Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080404

Circuit Simulation of an Analog Secure Communication based on Synchronized Chaotic Chua's System

M. Halimi[1], *K. Kemih*[2,*] *and M. Ghanes*[3]

[1] CRAN/ESSTIN, 2 Rue Jean Lamour 54519 Vanduvre Ls Nancy Cedex, France
[2] L2EI Laboratory, Jijel university, Algeria
[3] ECS/ENSEA, 6 Avenue du Ponceau, 95014 Cergy-Pontoise, France

Received: 5 Jul. 2013, Revised: 7 Oct. 2013, Accepted: 8 Oct. 2013
Published online: 1 Jul. 2014

Abstract: This paper presents an effective technique for both synchronization and secure communication. In particular, an adaptive sliding mode observer is developed and practically implemented. Only one component of the state vector of the transmitter, that satisfies the observability matching condition, is sent to the receiver via a public channel, which is a sliding mode observer. This observer is able to estimate the state vector of the transmitter and then, reconstruct the unknown information hidden in the transmitted with inclusion encryption. Finally, the chaotic secure communication system is simulated with matlab and then practically implemented by electrical circuits with Multisim software and Ultiboard software.

Keywords: Synchronization, chaotic systems, Chaotic Chua's system, sliding mode observers, chaos based secure communications.

1 Introduction

Due to the considerable progress in communication technologies over the past decades, the security of information exchange has become a "major concern." In this context, cryptography plays a crucial role because the information is mainly transported by public networks. The main objective of cryptography is precisely to hide the information transmitted through insecure channels, in other words, to guarantee the protection and confidentiality of communications. Despite the diversity of cryptographic techniques, two classes are usually distinguished: the public key cryptography and symmetric key encryption [1].

Chaos is one of the most complex dynamics may exhibit non-linear systems. The signals generated by chaotic systems have statistical properties similar to randomness in spite of being deterministic. This may well be one way to implement the principles of confusion and diffusion required by Shannon for cryptographic systems [2]. As a result, chaotic systems have been used for secure communication and different encryption systems based on chaos have been proposed in order to hide the information signal: additive masking [3], chaos shift keying [4], two channels transmission [5], parametric modulation[6]and inclusion encryption[7][8].

Most of the communication schemes consist of two parts: a generator of chaotic signals, which is called the transmitter, and a response system, which is called receiver. In symmetric encryption, the decryption of the unknown information requires the synchronization of the transmitter and the receiver. To achieve synchronization, the output of transmitter is sent to receiver. For the chaotic encryption, which is similar to the principle of symmetric encryption [9], synchronization, commonly known as synchronization of chaos since the work of Pecora and Carroll during the early 90 [10] [11], is ensured by observers[12] [13,14,15,16]. Others approaches have been proposed in the open literature to synchronize two chaotic systems [17,18,19,20,21,22], using passive control [23,24,25], or impulsive control [26].

The work presented in this paper propose a new secure communication, where the information to be sent is encrypted in the chaotic Chua's circuit, which is the transmitter. Then, only one component of the state vector of the transmitter is sent to the receiver, to achieve the synchronization, and therefore, reconstruct the unknown information. The synchronization is ensured using a sliding mode observer, which is a variable structure

* Corresponding author e-mail: k.kemih@gmail.com

observer able to take into account some structural singularity and also is robust in the parameter variations. If an observability matching condition is verified, the observer is able to estimate the state vector of the transmitter and then, reconstruct the unknown information. The effectiveness of the proposed secure communication is illustrated through matlab simulation. The main difference with the existing works is the implementation using Multisim software and Ultiboard software of the proposed secure communication.

The layout of this paper as well as the main contributions is now described. In Section 2, the design of the transmitter circuit is presented. Then, the receiver circuit design is detailed in Section 3 where the reconstruction of the unknown information is illustrated. Finally, some concluding remarks are given in Section 4.

