE Implementation. *Journal of Engineering Science & Technology Review*, 2015, vol. 8, no 2.

[14] VAIDYANATHAN, Sundarapandian, VOLOS, Christos, PHAM, V.-T., *et al.* Adaptive backstepping control, synchronization and circuit simulation of a 3-D novel jerk chaotic system with two hyperbolic sinusoidal nonlinearities. *Archives of Control Sciences*, 2014, vol. 24, no 3.

[15] PHAM, V.-T., VOLOS, Ch K., VAIDYANATHAN, S., *et al.* A Memristor-Based Hyperchaotic System with Hidden Attractors: Dynamics, Synchronization and Circuital Emulating. *Journal of Engineering Science & Technology Review*, 2015, vol. 8, no 2.

[16] Luo XS. Passivity-based adaptive control of chaotic oscillations in power system. *Chaos, Solitons & Fractals*. 2007, , vol 31, no 3, pp. 665-71.

[17] Ahn CK. A passivity approach to synchronization for time-delayed chaotic systems. *Modern Physics Letters B*. 2009, vol. 23, no 29, pp. 3531-41.

[18] Wang, Xiao Fan, and Zhi Quan Wang. "A robust demodulation approach to communications using chaotic signals." *International Journal of Bifurcation and Chaos, 2003, vol* 13, no. 01 . pp. 227-231.