Observer-based secure communication using indirect coupled synchronization

Rupak Kharel
School of Engineering
Manchester Metropolitan University
Manchester, UK
r.kharel@mmu.ac.uk

Krishna Busawon, Z Ghassemlooy
School of Computing, Engineering and Information Sciences
Northumbria Unviversity
Newcastle Upon Tyne, UK
krishna.busawon@northumbria.ac.uk,
z.ghassemlooy@northumbria.ac.uk

***Abstract*— In this paper, an observer-based secure communication system composed of four chaotic oscillators is proposed. Observer based synchronization is achieved between two of these oscillators and employed as a transmitter and a receiver. The other two oscillators are indirectly coupled and are employed as keystream generators. The novelty lies in the generation of the same chaotic keystream both in the transmitter and receiver side for encryption and decryption purposes. We show, in particular, that it is possible to synchronize the two keystream generators even though they are not directly coupled. So doing, an estimation of the keystream is obtained allowing decrypting the message. The performance of the proposed communication scheme is shown via simulation using the Chua and Lorenz oscillators.**

Keywords- Chaotic communication systems, chaotic synchronization, Lorenz System, Chua System

I. INTRODUCTION

In recent years, there has been a growing interest in the derivation of secure communication schemes using chaotic oscillators [1-6]. In effect, various chaotic synchronization methods have been proposed [3-5, 7, 8] together with a number of modulation methods for chaotic communication systems such as chaotic masking [1, 5], parameter modulation techniques [5], chaotic shift keying [2, 5], just to mention a few. Each of these methods requires chaotic synchronization for message extraction at the receiver side. On the other hand, different attacks methods have been derived in order to test the security of the modulation methods; namely the non-linear dynamics forecasting [9, 10], return maps analysis [11], artificial neural network analysis [12] and so on. As a result, methods such as chaotic masking, parameter modulation techniques and chaotic shift keying were found not to be secure. Similarly, other proposed methods based on the projective synchronization [13], phase synchronization [14], generalized synchronized [15] were broken as well [16, 17]. Methods based on the time delay or the hyperchaos were also looked upon for increasing the security but they too were found not to be entirely convincing [18, 19]. Therefore, there is a need of developing a method which will resist all the attack methods.

In [6], a method based on encryption technique was proposed, where a different output from chaotic transmitter which was transmitted in the channel was used as a keystream to encrypt the message signal. The encrypted message signal masked with another output of the chaotic oscillator was employed as the transmitted signal. It was claimed that since the intruder could not get hold of the keystream, it was impossible for the attackers to extract the message. Unfortunately a later work done by Parker & Short [20] showed that it was still possible to extract the keystream from the transmitted chaotic signal since the keystream carried the information of the dynamics of the transmitter. In fact, since, both the carrier and keystream were the outputs of same oscillator; the carrier held the dynamics of the keystream as well. Therefore, it was impossible to hide the dynamics of the keystream from intruders, as a signal has to be transmitted from the transmitter to the receiver for synchronization and message transmission purpose. However, since the principle of the method proposed in [6] is nevertheless interesting, there is a real incentive for finding ways for improving the method by eliminating its shortcomings. Based on this observation, an indirect coupled synchronization scheme was proposed in [7]. The scheme is composed of four chaotic oscillators. First observer based chaotic synchronization is performed between the two oscillators and are employed as transmitter and receiver. The other two oscillators are indirectly coupled and are employed as keystream generators. The key idea therefore is to generate a chaotic carrier signal from one oscillator while a chaotic keystream is generated from another chaotic oscillator. A suitable encryption rule is employed in order to encrypt the message using the generated keystream. The encrypted message is then modulated with the chaotic carrier in order to generate the transmitted signal. As a result, the transmitted signal does not contain the dynamics of the keystream oscillator, hence making it difficult for intruders to generate the keystream with the sole knowledge of the transmitted chaotic signal. At the receiver, the same keystream is generated and a decryption rule is applied to the recovered encrypted message signal that has been obtained from chaotic synchronization. This particular scheme relies on the fact

that it is possible to synchronize two chaotic oscillators even though they are not coupled together directly. However, the proposed scheme only works for some classes of chaotic oscillators.

