A Chaos-Based Communication Scheme Using Proportional and Proportional-Integral Observers

R. Kharel*, K. Busawon* and Z. Ghassemlooy*

Abstract: In this paper, we propose a new chaos-based communication scheme using the observers. The novelty lies in the masking procedure that is employed to hide the confidential information using the chaotic oscillator. We use a combination of the addition and inclusion methods to mask the information. The performance of two observers, the proportional observer (P-observer) and the proportional integral observer (PI-observer) is compared that are employed as receivers for the proposed communication scheme. We show that the P-observer is not suitable scheme since it imposes unpractical constraints on the messages to be transmitted. On the other hand, we show that the PI-observer is the better solution because it allows greater flexibility in choosing the gains of the observer and does not impose any unpractical restrictions on the message.

Keywords: Chaotic Synchronization, Duffing Oscillator, P & PI-observers, Secure Communication.

1 Introduction

There has been a growing interest in the problem of synchronisation of chaotic systems for secure communication purposes over the last decade. Being fundamentally broadband, the presence of information signal does not necessarily change the properties of the transmitted modulated chaotic carrier signal. Although it offers an advantage from a security viewpoint, the output power remains constant regardless of the information content (or lack of it). Note that, when a chaotic signal is adopted as a carrier, the unmodulated bandwidth is infinite (or it is clearly a broadband) compared to a conventional narrowband sinusoidal based carrier signal. Indeed, several chaotic communication schemes have been developed using different techniques including the method via addition/masking [1-6], chaotic shift keying [3, 7], chaotic modulation [3, 8] or inclusion [3, 9-11] etc. The classical masking technique where the message is added to the output of the chaotic oscillator or transmitter is illustrated in Fig. 1. This method of masking is sometimes known as the chaotic masking or masking by addition or simply the addition method [2]. In this scheme a message signal $m(t)$ is superimposed on to the chaotic carrier signal $y(t)$ before being transmitted over a communication channel. At the receiver, an observer is used to generate an estimate $\hat{y}(t)$ of $y(t)$ from the received signal $y_t(t) = y(t) + m(t)$. This implies that a certain degree of robustness must be exhibited by the observer in generating the estimated output $\hat{y}(t)$ since it is excited by the masked signal $y_t(t)$ which obviously provides only partial information about the carrier signal $y(t)$.

This implies that $m(t)$ should not be of too high amplitude and should be at least 20 to 30 dB lower than $y(t)$ [2]. As a result one drawback of this method is that it is difficult to retrieve the message if channel noise power is of the same order to that of the message power. One important criterion of the masking method is such that the strange attractor of the oscillator is not modified by the message. A message recovery module is used to recover $m(t)$, which performs the following subtraction:

$$m_r(t) = y_t(t) - \hat{y}(t) = y(t) - \hat{y}(t) + m(t) \qquad (1)$$

Here we have assumed that the channel is ideal and noise free hence $y_t(t) \approx y'_t(t)$. The observer is generally designed such that $\lim_{t\to+\infty} |y(t) - \hat{y}(t)| \to 0$. As a result, the difference $\xi(t) = y_t(t) - \hat{y}(t) = m_r(t)$ will

Iranian Journal of Electrical & Electronic Engineering, 2008.
Paper first received 25th June 2008 and in revised form 14th October 2008.
* The Authors are with the School of Computing, Engineering and Information Sciences, Northumbria University, Newcastle Upon Tyne, UK.
E-mail: rupak.kharel@unn,ac,uk, krishna.busawon@unn.ac.uk, fary.ghassemlooy@unn.ac.uk.

asymptotically converge to $m(t)$. Obviously, if $\hat{y}(t)$ converges exponentially to $y(t)$, then we will have a better convergence between $m_r(t)$ and $m(t)$. However, it has been shown that the above scheme is not perfectly secure [12-14]. In effect, it has been made known that this method of masking is sensitive to the external attack. Parameter modulation technique can be employed but it is shown to be insecure as well [15].