2 Design of the Transmitter circuit

Chua's circuit is the simplest oscillator exhibiting a variety of bifurcations and chaos, it was introduced in 1983 by Leon O. Chua [7].. This circuit contains a linear resistor (R, R_0), a single nonlinear resistor (f ($v1$)), and three linear energy-storage components: an inductor (L) and two capacitors (C_1, C_2).
The state equations for this circuit are given as follow [7]:

$$\begin{cases} \dot{v_1} = \frac{1}{C_1 R}(v_2 - v_1) - \frac{1}{C_1} f(v_1) \\ \dot{v_2} = \frac{1}{C_2 R}(v_1 - v_2) + \frac{1}{C_2} i_3 \\ \dot{i_3} = -\frac{1}{L} v_2 - \frac{R_0}{L} i_3 \end{cases} \quad (1)$$

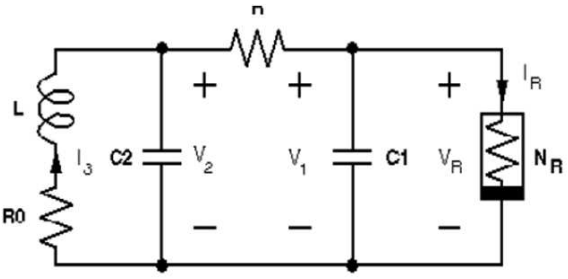
With:
$f(v_1) = G_b v_1 + \frac{1}{2}(G_a - G_b)(|v_1 + E| - |v_1 - E|)$, $\alpha = \frac{C_2}{C_1}$, $\beta = \frac{C_2}{L} R^2$, $m_1 = \frac{G_b}{R}$, $m_0 = \frac{G_a}{R}$, $\gamma = \frac{R\, R_0\, C_2}{L}$.
We proceed to the change of variable: $v_1 = x$, $v_2 = y$, $v_3 = z$.
Consequently, (1) turns into:

$$\begin{cases} \dot{x} = \alpha(y - x - H(x)) \\ \dot{y} = x - - y + z \\ \dot{z} = -\beta y - \gamma z \end{cases} \quad (2)$$

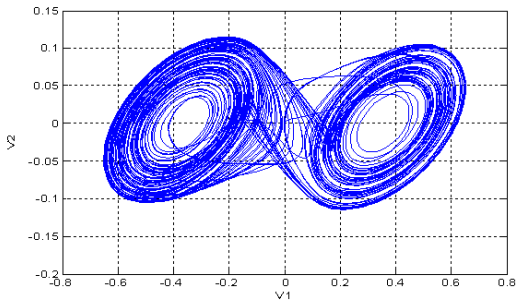
where: $H(x) = bx + \frac{1}{2}(a - b)(|x + 1| - |x - 1|)$; $\beta = 18.605$, $b = -0.732101$ $\gamma = 6.7781166 * 10^{-6}$, $a = -1.37067$

In Figure 1, the circuit diagram of the chaotic Chua's circuit and its chaotic attractor are shown.
Before proceeding to the design of the receiver, the transmitter must verify the following Assumption.
Assumption 1. The chaotic system

$$\dot{x}(t) = f(x(t), u(t))$$
$$y = h(x(t))$$



(a) Chua's circuit



(b) Chaotic phase trajectory

Fig. 1 Chaotic Chua's circuit

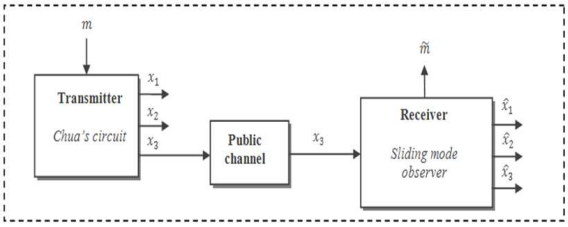


Fig. 2 Block diagram of a communication system

is locally weakly observable if it satisfies the observability rank condition:

$$rank \begin{bmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \end{bmatrix} = n$$

where dh denote the gradient of h ($dh = \nabla^t h$), $L_f h(x) = \sum_{i=1}^{n} f_i(x) \frac{\partial h}{\partial x_i}(x)$ *and* $L_f^0 h = h$ and $L_f^k h = L_f\left(L_f^{k-1} h\right)$, $\forall\, k \geq 1$.

Using assumption 1, the observability matrix in the neighborhood of the equilibrium point given by:

$$\begin{cases} OBS = \begin{bmatrix} dh \\ dL_f h \\ dL_f^2 h \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -\beta & -\gamma \\ -\beta & \beta+\gamma & \gamma^2-\beta \end{bmatrix} \\ With: h = x_3 \end{cases} \quad (3)$$

Rank (*OBS*) =3, which means that the system (2) is locally weakly observable.