In this paper, we propose to extend the previous indirect coupled synchronization scheme to a larger class of chaotic oscillators. For this the receiver is replaced by appropriate observers.

An outline of the paper is as follow: In Section II, the main methodology of the proposed technique is explained. In addition, indirect coupled synchronization is proven for a class of chaotic systems. In Section III, the proposed synchronization and secure chaotic communication scheme are implemented using the Lorenz system and Chua's system. In Section IV, simulation is carried out and results are outlined to show the performance of the proposed communication scheme. Finally in Section V, concluding remarks are made.

II. THE PROPOSED COMMUNICATION SYSTEM

The proposed chaotic communication scheme, based on cryptography, is shown in Fig. 1. The novelty here lies in the generation of the keystream. The chaotic transmitter (T) is first used to generate two output signals, $y_1(t)$ and $y_2(t)$. The signal $y_1(t)$ is used for modulation purpose while output $y_2(t)$ is used to drive chaotic oscillator (A) whose structure is different from the transmitter (T). The output $k(t)$ of key generator (A) is used as a keystream to encrypt the message $m(t)$ using an encryption rule $\phi(.)$. The resulting encrypted signal $\phi(m(t))$ is masked using $y_1(t)$ yielding the transmitted signal $y_t(t)$. The output $y_t(t)$ is fed back into the transmitter in the form of an output injection with the aim of cancelling the effect of non-linearity while performing synchronization at the receiver side. The modulated transmitted signal $y_t(t)$ is sent through the channel to the receiver.

At the receiver end, upon receiving the signal $y_t'(t)$, the chaotic observer (R) permits to obtain an estimate $\hat{y}_1(t)$ and $\hat{y}_2(t)$of the signals $y_1(t)$ and $y_2(t)$ respectively. The signals $\hat{y}_1(t)$ and $y_t'(t)$ are used to generate an estimate $\hat{\phi}(m(t))$ of the encrypted signal $\phi(m(t))$. The estimate $\hat{y}_2(t)$ is used to drive the chaotic key generator (B) - which is similar in structure to generator (A) – and which yields the keystream estimate $\hat{k}(t)$. Consequently, the message $m(t)$ can be recovered by using the decryption rule $\phi^{-1}(.)$.

Note that since, the chaotic key generators (A) and (B) are driven by $y_2(t)$ and $\hat{y}_2(t)$ respectively, an indirect coupled synchronization is required between these two chaotic oscillators. Also, $y_2(t)$ and $\hat{y}_2(t)$ are outputs of chaotic transmitter (T) and receiver (R) respectively and will be equal once synchronization is achieved. Intuitively, one would expect this synchronization to take place. However, in what follows this will be proven mathematically for a class of chaotic systems.

The important part of this method is the generation of the keystream. No information regarding the keystream is transmitted in the channel. In [6], it was possible to estimate the particular state which was used as keystream (as shown in [20]) since the state that was transmitted in the channel had some information of the dynamics of the keystream as they were the state variables of same chaotic oscillator.

In contrast, in this method, the keystream is generated from a chaotic oscillator with a totally different structure. It will not be possible to estimate the dynamics of the chaotic key generator from the signal being transmitted in the channel by using the method mentioned in [20]. Even if the intruder manages to get hold of the encrypted signal from the transmitted signal, without the knowledge of keystream, the message signal can't be decrypted back. Therefore, a secure communication link can be realized by implementing the proposed method.

Based on the communication scheme illustrated by Fig. 1, we assume that the transmitter oscillator (T) described by a dynamical system of the following form:

$$(\mathrm{T}):\begin{cases}\dot{x} = \mathrm{F}(y_t)x + g(t, y_t)\\ y_1 = C_1 x\\ y_2 = C_2 x\\ y_t = y_1 + e(m,k),\end{cases} \tag{1}$$

where the state $x \in \mathbb{R}^n$ with initial condition $x(0) = x_0$. The outputs of the oscillator $y_1 \in \mathbb{R}$ and $y_2 \in \mathbb{R}$. The matrices **F,** C_1 and C_2 are of appropriate dimension. The signal $y_t \in \mathbb{R}$ is the transmitted signal where $e(.)$ is the encryption function using key $k(t)$ and the function g is a smooth bounded function of time.

