A Novel Chaotic Encryption Technique for Secure Communication

Rupak Kharel, K. Busawon, Z. Ghassemlooy

School of Computing, Engineering and Information Sciences,
Northumbria University, NE1 8ST, UK
(Tel: 441912273841; e-mail: rupak.kharel@unn.ac.uk).

Abstract: In this work, a novel chaotic encryption technique is proposed to realize a secure communication system. In the proposed method, the message signal to be transmitted is first encrypted using a chaotic keystream and then modulated with a chaotic signal. At the receiver end, the received chaotic signal is used for synchronization and to recover the encrypted signal. After applying the same keystream used in transmitter side, the message signal could be decrypted back. The main contribution of this work is generation of the keystream which is not part of the transmitter chaotic oscillator but is produced using an oscillator of a different structure.

Keywords: Chaotic cryptosystem, synchronization, secure communication.

1. INTRODUCTION

In recent years, there has been major works done in order to utilize chaotic signals in secure communication. Being fundamentally broadband, sensitive to initial conditions, aperiodic and noise like yet having deterministic behaviour make chaotic signals a potential for secure communication. Many methods had been proposed in order to realize secure communication systems using chaotic signals (Cuomo and Oppenheim, 1993, Yang, 2004). Basically, there are two important issues related to chaotic communication; one being the synchronization of the transmitter and the receiver chaotic oscillator and the other is message signal mixing or modulation using the chaotic carrier such that the information is not revealed and a secure link is realized. There are a number of synchronization techniques that have been proposed such as Pecora & Caroll drive-response method (Pecora and Carroll, 1990), control theory based observer method (Nijmeijer and Mareels, 1997), extended Kalman filtering method (Fallahi et al., 2008), filtering method (Cruz and Nijmeijer, 2000) etc. to name a few. In addition to synchronization, the method adopted to mask, hide or modulate the message signal via the chaotic oscillator is very important for the communication link to be secure.

The chaotic masking method which consists in adding a low power message signal with the chaotic carrier was among the very first method proposed in (Cuomo and Oppenheim, 1993). However, lots of attacks methods have also been proposed to show that the masking method is not secure enough (Alvarez et al., 2004, Huang et al., 2001, Perez and Cerdeira, 1995, Short, 1994). Method of chaotic shift keying, parametric modulation and inclusion method has also been proposed but to no avail (Short, 1996, Yang et al., 1998). For a complete survey, the readers are encouraged to refer (Yang, 2004). A hybrid chaotic communication scheme was proposed in (Yang et al., 1997) where an encryption of the information signal using a keystream was also suggested. The keystream was one component of the chaotic system which was not transmitted. The transmitted chaotic signal was then used to recover the keystream, in the receiver side, by the method of chaotic synchronization and by employing the decryption function the information signal was revealed. It was claimed that, since the keystream was unavailable in the transmitted signal, one cannot possibly decrypt the message signal back; even if the encrypted signals was obtained by some means. The key reconstruction could not be performed by the intruders since there would be a large function space to choose from. However, the work by (Parker and Short, 2001) showed that the proposed method was not full proof because the keystream can still be obtained only by the knowledge of transmitted signal.

This present work is based on the spirit of the work done by (Yang et al., 1997). We present a new method to generate the chaotic keystream from an oscillator that is different to the transmitter. The keystream thus generated is used to encrypt the message signal. This encrypted message signal is combined with the chaotic carrier generated by transmitter oscillator and sent through the channel to the receiver. At the receiver side, the same chaotic oscillator which was used to generate the keystream in transmitter side is employed. The keystream was then applied to decrypt the encrypted signal. The encrypted signal is obtained via chaotic synchronization. Now the question arises, how is it possible to generate the same keystream signal from two chaotic systems independent from each other placed at transmitter and receiver side? The question is very valid because it is known that two chaotic systems, even if they have similar structure, starting from slightly different initial conditions will rapidly decorrelate from each other. So, in first appearance it might seem that the method proposed here will not work. However, we will show that it is still possible to synchronize these two chaotic oscillators that generate keystream even if they are not uni-directionally coupled as done in almost all previous chaotic communication systems. We demonstrate our method by using the Lorenz and the Chua oscillator.