The block diagram of the proposed secure communication system is shown in the figure 2.

The message *m*(*t*) is hidden in the transmitter using the encryption method by inclusion, thus, *m*(*t*) is added to the state x_1. Then, the state x_3 of the transmitter is selected as the output, transmitting information from the transmitter to the receiver in order to achieve the synchronization.

After inclusion, the system (2) becomes:

$$\begin{cases} \dot{x}_1 = \alpha\left(x_2 - x_1 - f(x_1)\right) + m \\ \dot{x}_2 = x_1 - - x_2 + x_3 \\ \dot{x}_3 = -\beta x_2 - \gamma x_3 \\ y = x_3 = h\left(x\right) \end{cases} \quad (4)$$

The system (4) is observable if the definition 3.7 in [4] is satisfied. To this end, system (4) can be written as:

$$\begin{cases} \begin{cases} \dot{x} = f\left(x\right) + p(x)m \\ y = Cx \end{cases} \\ with: p\left(x\right) = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \end{cases} \quad (5)$$

The computation of $OBS.p(x)$ gives:

$$OBS.p\left(x\right) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & -\beta & -\gamma \\ -\beta & \beta+\gamma & \gamma^2-\beta \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ -\beta \end{bmatrix}$$

Since $\beta \neq 0$, the observability matching condition given in [4] is verified.

Our objective is to synchronize receiver with transmitter and therefore, estimate the unknown information $\hat{m}$. To this end, the following lemma must be verified.

Lemma 1[4]:

It is possible to design a step-by-step observer (receiver) for system (4) if the flowing conditions are verified:

1. The state and unknown perturbation are bounded,
2. $rang\left(dh, dL_f h, \ldots, dL_f^{n-1}h\right)^T = n$
3. $\left((dh)^T, (dL_f h)^T, \ldots, \left(dL_f^{n-1}h\right)^T\right)^T p\left(x\right) = (0 \ldots 0\ \theta)^T$ *with* $\theta \neq 0$

The Simulink model of the transmitter is shown in Figure 3.

An analog implementation of the transmitter using Multisim is shown in Figure 4, where an operational amplifier LMC6482 and passive components are used. The transmitted signal *m*(*t*) is a sinusoidal signal with the frequency f = 50Hz.

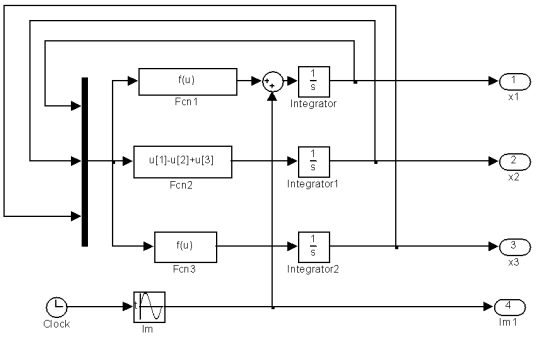


Fig. 3 Simulink model of the transmitter

3 Design of the receiver circuit

Let us design a slave system with sliding mode observer as follows:

$$\begin{cases} \dot{\hat{x}}_1 = \alpha\left(\tilde{x}_2 - \tilde{x}_1 - f(\tilde{x}_1)\right) + E_1\lambda_1 sgn\left(\tilde{x}_1 - \hat{x}_1\right) \\ \dot{\hat{x}}_2 = \hat{x}_1 - - \tilde{x}_2 + x_3 + E_2\lambda_2 sgn(\tilde{x}_2 - \hat{x}_2) \\ \dot{\hat{x}}_3 = -\beta\hat{x}_2 - \gamma x_3 + \lambda_3 sgn(x_3 - \hat{x}_3) \end{cases} \quad (6)$$