One alternative scheme to overcome this problem is to employ the method of inclusion [3, 10, 11, 16, 17] as illustrated in Fig. 2. In this method the message is either included in a state or the derivative of the state of the chaotic oscillator while a different state is used as the transmitted signal. This method has been proven to be more secure than the chaotic masking by addition scheme because it uses the message to modify the strange attractor of the chaotic oscillator. Also the transmitted state does not carry any information of the message or key. This signal is used only to synchronize with the oscillator at the receiving end to generate the key. Care should be taken so that the inclusion of the message does not disturb the chaotic regime of the oscillator and bring it to a normal periodic motion. However, with the inclusion method the message recovery becomes more difficult since it requires a inverse system at the receiving end [10, 16]. This problem is regarded as left invertible problem.

To address the above two issues, we propose the hybrid inclusion and the chaotic masking technique as illustrated in Fig. 3. In this scheme, the message signal actually drives the chaotic oscillator in addition to being superimposed on to the chaotic carrier signal. We compare the effectiveness of the above schemes by using a class of chaotic oscillators. We study the effect of employing two different observers at the receiver; namely a proportional observer (P-observer) and a proportional integral observer (PI-observer) [18]. We show that the P-observer does not work properly for this particular oscillator. In effect, a residual term is always present in the error dynamics of the observer, which implies that the convergence of the observer is only asymptotic. Also, the inclusion of the message signal changes the chaotic regime of the oscillator into a normal periodic behaviour.

On the other hand we show that the PI-observer is the most adequate solution for this scheme when using the Duffing oscillator. The gain of the PI-observer can be chosen in such a way that the effect of the message signal is negligible in the error dynamics. Simulations are carried out to support the above argument and to show the performance of both observers. In Section 2 details are described for the observer based chaotic communication systems using the P-observer and the PI-observer. Also, the message recovery procedure is described mathematically and the simplicity of using a hybrid system to recover the message signal is shown. Simulations are carried out for both observers using the Duffing oscillator and the performance are compared and presented in Section 3. Finally, concluding remarks are outlined in Section 4.

2 Main Methodology

There are number of possible methods that have been developed for synchronization in chaotic communications. In the masking method, synchronization is achieved by simply if the conditional Lyapunov exponents for the systems are negative for the given operating parameters. Thus, one could simply recover the message signal from the received chaotic signal through by means of a subtraction at the receiver. This synchronization is robust against small perturbations of the carrier signal. In the chaotic modulation method the message signal becomes part of the dynamics, which is more robust because of the greater symmetry between chaotic oscillator and response. In the chaos shift keying technique the message information is encoded onto the attractor by means of modulating a parameter of the chaotic oscillator, typically in a binary manner. In all these three schemes synchronization is an obvious way of recovering the original information. In this section, the proposed observer-based chaotic synchronization scheme for a secure communication link, illustrated by Fig. 3, is described.

We assume that the transmitter is a chaotic system described by:

$$\left.\begin{aligned} \dot{\mathbf{x}} &= \mathbf{A}\mathbf{x} + \mathbf{B}f(y) + \mathbf{h}(t) \\ y &= \mathbf{C}\mathbf{x} \end{aligned}\right\} \tag{2}$$

where $\mathbf{x} \in R^n$, $y \in R$, f is a smooth function and h is the forcing function. The matrices A, B and C are of the following form:

$$\mathbf{A} = \begin{pmatrix} 0 & 1 & & 0 \\ \vdots & & \ddots & \\ & & & 1 \\ a_1 & & \cdots & a_n \end{pmatrix}, \quad \mathbf{B} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \tag{3}$$
$$\mathbf{C} = \begin{pmatrix} 1 & \mathbf{0}_{1\times n-1} \end{pmatrix}$$

For simplicity, we have considered only one non linearity to clarify the design procedure. Note that many chaotic systems, if not of the above form, can be transformed into it by a change of variable. However the Duffing oscillator is already of the above form.