An outline of the paper is as follows: In the next section a qualitative description of the proposed method is given. In Section 3, we demonstrate the method by the Lorenz and the Chua oscillator. Finally, some simulations are carried out and some conclusions are drawn.

2. PROPOSED TECHNIQUE

The proposed chaotic communication, 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) which is not necessarily of the same structure as 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 $e(.)$. The resulting encrypted signal $e(m(t))$ is modulated using $y_1(t)$ yielding the transmitted signal $y_t(t)$. The output $y_t(t)$ is fed back in to the transmitter as a form of output injection with the aim of reducing the effect of non-linearity while performing synchronization at the receiver side. The 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 receiver (R) - which is similar in structure to the transmitter (T) - 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 by synchronization. This can be done by using any techniques existing in the literature (Nijmeijer and Mareels, 1997, Morgul et al., 2003, L'Hernault et al., 2008). The signals $\hat{y}_1(t)$ and $y'_t(t)$ are used to generate an estimate $\hat{e}(m(t))$ of the encrypted signal $e(m(t))$. The estimate $\hat{y}_2(t)$ is used to drive the chaotic key generator (B) - which is similar in structure to generator (A) – which yields the keystream estimate $\hat{k}(t)$. Consequently, the message $m(t)$ can be recovered by using the decryption rule $d(.)$.

Note that since, the chaotic key generators (A) and (B) are driven by $y_2(t)$ and $\hat{y}_2(t)$ respectively, a non-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 obtained. Intuitively, one would expect this synchronization to take place. However, we will prove this mathematically in the next section using the Lorenz and Chua oscillator.

The important part of this method is the generation of the keystream. No information regarding the key stream is transmitted in the channel. In (Yang et al., 1997), the state which was used as keystream was possible to be estimated as shown in (Parker and Short, 2001) since the state which was transmitted in the channel had some information of the dynamics of the keystream since they were states of same chaotic oscillator. But in this method, the keystream is generated from totally different structured chaotic oscillator. 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 methods mentioned in (Parker and Short, 2001). Even if the intruder manages to get the encrypted signal from the transmitted signal, without the knowledge of keystream, message signal could not be decrypted back. Therefore, a secure communication link can be realized by implementing the proposed method.

3. IMPLEMENTATION USING LORENZ & CHUA OSCILLATOR

The method proposed above is implemented by using the Lorenz and the Chua's oscillator. Oscillators (T) and (R) are designed using Lorenz's equations while key generating oscillators (A) and (B) are designed using Chua's oscillator. The Lorenz's equations are given by:

$$\begin{cases} \dot{u} = -\sigma u + \sigma v \\ \dot{v} = -20uw + ru - v \\ \dot{w} = 5uv - bw, \end{cases} \quad (1)$$

where σ, r and b are constants. The dimensionless Chua's equations are given by:

$$\begin{cases} \dot{p} = \alpha(q - p - f(p)) \\ \dot{q} = p - q - s \\ \dot{s} = -\beta q - \gamma s, \end{cases} \quad (2)$$

where α, β and γ are constants and $f(x)$ is the piecewise-linear characteristic of the Chua's diode which is given by,

$$f(p) = G_b p + 0.5(G_a - G_b)(|p+1| - |p-1|),$$

where $G_a < G_b < 0$.

Based on the communication scheme illustrated by Fig. 1, we assume that $y_1 = u$ and $y_2 = v$ so that the state equation for oscillator (T) can be expressed as:

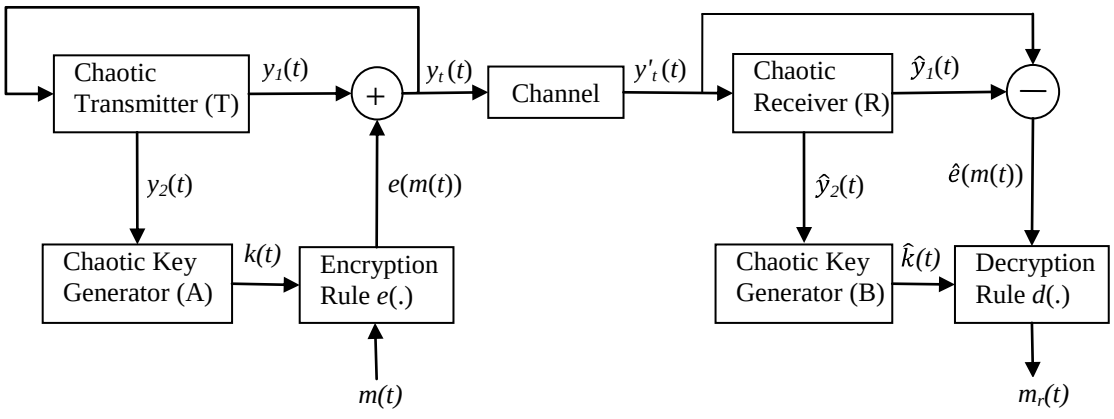

Fig. 1. Block diagram of the proposed chaotic communication based on cryptography.

$$(\mathrm{T}):\begin{cases}\dot{u}=-\sigma u+\sigma v\\ \dot{v}=-20y_t w+ry_t-v\\ \dot{w}=5y_t v-bw\\ y_1=u\\ y_2=v\\ y_t=y_1+e\big(m(t)\big).\end{cases}\tag{3}$$

The encryption function *e*(.) used is a *n*-shift cipher algorithm as used in (Yang et al., 1997) and is given as,

$$e\big(m(t)\big)=\underbrace{f_1(\dots f_1(f_1}_{n}(m(t),\underbrace{k(t)),k(t),\dots,k(t)}_{n}),\tag{4}$$

where $f_1(*,*)$ is the following non-linear function

$$f_1(m,k)=\begin{cases}(m+k)+2h, & -2h\le(m+k)\le-h\\ (m+k), & -h<(m+k)<h\\ (m+k)-2h, & h\le(m+k)\le 2h.\end{cases}$$

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

The keystream $k(t)$ is generated using the Chua's equations described as in (2) where the latter is driven by the output y_2 of transmitter (T). More specifically, the keystream generator (A) is expressed as,

$$(\mathrm{A}):\begin{cases}\dot{p}=\alpha\big(q-p-f(y_2)\big)\\ \dot{q}=y_2-q-s\\ \dot{s}=-\beta q-\gamma s\\ k=d_0 p,\end{cases}\tag{5}$$

where d_0 is a scaling factor such that $k(t)$ lie within the interval [-*h*,*h*]. Note that here the signal $y_2(t)$ is injected in the nonlinearity *f* (.).

We assume that the channel is perfect and that no distortion of the transmitted message has taken place; that is $y_t'=y_t$.

The state equation of oscillator (R) is defined as,

$$(\mathrm{R}):\begin{cases}\dot{\hat{u}}=-\sigma\hat{u}+\sigma\hat{v}\\ \dot{\hat{v}}=-20y_t\hat{w}+ry_t-\hat{v}\\ \dot{\hat{w}}=5y_t\hat{v}-b\hat{w}\\ \hat{y}_1=\hat{u}\\ \hat{y}_2=\hat{v}.\end{cases}\tag{6}$$

It will be shown that oscillator (T) and (R) will synchronize with each other. For this, we will first present a technical lemma that will be used subsequently.

Lemma 1. *Consider the time varying matrix*

$$\mathbf{A}\big(\xi(t)\big)=\begin{pmatrix}-a & a & 0\\ 0 & -d & -\xi(t)\\ 0 & \delta\xi(t) & -c\end{pmatrix},\tag{7}$$

where $\xi(t)$ is real valued function of time and a, d, c and δ are positive real numbers. Let **P** *and* **Q** *be two symmetric matrices defined as*

$$\mathbf{P}=\begin{pmatrix}l_1 & 0 & 0\\ 0 & l_2 & 0\\ 0 & 0 & l_3\end{pmatrix}\ and\ \mathbf{Q}=\begin{pmatrix}2al_1 & -al_1 & 0\\ -al_1 & 2dl_2 & 0\\ 0 & 0 & 2cl_3\end{pmatrix},\tag{8}$$

with $l_1,l_2,l_3>0$ and $l_2=\delta l_3$ and $0<l_1<\frac{4d}{a}l_2$. Then **P** *and* **Q** *are positive definite and satisfy the following algebraic Lyapunov equation*

$$\mathbf{PA}(\xi(t))+\mathbf{A}^{\mathrm{T}}(\xi(t))\mathbf{P}=-\mathbf{Q}.\tag{9}$$

for all t.