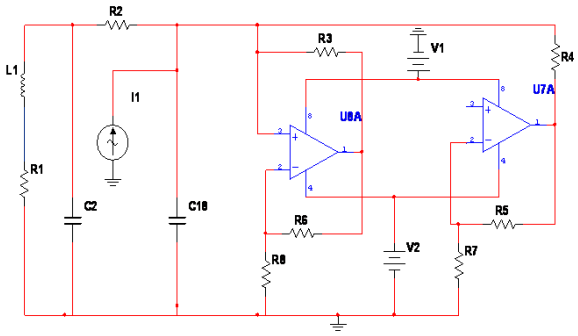
Where: $(\hat{x}_1, \hat{x}_2, \hat{x}_3)$are the estimated states, $\tilde{x}_i = \hat{x}_i - (\lambda_{i+1} sgn\left(\tilde{x}_{i+1} - \hat{x}_{i+1}\right)\ )_{eq}$is the auxiliary system, λ_i is an observer gain which is adapted by an adaptive law and the estimated message is $\hat{m} = ((E_3\lambda_1/\alpha) sgn(\tilde{x}_1 - \hat{x}_1)\ )_{eq}$. If$x_i \neq \hat{x}_i$, the term$E_i = 0$, otherwise$E_i = 1$. The subscript *eq* means equivalent control that can be obtained by passing the term $\lambda_{i+1} sgn\left(x_{i+1} - \hat{x}_{i+1}\right)$ through a low pass filter. Although ideal sliding mode cannot exist due to imperfections and a high frequency oscillation called chattering phenomenon, the high frequency switching term is eliminated by the low pass filter and filter output yields the equivalent control.

The Simulink model of the receiver is presented in Figure 5.

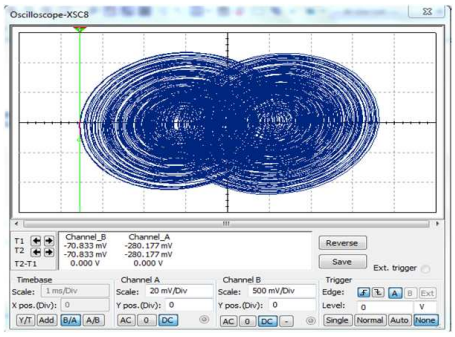
For experimental realization of the sliding-mode observer, we have considered only the corrector terms. The equations of such observer are given by:

$$\begin{cases} \dot{\hat{x}}_1 = \lambda_1\ sign\left(\tilde{x}_1 - \hat{x}_1\right) \\ \dot{\hat{x}}_2 = \lambda_2\ sign\left(\tilde{x}_2 - \hat{x}_2\right) \\ \dot{\hat{x}}_3 = \lambda_3\ sign(x_3 - \hat{x}_3) \\ With: \\ \tilde{x}_2 = x_3 + \lambda_3 \frac{L}{R_0}\ sign\left(x_3 - \hat{x}_3\right) \\ \tilde{x}_1 = \tilde{x}_2 + \frac{R}{R_0} x_3 + \lambda_2\ C_2 R\ sign\left(\tilde{x}_2 - \hat{x}_2\right) \\ \tilde{m} = \frac{1}{R}\left(\tilde{x}_1 - \tilde{x}_2\right) + f\left(\tilde{x}_1\right) + \lambda_1\ C_1\ sign(\tilde{x}_1 - \hat{x}_1) \end{cases} \quad (7)$$

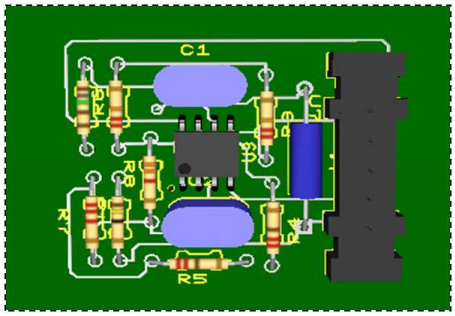
Step 1. Construction of $\hat{x}_3$*:* The signal $\hat{x}_3$ is defined by the expression given in (7). The constructing block diagram is given in Figure 6.



(a) Transmitter circuit



(b) simulation of transmitter circuit with Multisim



(c) Transmitter circuit with Ultiboard

Fig. 4 Transmitter circuit realization

Step 2. Construction of $\hat{x}_2$: for that, we calculate the estimation error e_3 in order to calculate the auxiliary state $\tilde{x}_2$.

$$\begin{cases} e_3 = x_3 - \hat{x}_3 = 0 \implies \\ \dot{e}_3 = \dot{x}_3 - \dot{\hat{x}}_3 = 0 \implies \\ \tilde{x}_2 = x_3 + \lambda_3 \frac{L}{R_0} sign\,(x_3 - \hat{x}_3) \end{cases} \quad (8)$$