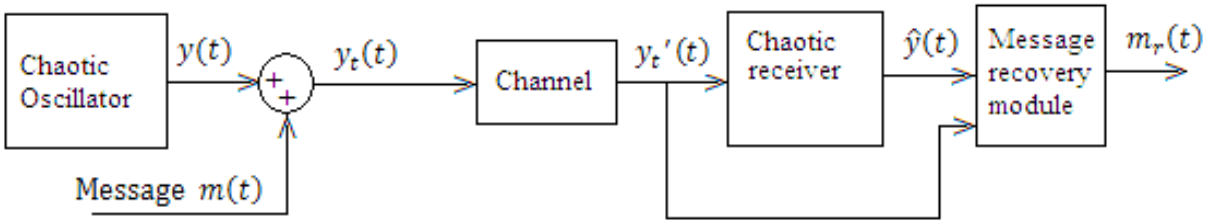


Fig. 1 A schematic block diagram of chaotic masking system.

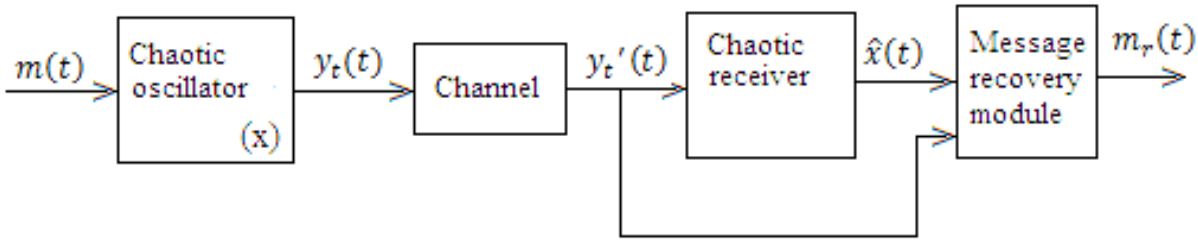


Fig. 2 Schematic block diagram of chaotic inclusion method.

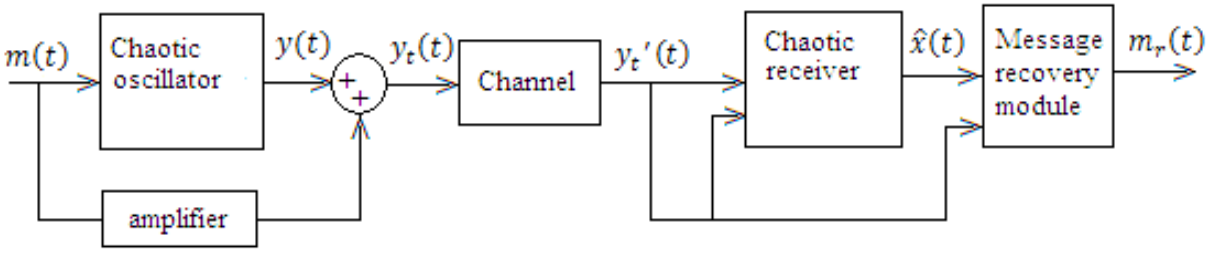


Fig. 3 A block diagram of the hybrid chaotic masking and inclusion method.

2.1 Masked System

According to the proposed scheme, the masked system is described as:

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}\mathrm{f}(\mathrm{y}_t) + \mathbf{h}(\mathrm{t}) + \mathbf{B}\mathrm{m}(\mathrm{t}) \\ \mathrm{y}_t = \mathbf{C}\mathbf{x} + \mathrm{d}_0\mathrm{m}(\mathrm{t}) \end{cases} \tag{4}$$

Note, that the message is located in the last row; i.e. on the derivative of the state variable x_n.