The keystream $k(t)$ is generated using another chaotic oscillator of similar form:

$$(\mathrm{A}):\begin{cases}\dot{z} = \mathrm{A}z + b_2(t, y_2)\\ k = h(z),\end{cases} \tag{2}$$

which is driven by the output $y_2(t)$. Here, $z \in \mathbb{R}^q$ (q is not necessarily equal to n), $k \in \mathbb{R}$ is the keystream, h is an analytical vector function and b_2 is a smooth bounded function of time. It is assumed that the channel is perfect and that no distortion of the transmitted signal has taken place; that is $y_t = y_t'$.

The receiving chaotic oscillator (R) is given by:

$$(\mathrm{R}):\begin{cases}\dot{\hat{x}} = \mathrm{F}(y_t)\hat{x} + g(t, y_t) + K(y_t - \hat{y}_1)\\ \hat{y}_1 = C_1\hat{x}\\ \hat{y}_2 = C_2\hat{x}.\end{cases} \tag{3}$$

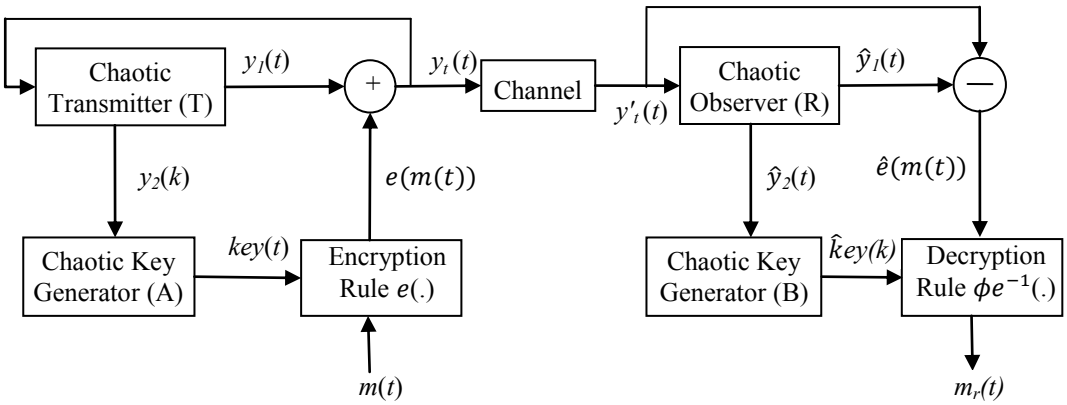

Fig. 1. Block diagram of the proposed chaotic communication based on cryptography.

Finally, the key generator (B) is given by:

$$(\mathrm{B}):\begin{cases}\dot{\hat{z}} = \mathrm{A}\hat{z} + b_2(t,\hat{y}_2) \\ \hat{k} = h(\hat{z}).\end{cases} \tag{4}$$

We shall make the following assumptions:

A1) There exist symmetric positive definite (SPD) matrices $\mathbf{P}_1$, $\mathbf{P}_2$, $\mathbf{Q}_1$ and $\mathbf{Q}_2$ such that

$$P_1(F - KC_1) + (F - KC_1)^T P_1 = -Q_1$$
$$P_2 A + A^T P_2 = -Q_2$$

A2) The output function $h(x)$ is globally Lipschitzian with respect to x.

The objective is to show that the transmitter (T) and the receiver (R) synchronize as well as generators (A) and (B) are synchronized with each other even though there is no direct link between them. In effect, based on the above assumptions, we state the following:

Theorem 1. *Under the assumption A1), there exist two constants* $\lambda, \eta > 0$ *such that* $\|x(t) - \hat{x}(t)\| \le \eta e^{-\lambda t}\|x(0) - \hat{x}(0)\|$ *for all* $t \ge 0$. *In other words, the receiver (R) synchronizes exponentially with the transmitter (T).*

Theorem 2. *Assume that system (A) and (B) satisfies assumption A1), then* $\lim_{t\to\infty}\|z(t) - \hat{z}(t)\| = 0$. *That is, the keystream generator (A) synchronizes asymptotically with the keystream generator (B).*

The proof of these two theorems are done in a similar fashion as in [7].