Proof: First let us show that **P** and **Q** are indeed positive definite (SPD) matrices. It is clear that **P** is SPD since l_1, l_2 *and* l_3 are all positive. Let $\boldsymbol{\nu}=(x\quad y\quad z)^T\epsilon R^3$ then after some simplification, it can be shown that

$$\boldsymbol{\nu}^T\mathbf{Q}\boldsymbol{\nu}=2al_1\left(x-\frac{y}{2}\right)^2+2al_1\left(\frac{dl_2}{al_1}-\frac{1}{4}\right)y^2+2cl_3z^2.$$

Since $l_1<\frac{4d}{a}l_2$, the term $\frac{dl_2}{al_1}-\frac{1}{4}>0$ and consequently, $\boldsymbol{\nu}^T\mathbf{Q}\boldsymbol{\nu}>0$ for all $\boldsymbol{\nu}\epsilon R^3$. Now, a direct computation shows that

$$\mathbf{PA}\big(\xi(t)\big)+\mathbf{A}^{\mathrm{T}}\big(\xi(t)\big)\mathbf{P}=-\mathbf{Q}.\qquad\blacksquare$$

Remark 1. *Note that, at first sight, one would expect the matrices* **P** *and* **Q** *to be time dependent since* $\mathbf{A}(\xi(t))$ *is time dependent. However, interestingly enough, due to the particular form of* $\mathbf{A}(\xi(t))$ *the matrices* **P** *and* **Q** *turn out to be constant.*

We now state our first result:

Theorem 1. *The receiver (R) synchronises exponentially with the transmitter (T). More precisely, $\exists\mu>0$ such that $\|\boldsymbol{e}(t)\|\le exp(-\mu t)\,\|\boldsymbol{e}(0)\|$ where $\boldsymbol{e}=(e_u,\ e_v,\ e_w)^T$ with $e_u=u-\hat{u}$, $e_v=v-\hat{v}$ and $e_w=w-\hat{w}$.*

Proof: By defining $\boldsymbol{e}(t)$ as above, error dynamics between the transmitter (T) and the receiver (R) is given by:

$$\dot{\boldsymbol{e}}=\begin{pmatrix}\dot{e}_u\\ \dot{e}_v\\ \dot{e}_w\end{pmatrix}=\begin{pmatrix}-\sigma & \sigma & 0\\ 0 & -1 & -20y_t\\ 0 & 5y_t & -b\end{pmatrix}\begin{pmatrix}e_u\\ e_v\\ e_w\end{pmatrix}=\mathbf{A}(y_t(t))\boldsymbol{e}.\tag{10}$$

$\mathbf{A}(y_t(t))$ is of the form (7) where $\xi(t)=20y_t(t)$, $\delta={}^1\!/_4$, $a=\sigma, d=1$ and $b=c$. Considering Lemma 1, a candidate Lyapunov function of error dynamics can now be defined as:

$$\mathrm{V}(\boldsymbol{e})=\boldsymbol{e}^T\mathbf{P}\boldsymbol{e},$$

where **P** is of the same form as in (8) with values $l_1,l_2,l_3>0\ and\ l_2=\delta l_3\ and\ 0<l_1<\frac{4}{\sigma}l_2$.

Therefore,

$$\dot{V}(\boldsymbol{e}) = 2\boldsymbol{e}^{T}\mathbf{P}\dot{\boldsymbol{e}} = 2\boldsymbol{e}^{T}\mathbf{P}\mathbf{A}(y_t(t))\boldsymbol{e}.$$

Owing to Lemma 1, we have

$$\dot{V}(\boldsymbol{e}) = -\boldsymbol{e}^{T}\mathbf{Q}\boldsymbol{e} < 0,$$

where **Q** is as in (8) with values chosen earlier. Consequently,

$$\| \dot{\boldsymbol{e}}(t) \| = -\mu \| \boldsymbol{e}(\boldsymbol{t}) \|,$$

where μ is the ratio of the smallest eigenvalue of **Q** and the smallest eigen value of **P**.