2.2 Proportional-Observer-Based Scheme

A classical Luenberger type observer for the masked system (4) is given by:

$$\begin{aligned} \dot{\hat{\mathbf{x}}} &= \mathbf{A}\hat{\mathbf{x}} + \mathbf{B}\mathrm{f}(\mathrm{y}_t) + \mathbf{h}(\mathrm{t}) + \mathbf{K}_\mathrm{p}(\mathrm{y}_t - \mathbf{C}\hat{\mathbf{x}}) \\ \dot{\hat{\mathbf{x}}} &= (\mathbf{A} - \mathbf{K}_\mathrm{p}\mathbf{C})\hat{\mathbf{x}} + \mathbf{B}\mathrm{f}(\mathrm{y}_t) + \mathbf{h}(\mathrm{t}) + \mathbf{K}_\mathrm{p}\mathrm{y}_t \end{aligned} \tag{5}$$

where the gain $\mathbf{K}_\mathrm{p}$ is chosen such that the matrix $(\mathbf{A} - \mathbf{K}_\mathrm{p}\mathbf{C})$ is stable so that the error converges to zero as we will see later.

We shall show that Eq. (5) is an asymptotic observer for Eq. (4). In effect, let $\mathbf{e} = \mathbf{x} - \hat{\mathbf{x}}$ be the error between real and estimated states. Then, the error dynamics is given by:

$$\begin{aligned} \dot{\mathbf{e}} &= \mathbf{A}\mathbf{e} + \mathbf{B}\mathrm{m}(\mathrm{t}) - \mathbf{K}_\mathrm{p}(\mathrm{y}_t - \mathbf{C}\hat{\mathbf{x}}) \\ &= \mathbf{A}\mathbf{e} + \mathbf{B}\mathrm{m}(\mathrm{t}) - \mathbf{K}_\mathrm{p}(\mathbf{C}\mathbf{x} + \mathrm{d}_0\mathrm{m}(\mathrm{t}) - \mathbf{C}\hat{\mathbf{x}}) \\ &= (\mathbf{A} - \mathbf{K}_\mathrm{p}\mathbf{C})\mathbf{e} + (\mathbf{B} - \mathbf{K}_\mathrm{p}\mathrm{d}_0)\mathrm{m}(\mathrm{t}) \\ &= (\mathbf{A} - \mathbf{K}_\mathrm{p}\mathbf{C})\mathbf{e} + \mathbf{E}\mathrm{m}(\mathrm{t}) \end{aligned} \tag{6}$$

Ideally, we would like to choose such that in order to eliminate the influence of the message on the error dynamic $\dot{\mathbf{e}}$. This is mainly because the message here is seen as a 'noise' which is affecting the convergence of

the error to zero. However, if $\mathbf{K}_p = \mathbf{B}d_0^{-1}$ then it is not possible to arbitrarily choose the eigen values of the matrix $\mathbf{A}-\mathbf{K}_p\mathbf{C}$ so that the latter is stable. Consequently, one has to choose $\mathbf{K}_p$ judiciously such that the matrix $\mathbf{A}-\mathbf{K}_p\mathbf{C}$ is stable while at the same time reducing the influence of m(t). It is clear that one cannot achieve exponential convergence of the error to zero with the proportional observer. Only asymptotic convergence to zero can be achieved, therefore the message is retrieved by performing the following difference:

$$y_t(t)-\hat{y}(t)=y(t)-\hat{y}(t)+d_0m(t)=\xi(t). \tag{7}$$

Since $\lim_{t\to\infty}\left|y_t(t)-\hat{y}_t(t)\right|\to 0$, we have:

$$m(t)\approx\frac{\xi(t)}{d_0}=m_r(t) \tag{8}$$

We shall see next that the PI-observer provides a better solution in terms of much reduced influence of the message signal on the error dynamics.