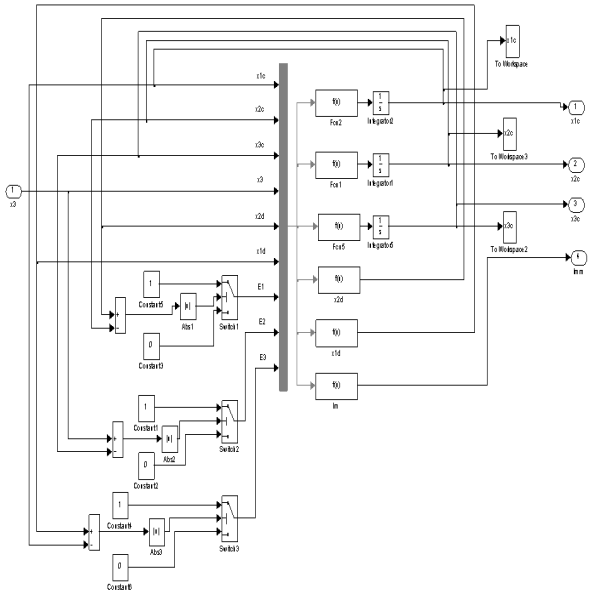


Fig. 5 Simulink model of the Receiver

This equation can be expressed by the block diagram shown in Figure 7.

Then $\hat{x}_2$ is calculated and constructed in the same way than $\hat{x}_3$.

Step 3. Construction of $\hat{x}_1$: $\tilde{x}_1$ is built using the same procedure given previously to construct $\tilde{x}_2$.

$$\begin{cases} e_2 = x_2 - \hat{x}_2 = 0 \implies \\ \dot{e}_3 = \dot{x}_2 - \dot{\hat{x}}_2 = 0 \implies \\ \tilde{x}_1 = \tilde{x}_2 + \frac{R}{R_0} x_3 + C_2 R\, \lambda_2\, sign\,(\tilde{x}_2 - \hat{x}_2) \end{cases} \quad (9)$$

The corresponding block diagram is shown in Figure.8. Then $\hat{x}_1$ is calculated and constructed in the same way than $\hat{x}_3$ and $\hat{x}_2$.

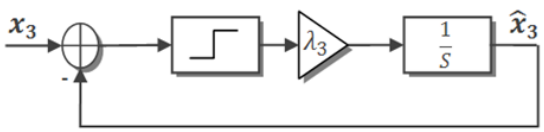


Fig. 6 The block diagram for constructing $\hat{x}_3$

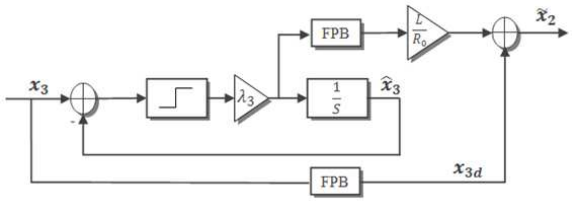


Fig. 7 The block diagram for constructing $\tilde{x}_2$

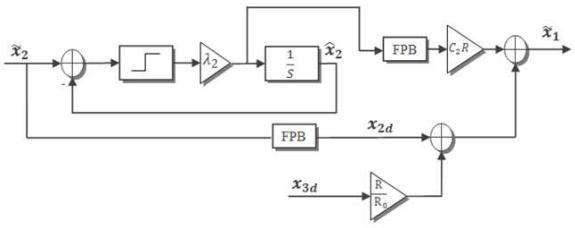


Fig. 8 The block diagram for constructing $\tilde{x}_1$

Step 4. Construction of $\hat{m}$: the message m(t) can be reconstructed when $\tilde{x}_1 = \hat{x}_1$, then :

$$\begin{cases} e_1 = x_1 - \hat{x}_1 = 0 \implies \\ \dot{e}_1 = \dot{x}_1 - \dot{\hat{x}}_1 = 0 \implies \\ \tilde{I}_m = \frac{1}{R}(\tilde{x}_1 - \tilde{x}_2) + f(\tilde{x}_1) + \lambda_1 C_1 \, sign(\tilde{x}_1 - \hat{x}_1) \end{cases} \quad (10)$$

The corresponding block diagram is shown in Figure 9.