Therefore $\| \boldsymbol{e}(t) \| \leq exp(-\mu t) \| \boldsymbol{e}(0) \|$. Hence, system (10) is exponentially stable. ■

Now, let us consider the synchronisation of the keystream generators (A) and (B). Based on Fig. 1, the keystream generator (B) is expressed as:

$$(\mathrm{B}): \begin{cases} \dot{\hat{p}} = \alpha\left(\hat{q} - \hat{p} - f(\hat{y}_2)\right) \\ \dot{\hat{q}} = \hat{y}_2 - \hat{q} - \hat{s} \\ \dot{\hat{s}} = -\beta\hat{q} - \gamma\hat{s}. \end{cases} \tag{11}$$

Now, set $\boldsymbol{\varepsilon} = \left(e_p,\ e_q,\ e_s\right)^{\mathrm{T}} = (p - \hat{p},\ q - \hat{q},\ r - \hat{r})^{\mathrm{T}}$. Then, the error dynamics between generators (A) and (B) is given by:

$$\begin{pmatrix} \dot{e}_p \\ \dot{e}_q \\ \dot{e}_s \end{pmatrix} = \begin{pmatrix} -\alpha & \alpha & 0 \\ 0 & -1 & -1 \\ 0 & -\beta & -\gamma \end{pmatrix} \begin{pmatrix} e_p \\ e_q \\ e_s \end{pmatrix} + \begin{pmatrix} \alpha[f(y_2) - f(\hat{y}_2)] \\ y_2 - \hat{y}_2 \\ 0 \end{pmatrix}. \tag{12}$$

One can rewrite the error dynamics as:

$$\dot{\boldsymbol{\varepsilon}} = \mathbf{F}\boldsymbol{\varepsilon} + \boldsymbol{g}(y_2, \hat{y}_2). \tag{13}$$

Theorem 2. *The origin of system (13) is asymptotically stable. In other words, the keystream generator (A) synchronises asymptotically with keystream generator (B).*

Proof (sketch): The matrix **F** is similar to matrix **A** in (7) with $\xi(t) = 1, \delta = -\beta, a = \alpha, d = 1$ and $c = \gamma$. Owing to Lemma 1, a candidate Lyapunov function of the error dynamics (13) is simply given by:

$$\mathbf{W}(\boldsymbol{\varepsilon}) = \boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{P}\boldsymbol{\varepsilon} = \| \boldsymbol{\varepsilon} \|^2.$$

where **P** is as in (8) with values $l_1, l_2, l_3 > 0$ *and* $l_2 = -\beta l_3$ *and* $0 < l_1 < \frac{4}{\alpha} l_2$.

Therefore,

$$\begin{aligned} \dot{\mathbf{W}}(\boldsymbol{\varepsilon}) &= 2\boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{P}\dot{\boldsymbol{\varepsilon}} \\ &= 2\boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{P}[\mathbf{F}\boldsymbol{\varepsilon} + \boldsymbol{g}(y_2, \hat{y}_2)] \\ &= 2\boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{P}\mathbf{F}\boldsymbol{\varepsilon} + 2\boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{P}\boldsymbol{g}(y_2, \hat{y}_2) \\ &= -\boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{Q}\boldsymbol{\varepsilon} + 2\boldsymbol{\varepsilon}^{\mathrm{T}}\mathbf{P}\boldsymbol{g}(y_2, \hat{y}_2). \end{aligned}$$

where **Q** is as in (8) with values chosen accordingly.

Now,

$$\dot{\mathbf{W}}(\boldsymbol{\varepsilon}) \leq -\lambda\mathbf{W}(\boldsymbol{\varepsilon}) + 2|\boldsymbol{\varepsilon}\mathbf{P}\boldsymbol{g}(y_2, \hat{y}_2)|,$$

where λ is the ratio of the smallest eigenvalue of **Q** and the largest eigen value of **P**.