2.2 Proportional-Integral Observer-Based Scheme

Fig. 4 depicts a block diagram of PI-observer based communication systems, where an integrator s^{-1} is placed at the receiver side. As shown in figure, both the transmitted message and its integrated version are applied to the chaotic receiver in order to provide an estimate of the state of the oscillator. To design the PI-observer, we set $x_0=\int_0^t y_t(\tau)d\tau=y_I$. In other words $\dot{x}_0=y_t=x_1+d_0m(t)$. We then have the following augmented system:

$$\begin{cases}\dot{x}_0=x_1+d_0m(t)\\ \dot{\mathbf{x}}=\mathbf{A}\mathbf{x}+\mathbf{B}f(y_t)+\mathbf{h}(t)+\mathbf{B}m(t)\\ y_t=x_1+d_0m(t)\\ y_I=x_0\end{cases} \tag{9}$$

A PI-observer for the above system is given by:

$$\begin{aligned}\dot{\hat{x}}_0&=\hat{x}_1+l_0(y_t-\hat{x}_1)+k_0(y_I-\hat{x}_0)\\ \dot{\hat{\mathbf{x}}}&=\mathbf{A}\hat{\mathbf{x}}+\mathbf{B}f(y_t)+\mathbf{h}(t)+\mathbf{K}_p(y_t-\mathbf{C}\hat{\mathbf{x}})+\mathbf{L}_I(y_I-\hat{x}_0)\end{aligned} \tag{10}$$

where $\mathbf{K}_p$ and $\mathbf{L}_I$ are the proportional gain and the integral gain, respectively. It should be noted that channel is considered to be ideal with unity gain and noise free in Eq. (10).

We will show that Eq. (10) is an asymptotic observer for Eq. (9) but offering greater flexibility with regards to the choice of the gains compared to the proportional observer. For this, let $\mathbf{e}=\mathbf{x}-\hat{\mathbf{x}}$ and $e_0=x_0-\hat{x}_0$. Then, the error dynamics is given by:

$$\begin{aligned}\dot{e}_0&=e_1+d_0m(t)-k_0(y_t-\hat{x}_1)-l_0(y_I-\hat{x}_0)\\ \dot{\mathbf{e}}&=\mathbf{A}\mathbf{e}+\mathbf{B}m(t)-\mathbf{K}_p(y_t-\hat{x}_1\mathbf{C}\hat{\mathbf{x}})-\mathbf{L}_I(y_I-\hat{x}_0)\end{aligned} \tag{11}$$

After replacing y_t and y_I by their expression, we get:

$$\begin{aligned}\dot{e}_0&=e_1+d_0m(t)-k_0(e_1+d_0m(t))-l_0e_0\\ \dot{\mathbf{e}}&=\mathbf{A}\mathbf{e}+\mathbf{B}m(t)-\mathbf{K}_p(e_1+d_0m(t))-\mathbf{L}_Ie_0\end{aligned} \tag{12}$$

After simplification, we obtain:

$$\begin{aligned}\dot{e}_0&=-l_0e_0+(1-k_0)e_1+(1-k_0)d_0m(t)\\ \dot{\mathbf{e}}&=-\mathbf{L}_Ie_0+\mathbf{A}\mathbf{e}-\mathbf{K}_pe_1+(\mathbf{B}-\mathbf{K}_pd_0)m(t)\end{aligned} \tag{13}$$

We now choose the gains as follows:

$$\begin{aligned}k_0&=1-\varepsilon\\ \mathbf{K}_p&=d_0^{-1}\mathbf{B}\end{aligned} \tag{14}$$

We then obtain:

$$\begin{aligned}\dot{e}_0&=-l_0e_0+\varepsilon e_1+\varepsilon d_0m(t)\\ \dot{\mathbf{e}}&=-\mathbf{L}_Ie_0+\mathbf{A}\mathbf{e}-d_0^{-1}\mathbf{B}e_1\end{aligned} \tag{15}$$

The main idea here is to make the error dynamic less dependent on the message as much as possible. However, one could not choose $k_0=1$ this is because the first equation of augmented system Eq. (9) will be independent from the remaining equations; hence making it impossible to choose $\mathbf{L}_I$ in order to stabilise the overall augmented system.