III. APPLICATION OF THE PROPOSED TECHNIQUE USING THE CHUA AND THE LORENZ OSCILLATOR

In this section, the performance of the proposed communication system is demonstrated using the Lorenz system as the transmitter (T) and the receiver (R). More specifically, (T) and (R) are chosen as:

$$(\mathrm{T}):\begin{cases}\dot{u} = -\sigma u + \sigma v \\ \dot{v} = -20 y_t w + r y_t - v \\ \dot{w} = 5 y_t v - b w \\ y_1 = u \\ y_2 = v \\ y_t = y_1 + e(m,k).\end{cases}$$
$$(\mathrm{R}):\begin{cases}\dot{\hat{u}} = -\sigma \hat{u} + \sigma \hat{v} \\ \dot{\hat{v}} = -20 y_t \hat{w} + r y_t - \hat{v} \\ \dot{\hat{w}} = 5 y_t \hat{v} - b \hat{w} \\ \hat{y}_1 = \hat{u} \\ \hat{y}_2 = \hat{v}.\end{cases} \tag{6}$$

Again it can easily be seen that (6) are in the form (1) and (3) with $\mathbf{F}(y_t)$ given as:

$$\mathbf{F}(y_t) = \begin{pmatrix} -\sigma & \sigma & 0 \\ 0 & -1 & -20 y_t \\ 0 & 5 y_t & -b \end{pmatrix}.$$

For these systems Assumption A1 is satisfied for the following matrices $\mathbf{P}_2$ and $\mathbf{Q}_2$:

$$\mathbf{P}_1 = \begin{pmatrix} l_1 & 0 & 0 \\ 0 & l_2 & 0 \\ 0 & 0 & l_3 \end{pmatrix} \quad \mathbf{Q}_1 = \begin{pmatrix} 2\alpha l_1 & -\alpha l_1 & 0 \\ -\alpha l_1 & l_2 & 0 \\ 0 & 0 & 2\gamma l_3 \end{pmatrix},$$

and $\boldsymbol{K}$ is chosen as

$$\mathbf{K} = \begin{pmatrix} 3\theta \\ 3\theta^2 \\ \theta^3 \end{pmatrix}$$

where θ>0.

For the key generating oscillators A and B, the Chua's system is adopted given as below:

$$(\mathrm{A}): \begin{cases} \dot{p} = \alpha(q - p - f(y_2)) \\ \dot{q} = y_2 - q - s \\ \dot{s} = -\beta q - \gamma s \\ k = d_0 p. \end{cases}$$

$$(\mathrm{B}): \begin{cases} \dot{\hat{p}} = \alpha(\hat{q} - \hat{p} - f(\hat{y}_2)) \\ \dot{\hat{q}} = \hat{y}_2 - \hat{q} - \hat{s} \\ \dot{\hat{s}} = -\beta \hat{q} - \gamma \hat{s} \\ \hat{k} = d_0 \hat{p}. \end{cases} \quad (7)$$

The non-linear function $f(\cdot)$ is a piecewise linear function given as:

$$f(\psi) = G_b\psi + 0.5(G_a - G_b)(|\psi + 1| - |\psi - 1|).$$

Note that equation (7) are in the form (2) and (4) respectively with $\mathbf{A}$ and $b_2(t, y_2)$ given as:

$$\mathbf{A} = \begin{pmatrix} -\alpha & \alpha & 0 \\ 0 & -1 & -1 \\ 0 & -\beta & -\gamma \end{pmatrix}, b_2(t, y_2) = \begin{pmatrix} -\alpha f(y_2) \\ y_2 \\ 0 \end{pmatrix}.$$