After some computation and using norms of **P** and **Q**, one can show that there exists two positive constant $\bar{\lambda}$ and $\bar{k}$ such that,

$$\begin{aligned} \dot{\mathbf{W}}(\boldsymbol{\varepsilon}) &\leq -\bar{\lambda}\mathbf{W}(\boldsymbol{\varepsilon}) + \bar{k}\|\boldsymbol{e}\|^2 \\ &= -\bar{\lambda}\mathbf{W}(\boldsymbol{\varepsilon}) + \bar{k}\exp(-\mu t) \| \boldsymbol{e}(0) \|. \end{aligned} \tag{14}$$

due to Theorem 1.

We can see from (14) that **W** satisfies a linear differential equation which can easily be solved and from which one can conclude that $\| \boldsymbol{\varepsilon}(\mathrm{t}) \| \to 0$ as $t \to +\infty$. ■

Remark 2: It was seen that $\delta = -\beta$ and since k>0, β has to be < 0. Also, if we had chosen Lorenz for key generating oscillator as well, exponential convergence would have been possible as shown in Theorem 1. But in order to enhance the security by not allowing the intruder to know the system dynamics whatsoever of the chaotic key generating oscillator, a different structured oscillator, Chua's circuit, is chosen although only asymptotic synchronization is realized.

Once the keystream generator (A) synchronises 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:

$$\begin{aligned} m_r(t) &= d\left(\hat{e}\left(m(t)\right)\right) \\ &= \underbrace{f_1(\ldots f_1(f_1}_{n}(\hat{e}(m(t)), -\underbrace{\hat{k}(t)), -\hat{k}(t), \ldots, -\hat{k}(t))}_{n}, \end{aligned}$$

where $\hat{k}(t)$ is the estimated key stream where $\hat{e}\left(m(t)\right) = y_t - \hat{y}_1$.

It is now clear that the performance of generator (A) to synchronise with generator (B) is crucial to the perfect recovery of message signal but is of less significance since (A) is exponentially converging to (B) as shown in theorem 1.

In the next section, simulation will be performed and it will be shown that the proposed method is able to extract the message successfully.

4. SIMULATION RESULTS AND ANALYSIS

In this section the performance of the proposed scheme will be verified using the simulation package Matlab/Simulink.

The parameters in equation (3), (5), (6), (11) are given as follows,

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

The encryption parameter $h=0.3$ and the message $m(t)= 0.1sin(2\pi t)$. Also, in encryption rule (4), a 30-shift cipher is used. The initial conditions for each oscillator are chosen arbitrarily different.

Fig. 2 shows the encrypted message signal using (4) and signal $k(t)$ as a key. Fig. 3 shows the transmitted signal. It can be seen that the transmitted signal is a chaotic signal and the message signal is totally buried in it.

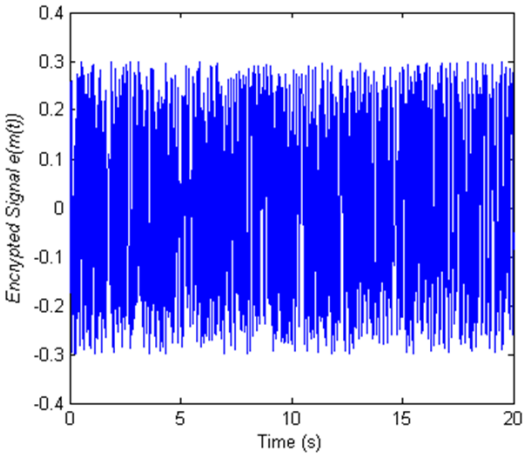

Fig. 2. Encrypted message signal $e(m(t))$.

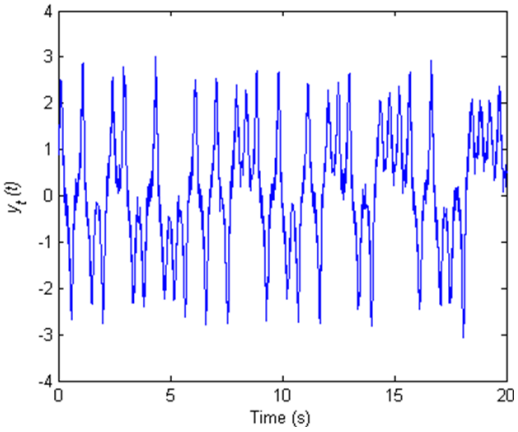

Fig. 3. Transmitted Signal y_t (t) generated from Oscillator (T).