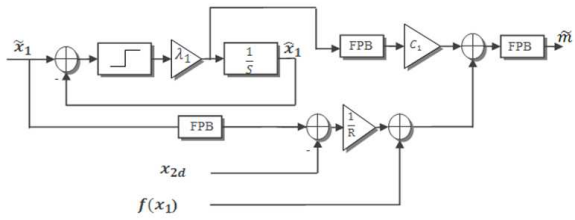


Fig. 9 The block diagram for constructing $\tilde{m}$

The reconstruction error is illustrated in Figure 10 with the corresponding gain values $\lambda_1 = 220$, $\lambda_2 = 130$, $\lambda_3 = 300$. From Figure 10, it's clear that the synchronization of the transmitter and the receiver is achieved since $e_1 = 0$, $e_2 = 0$ and $e_3 = 0$. Consequently, the unknown information is also well reconstructed as illustrated in Figure 11.

Equations (8) (9) (10) can be expressed by the diagram in Figure 12 and Figure 13 show the electronics

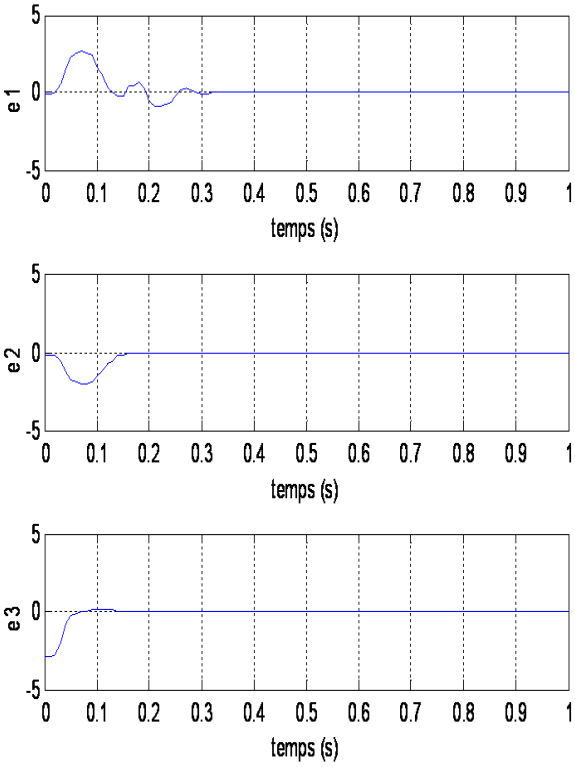


Fig. 10 The synchronization error using the sliding-mode observer

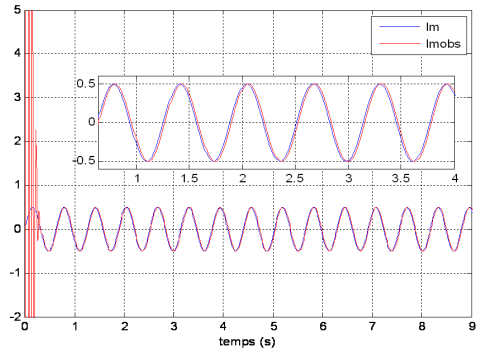


Fig. 11 Original and reconstructed transmitter message using sliding mode observer