It can also be shown that Assumption A1) is satisfied for the following matrices $\mathbf{P}_2$ and $\mathbf{Q}_2$:

$$\mathbf{P}_2 = \begin{pmatrix} l_1 & 0 & 0 \\ 0 & l_2 & 0 \\ 0 & 0 & l_3 \end{pmatrix} \& \mathbf{Q}_2 = \begin{pmatrix} 2\alpha l_1 & -\alpha l_1 & 0 \\ -\alpha l_1 & l_2 & 0 \\ 0 & 0 & 2\gamma l_3 \end{pmatrix},$$

where $l_1, l_2, l_3, \alpha > 0$, $\beta < 0, \gamma \geq 0$, $l_2 = -\beta l_3$ and $0 < l_1 < \frac{4}{\alpha} l_2$. Finally, it is obvious that A2) is satisfied. For the key generating oscillators A and B, the Lorenz system defined as is adopted:

The encryption function $e(.)$ used is a n-shift cipher algorithm given as: (as used in [6]):

$e(m(t)) = \underbrace{f_1(\ldots f_1(f_1}_{n}(m(t), \underbrace{k(t)), k(t)), \ldots, k(t)}_{n}))$, where $f_1(.,.)$ is a non-linear function given by:

$$f(m,k) = \begin{cases} m + k + 2h, & \text{for } -2h \leq m + k \leq -h \\ m + k, & \text{for } -h \leq m + k \leq h \\ m + k - 2h, & \text{for } h \leq m + k \leq 2h \end{cases},$$

with h being an encryption parameter which is chosen such that m and k lie within the interval $[-h, h]$.

Once the keystream generator (A) synchronizes asymptotically with generator (B), the message $m(t)$ can be recovered using a decryption rule corresponding to the encryption rule and which is given by:

$m_r(t) = e^{-1}(\hat{e}(m(t))$

$= \underbrace{f_1(\ldots f_1(f_1}_{n}(\hat{e}(m(t), -\underbrace{\hat{k}(t)), -\hat{k}(t)), \ldots, -\hat{k}(t)}_{n}))$, where $\hat{k}(t)$ is the estimated key stream and $\hat{e}(m(t)) = y_t - \hat{y}_1$.

In the next section, simulations are carried out using Matlab/Simulink and it will be shown that the proposed method is able to synchronize satisfactorily and extract the message successfully.

IV. Simulation Results

The parameters employed in equation (15,16,18 and 19) are as follows:

$$\sigma = 16, r = 45.6, b = 4.2, \alpha = 10, \beta = -14.87$$
$$\gamma = 0, G_a = -1.27, G_b = -0.68, d_0 = 0.05, \theta = 2.$$

The encryption parameter h is chosen to be 0.3 and the message $m(t)$ is taken as a square wave modulating digital binary bits. Also in encryption rule, a 30-shift cipher is used. The initial conditions for each oscillator are chosen to arbitrarily different.

Fig. 2 shows the autocorrelation function of the keystream signal $k(t)$. It is clear that the keystream is not similar to itself with any amount of time shift so its autocorrelation function has only a single spike at point of zero time shift. This means the keystream generated is chaotic in nature and therefore has limited predictability. Fig. 3 shows the encrypted message signal and signal $k(t)$ as keystream. Fig. 4 depicts the transmitted chaotic carrier and it can be seen that message signal is totally buried inside it.

Fig. 5 illustrates the error in estimating the keystream and it can be seen that although two oscillators are starting from different initial conditions, the error converges rapidly to zero after some initial period taken for synchronization.

Fig. 6 shows the performance of the proposed method in decrypting the message signal back and it is readily seen that the transmitted message signal has been estimated convincingly. The method proposed here is an improved technique from the one mentioned in [6] where the keystream is utilized from the chaotic oscillators that have been indirectly coupled. In [6], keystream from the same chaotic oscillator, from where the transmitted chaotic signal was generated, was used. The authors in that paper has successfully shown that attack methods such as [10] that uses NLD based forecasting is not useful for the chaotic system based on cryptography. Therefore, the method proposed here is also immune to the attack method proposed in [10]. The problem in [6] was that the keystream could successfully be estimated as mentioned in [20]. Since

keystream was generated from the same oscillator as the transmitted signal, the dynamics of the keystream could be estimated, therefore possibility of revealing the transmitted message. In this method, however, the keystream is generated via indirect coupled synchronization in the transmitter and receiver from separate chaotic oscillators which have different structure and dynamics from the transmitter. Therefore, the method in [20] will not be useful to estimate the keystream.