Fig. 4 shows the error in estimating the keystream. It can be seen that after some initial period, the error is converging rapidly to zero. Fig. 5 shows the recovered message signal and it can be seen that the message signal has been estimated convincingly.

Next, we will test the performance of the proposed method in the presence of noise since any practical channel comprises

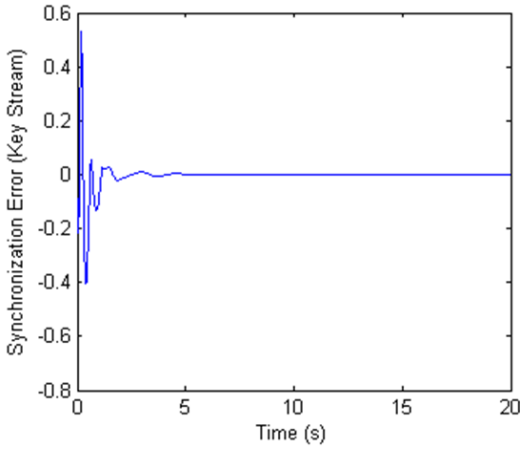

Fig. 4. Synchronization error in the estimation of keystream.

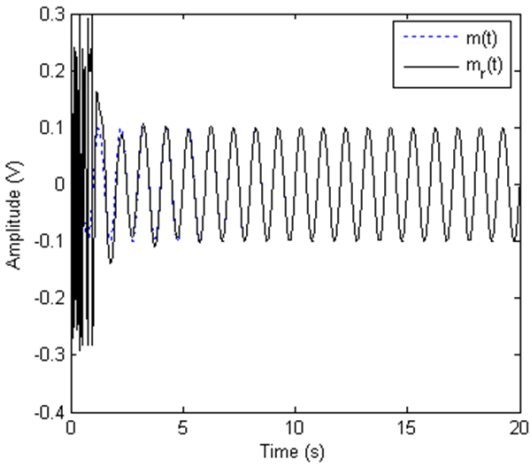

Fig. 5. Plot of extracted message $m_r(t)$ versus transmitted message signal $m(t)$.

of some level of noise in it. For this purpose, an additive white Gaussian noise (AWGN) channel is used having signal-to-noise ratio (SNR) of 40dB. This level of SNR is chosen since in (Alvarez and Li, 2006), it is mentioned that for a practically viable chaotic cryptography scheme the recommended value of the SNR is 40 dB. Fig. 6 shows the message extracted from the proposed method even in the presence of noise. Apart from the jitter in amplitude, which can be removed from standard filtering operation, the necessary information about the message (form, frequency and amplitude) is obtained.

5. CONCLUSIONS

A secure chaotic communication scheme is proposed and simulation results are shown. The proposed method is secure because the key used to encrypt the message sequence is not part of the transmitted chaotic signal in fact even the oscillator. A non-coupled synchronization is obtained between two chaotic oscillators at transmitter and receiver to generate the keystream and the synchronization for both sets of chaotic oscillators is proven mathematically. Since, both oscillators are driven by a common signal, synchronization was possible. Even if the encrypted signal is produced by

some attack method, without the knowledge of key stream; intruders will not be able to retrieve the message back. No attack methods reported until now can estimate the keystream, since there is no information whatsoever of the dynamics of key generating chaotic oscillator. Hence, the method proposed here can be claimed to be secure. Also, the performance of accurately estimating the message signal under the influence of AWGN channel with SNR = 40dB is shown and therefore the proposed method is practicable in real environment.