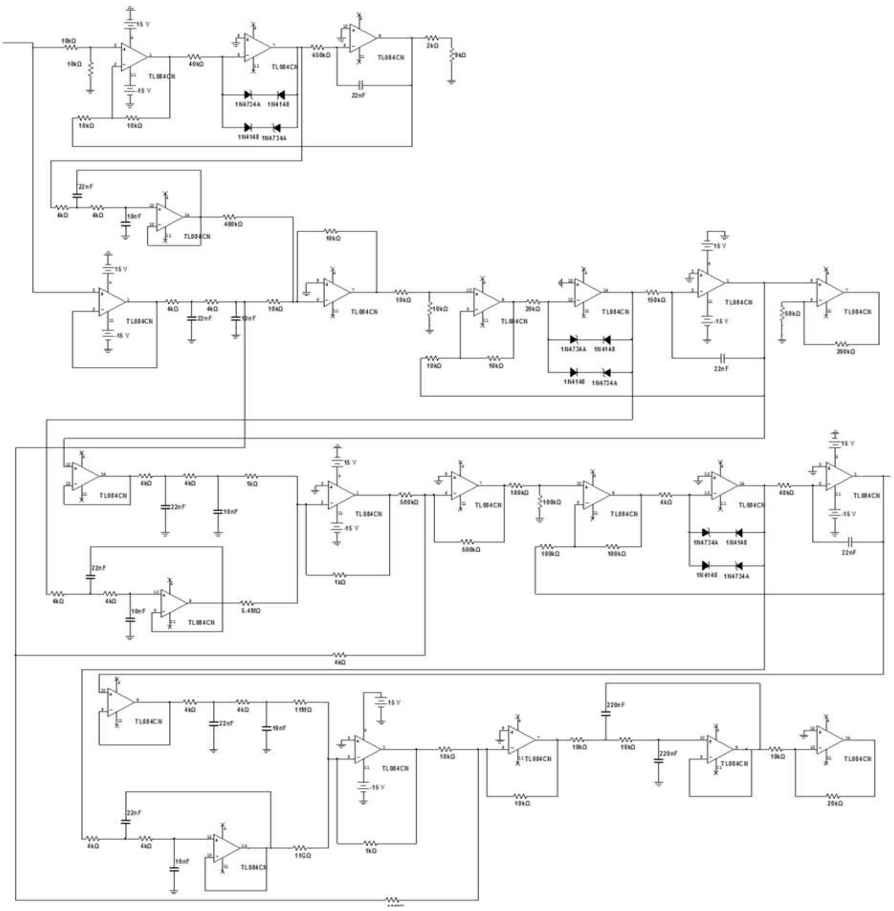


Fig. 12 Electronic circuit of the receiver with Multisim software

circuit of the receiver. From Figure 14 we see that there exists a phase shift between the transmitted and reconstructed message which is once again because of the low-pass filter's transfer function. However, we obtain the necessary information about the message.

4 Conclusion

In this paper, we investigate the synchronization problem based on observers in chaotic communication approach. The unknown information is encrypted in the transmitter, by injection method, and by a sliding mode observer, the synchronization is achieved and the hidden information is reconstructed. A numerical simulation is provided to show the effectiveness of the proposed method. Finally, an implementation of the secure communication circuit, using Multisim software, has also been proposed to shown the feasibility of this method for applications at low frequencies.

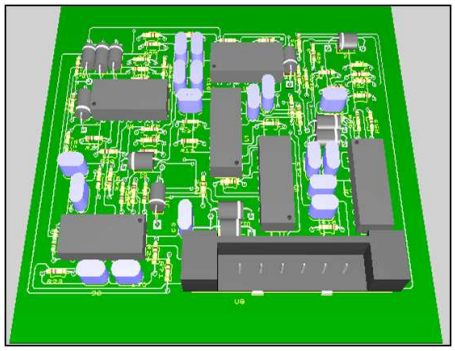
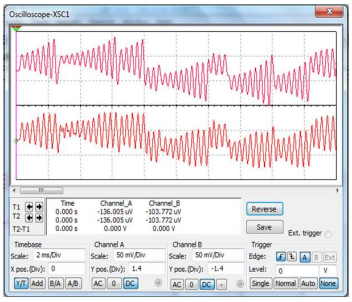


Fig. 13 Electronic circuit of the receiver with Ultiboard software

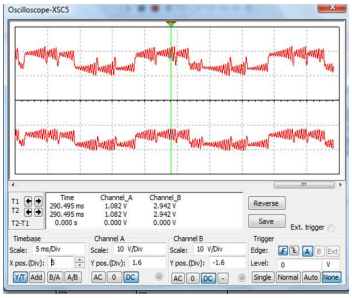
Acknowledgment

The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper.