Next, we will see another popular attack based on RM on the proposed method. It turns out that it destroys the possibility of the phase space reconstruction of the sender dynamics by analysing the transmitted chaotic signal using RM since it blurs the map and no distinct branching is seen. Fig. 7 shows the RM of the transmitted signal generated from the proposed system that modulates the digital bits. It can be seen that the map is totally blurred with no apparent information in it regarding the transmitted bits. Even if the local maxima and minima, i.e. small fluctuations, are filtered out from the transmitted signal, and RM is plotted, as shown in Fig. 8, there is no distinct branching of the RM to reveal the transmitted bits. Therefore, it can be concluded that the proposed method is immune to methods based on NLD and RM.

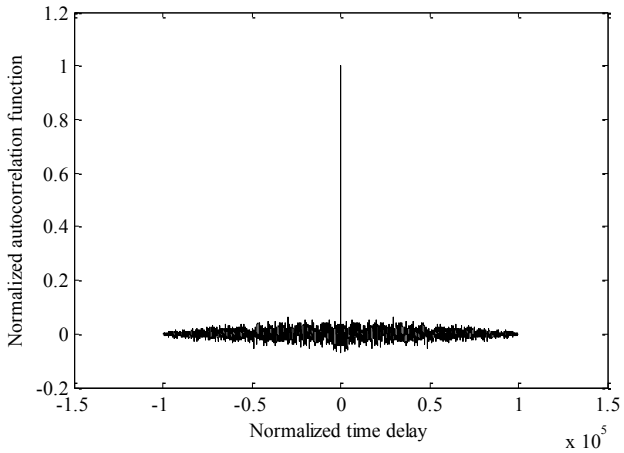

Fig. 2. Autocorrelation of key stream signal $k(t)$.

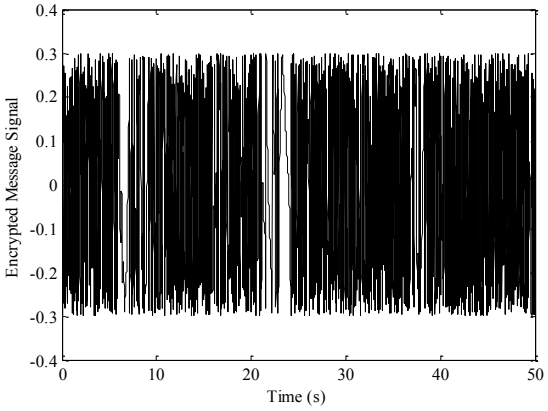

Fig. 3. Encrypted message signal $e(m(t))$.

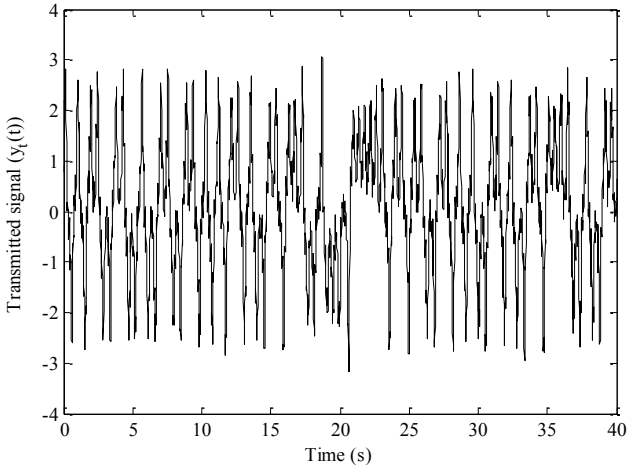

Fig. 4. Transmitted signal $y_t(t)$ generated from oscillator T.