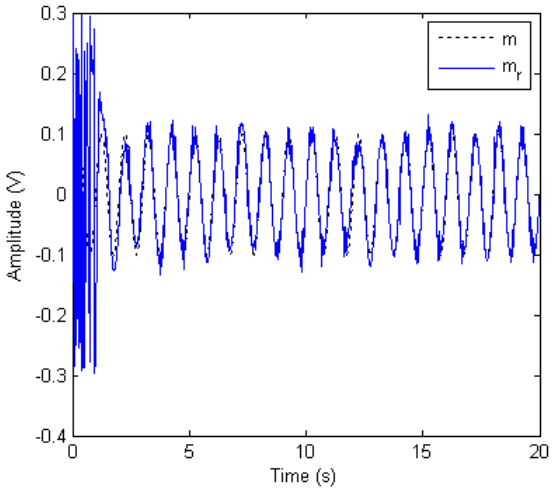

Fig. 6. Message extraction in AWGN channel of SNR 40 dB.

REFERENCES

ALVAREZ, G., MONTOYA, F., ROMERA, M. & PASTOR, G. (2004) Breaking Two Secure Communication Systems Based on Chaotic Masking. *IEEE Transaction on Circuit and Systems-II: Express Briefs*, 51**,** 505-506.

ALVAREZ, G. & LI, S. (2006) Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *International Journal of Bifurcation and Chaos*, 16**,** 2129-2151.

ALVAREZ, G., MONTOYA, F., ROMERA, M. & PASTOR, G. (2004) Breaking Two Secure Communication Systems Based on Chaotic Masking. *IEEE Transaction on Circuit and Systems-II: Express Briefs*, 51**,** 505-506.

CRUZ, C. & NIJMEIJER, H. (2000) Synchronization through filtering. *International Journal of Bifurcation and Chaos*, 10**,** 763-775.

CUOMO, K. M. & OPPENHEIM, A. V. (1993) Circuit implementation of synchronized chaos with applications to communications. *Phys. Rev. Lett.*, 71**,** 65-68.

FALLAHI, K., RAOUFI, R. & KHOSHBIN, H. (2008) An application of Chen system for secure chaotic communication based on extended Kalman filter and multi-shift cipher algorithm *Communications in Nonlinear Science and Numerical Simulation*, 13**,** 763-781.

HUANG, X., XU, J., HUANG, W. & LU, Z. (2001) Unmasking chaotic mask by a wavelet multiscale decomposition algorithm. *International Journal of Bifurcation and Chaos*, 11**,** 561-569.

L'HERNAULT, M., BARBOT, J.-P. & OUSLIMANI, A. (2008) Feasibility of Analog Realization of a Sliding-Mode Observer: Application to Data Transmission. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 55**,** 614-624.

MORGUL, O., SOLAK, E. & AKGUL, M. (2003) Observer based chaotic message transmission. *International Journal of Bifurcation and Chaos.*, 13**,** 1003-1017.

NIJMEIJER, H. & MAREELS, I. M. Y. (1997) An observer looks at synchronization. *IEEE Transactions on Circuits and Systems - I: Fundamental thoery and applications*, 44**,** 882-890.

PARKER, A. T. & SHORT, K. M. (2001) Reconstructing the keystream from a chaotic encryption. *IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications*, 48**,** 624-630.

PECORA, L. M. & CARROLL, T. L. (1990) Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64**,** 821-824.

PEREZ, G. & CERDEIRA, H. A. (1995) Extracting messages masked by chaos. *Phys. Rev. Lett.*, 74**,** 1970-1973,.

SHORT, K. M. (1994) Steps toward unmasking secure communications. *International Journal of Bifurcation and Chaos*, 4**,** 959-977.

SHORT, K. M. (1996) Unmasking a modulated chaotic communications scheme. *International Journal of Bifurcation and Chaos*, 6**,** 367-375.

YANG, T. (2004) A survey of chaotic secure communication systems. *International Journal of Computational Cognition*, 2**,** 81-130.

YANG, T., WU, C. W. & CHUA, L. O. (1997) Cryptography based on chaotic systems. *IEEE Transactions on Circuits and Systems-I: Fundamental Theory and Applications*, 44**,** 469-472.

YANG, T., YANG, L. B. & YANG, C. M. (1998) Application of neural networks to unmasking chaotic secure communication. *Physica D*, 124**,** 248-257.