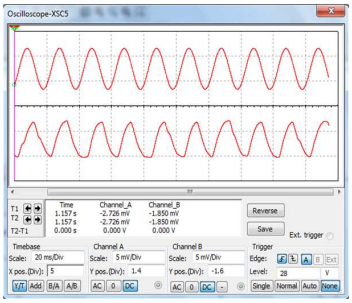
(a) x_1 and $\hat{x}_1$



(b) x_2 and $\hat{x}_2$



(c) x_3 and $\hat{x}_3$

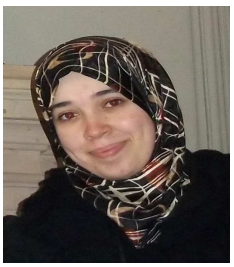


(d) m and $\hat{m}$

Fig. 14 Simulation results with Multisim software

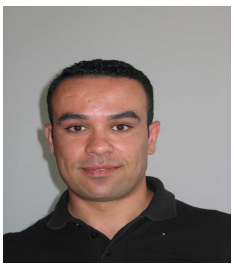
References

[1] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography. CRC Press, (1996).
[2] C. E. Shannon, Bell Systems and Technology Journal, **28**, 657-715 (1949).
[3] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, IEEE Transactions on Circuits and Systems II, **40**, 626-633 (1993).
[4] M. L'Hernault, J. P. Barbot and A. Ouslimani, IEEE Trans. Circuits Syst. I, **55**, 614-624 (2008).
[5] Z. P Jiang,IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications, **49**, 92-96 (2002).
[6] K. Kemih, M. Halimi and M. Ghanes, AIP Conf. Proc, **1400**, 344-347 (2011).
[7] L. O. Chua, Arch. Electron. bertagungstechn, **46**, 250-257 (1992).
[8] K. Y. Lian, and P. Liu, IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, **47**, 1418-1424 (2000).
[9] G. Millrioux, J. M. Amig and J. Daafouz, IEEE Transactions on Circuits and Systems I : Regular Papers, **55**, 1695-1703 (2008).
[10] L. Pecora and T. Caroll, Physical Review Letters, **64**, 821-824 (1990).
[11] T. L. Carroll and L. M. Pecora, IEEE Transactions on Circuits and Systems, **38**, 453-456 (1991).
[12] K. Kemih, Chaos, Solitons and Fractals, **41**, 1897-1901 (2009).
[13] G. Grassi and S. Mascolo, IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications, **44**, 1011-1014 (1997).
[14] M. Itoh, C. W. Wu and L. O. Chua, ,International Journal of Bifurcation and Chaos, **7**, 275-286 (1997).
[15] G. Millrioux, International Journal of Bifurcation and Chaos, **7**, 1635-1649 (1997).
[16] H. Nijmeijer and I. M. Y. Mareels, IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications, **44**, 882-890 (1997).
[17] Jin Ying-Hua and Xu Zhen-Yuan, Chinese Phys. B, **20**, 120505 (2011).
[18] Wang Xing-Yuan et al,Chinese Phys. B, **20**, 020507 (2011).
[19] Zhang Qing-Ling and L Ling, Chinese Phys. B, **20**, 010510 (2011).
[20] Emad E. Mahmoud. Journal of the Franklin Institute, **349**, 1247-1266 (2012).
[21] Chai Yuan et al, Chinese Phys. B, **21**, 030506 (2012).
[22] G.Zheng, D. Boutat, T. Floquet and J.P. Barbot, Int. J. of Bifur. Chaos, **18**, 2063-2072 (2008).
[23] K. Kemih, A. Kemiha and M. Ghanes, Chaos, Solitons Fractals, **42**, 735-744 (2009).
[24] Emad E. Mahmoud, Ayman A Arafa and Gamal M. Mahmoud. Physica Scripta, **87**, 055002 (2013).
[25] Emad E. Mahmoud, Applied Mathematics Information Sciences, **7**, 1429-1436 (2013).
[26] T. Yang T and L. O. Chua, IEEE Trans, Circ. Syst. I, **43**, 817-819 (1996).



Meriem Halimi is a PhD student in Automatic at CRAN, University of Lorraine, France, since 2010. His main research areas include secure communication systems, synchronization of chaotic system, mode detection and observer synthesis.

Karim Kemih received his PhD from University of Constantine in 2007. Currently, he is an Associate Professor in the Department of Electronics at Jijel University Algeria. His main research areas include secure communications system, control and synchronization of chaotic system, wireless communications; communications systems:multi-user communication, satellite and terrestrial.



Malek Ghanes received his PhD in Applied Automatic and Informatics both from IRCCyN, Ecole Centrale Nantes in 2005. From 2005 to 2006, he holds a postdoctoral position at GReyC. Since 2006, he has been an Associate Professor at ENSEA, France. His research interests include observation and control of non-linear system, with applications to electric and chaotic systems.Since Nov. 2008 he is the Head of Automatic Department. In Nov. 2012, he obtained his Accreditation to Supervise Research (HDR).