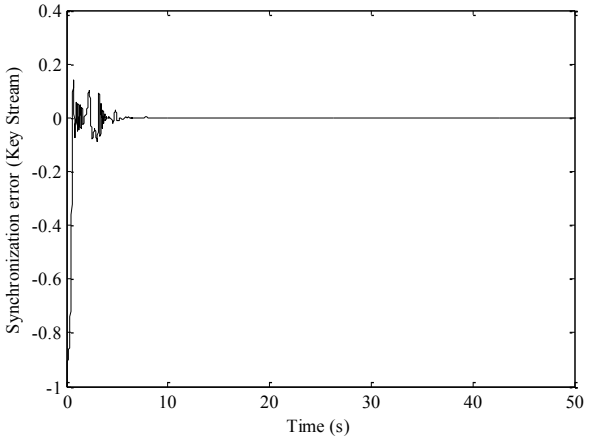

Fig. 5. Synchronization error in estimation of keystream.

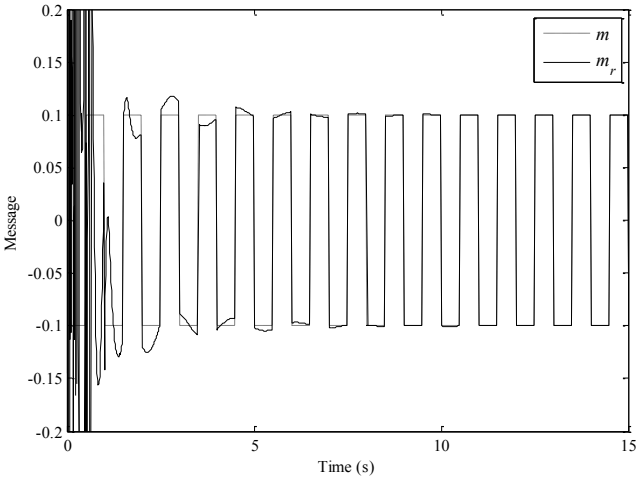

Fig. 6. Plot of the extracted message $m_r(t)$ and $m(t)$.

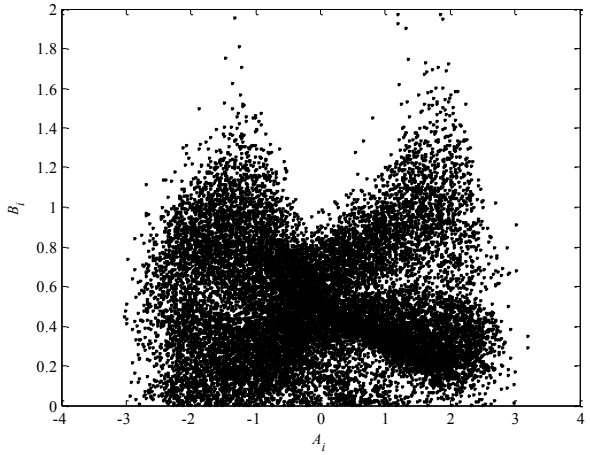

Fig. 7. Return map of the transmitted signal $y_t(t)$.

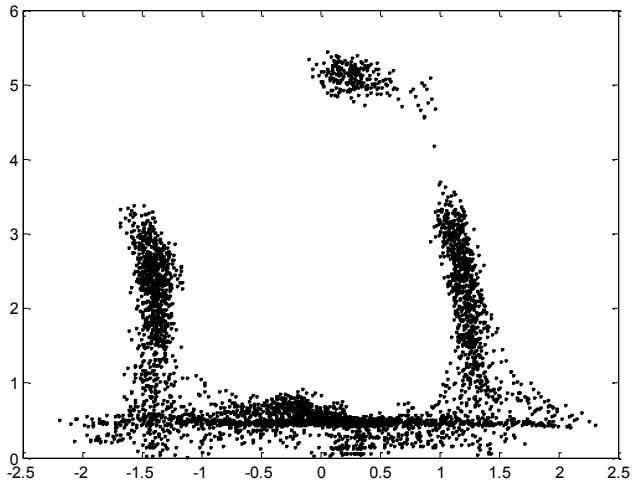

Fig. 7. Return map (small fluctuations filtered out) of the transmitted signal $y_t(t)$.

V. CONCLUSIONS

In this paper, a method of synchronizing two chaotic oscillators that are not directly coupled together in a master-slave configuration is proposed and applied to generate the keystream at transmitter and receiver. Synchronization is explained and simulation results are presented. The main advantage of the proposed method is that, unlike previous work on the topic, the keystream is generated from a different oscillator to that of the transmitter and hence improving the security of the system; since the transmitted signal does not include the information of the dynamics of the key generator. Consequently, even if the encrypted signal is known to the intruders, without the knowledge of the keystream extraction of the message signal will not be possible providing secure communication link.

REFERENCES

[1] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," Phys. Rev. Lett., vol. 71, pp. 65-68, 1993.

[2] L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," International Journal of Bifurcation and Chaos, vol. 2, pp. 973-977, 1992.

[3] M. L'Hernault, J.-P. Barbot, and A. Ouslimani, "Feasibility of Analog Realization of a Sliding-Mode Observer: Application to Data Transmission," IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 55, pp. 614-624, 2008.

[4] O. Morgul, E. Solak, and M. Akgul, "Observer based chaotic message transmission," International Journal of Bifurcation and Chaos., vol. 13, pp. 1003-1017, 2003.

[5] T. Yang, "A survey of chaotic secure communication systems," International Journal of Computational Cognition, vol. 2, pp. 81-130, 2004.

[6] T. Yang, C. W. Wu, and L. O. Chua, "Cryptography based on chaotic systems," IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications, vol. 44, pp. 469-472, 1997.

[7] R. Kharel, K. Busawon and Z. Ghassemlooy, Secure communication based on indirect coupled synchronization, Globenet, Reunion, 2012.

[8] H. Nijmeijer and I. M. Y. Mareels, "An observer looks at synchronization," IEEE Transactions on Circuits and Systems - I: Fundamental thoery and applications, vol. 44, pp. 882-890, 1997.

[9] K. M. Short, "Steps toward unmasking secure communications," International Journal of Bifurcation and Chaos, vol. 4, pp. 959-977, 1994.

[10] K. M. Short, "Unmasking a modulated chaotic communications scheme," International Journal of Bifurcation and Chaos, vol. 6, pp. 367-375, 1996.

[11] T. Yang, L. B. Yang, and C. M. Yang, "Cryptanalyzing chaotic secure communication using return maps," Physics Letters A, vol. 245, pp. 495-510, 1998.

[12] T. Yang, L. B. Yang, and C. M. Yang, "Application of neural networks to unmasking chaotic secure communication," Physica D, vol. 124, pp. 248-257, 1998.

[13] Z. Li and D. Xu, "A secure communication scheme using projective chaos synchronization," Chaos, Solitons & Fractals, vol. 22, pp. 477-481, 2004.

[14] J. Y. Chen, K. W. Wong, L. M. Cheng, and J. W. Shuai, "A secure communciation scheme based on the phase synchronization of chaotic systems," Chaos, vol. 13, pp. 508-514, 2003.

[15] M. Boutayeb, M. Darouach, and H. Rafaralahy, "Generalized State-Space Observers for Chaotic Synchronization and Secure Communication," IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications, vol. 49, pp. 345-349, 2002.

[16] G. Alvarez, S. Li, F. Montoya, M. Romera, and G. Pastor, "Breaking projective chaos synchronization secure communication using filtering and generalized synchronization," Chaos Solitons & Fractals, vol. 24, pp. 775-883, 2005.

[17] G. Alvarez, F. Montoya, G. Pastor, and M. Romera, "Breaking a secure communication scheme based on the phase synchronization of chaotic systems," Chaos, vol. 14, pp. 274-278, 2004.

[18] K. M. Short and A. T. Parker, "Unmasking a hyperchaotic communication scheme," Physical Review E, vol. 58, pp. 1159-1162, 1998.

[19] C. Zhou and C. H. Lai, "Extracting messages masked by chaotic signals of time-delay systems," Physical Review E, vol. 60, pp. 320-323, 1999.

[20] A. T. Parker and K. M. Short, "Reconstructing the keystream from a chaotic encryption," IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications, vol. 48, pp. 624-630, 2001.