The Eq. (13) can be written in the matrix form as follows:

$$\begin{aligned}\begin{bmatrix}\dot{e}_0\\ \dot{\mathbf{e}}\end{bmatrix}&=\begin{bmatrix}-l_0 & \varepsilon\overline{\mathbf{C}}\\ -\mathbf{L}_I & \mathbf{A}-\frac{1}{d_0}\mathbf{B}\overline{\mathbf{C}}\end{bmatrix}\begin{bmatrix}e_0\\ \mathbf{e}\end{bmatrix}+\begin{bmatrix}\varepsilon d_0\\ 0\end{bmatrix}m(t)\\ &=\mathbf{F}\begin{bmatrix}e_0\\ \mathbf{e}\end{bmatrix}+\overline{\mathbf{E}}m(t)\end{aligned} \tag{16}$$

where $\overline{\mathbf{C}}=\begin{bmatrix}0 & 1 & 0 & \cdots & 0\end{bmatrix}$.

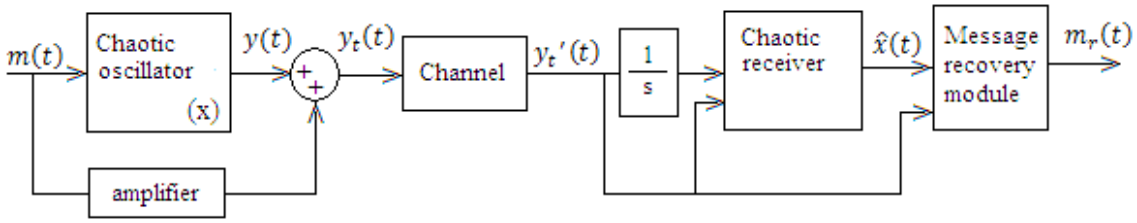


Fig. 4 A block diagram of PI-observer based scheme.

We can now choose $\mathbf{L}_1$ such that the matrix $\mathbf{F}$ is stable. Also, we can choose ε and d_0 to be small in order to diminish the effect of m(t) on the error dynamics. As before, when the convergence is achieved, the message is retrieved by calculating the following difference equation:

$$y_t(t) - \hat{y}(t) = y(t) - \hat{y}(t) + d_0 m(t) = \xi(t).$$

Again, since $\lim_{t\to+\infty} |y(t) - \hat{y}(t)| \to 0$, we can have:

$$m(t) \approx \xi(t)/d_0 = m_r(t) \tag{17}$$

We can see that the PI-observer scheme offers more flexibility on the choice of gains in order to deal with the effect of m(t) on the error dynamics. This will be demonstrated with an example using the Duffing oscillator in the next section.

3 Application Using the Duffing Oscillator

In this section, we shall compare both P and PI-observer-based synchronization schemes described in Fig. 4 when using the Duffing oscillator as the drive system, which is described by [4]:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = -x_1/4 - x_1^3 + 11\cos t \end{cases} \tag{18}$$

We assume that the state variable x_1 is measured, i.e. the output equation is $y = x_1$ so that the system can be written in a matrix form as:

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}f(y) + \mathbf{h}(t) \\ y = \mathbf{C}\mathbf{x} \end{cases} \tag{19}$$

where

$$\mathbf{A} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ \mathbf{B} = \begin{pmatrix} 0 \\ 1 \end{pmatrix},\ \mathbf{C} = \begin{pmatrix} 1 & 0 \end{pmatrix}$$
$$f(y) = -y/4 - y^3,\ \mathbf{h}(t) = \begin{pmatrix} 0 \\ 11\cos t \end{pmatrix} \tag{20}$$

Therefore, this system is in the form described by Eq. (2).

Here the masked system is given by:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = -\dfrac{y_t}{4} - y_t^3 + 11\cos t + m(t) \\ y_t = x_1 + d_0 m(t) \end{cases} \tag{21}$$

Note that m(t) is present in the derivative of the second state variable x_2 and the output of the system $y_t(t)$. The masked system can be written in matrix form as:

$$\begin{cases} \dot{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{B}f(y_t) + \mathbf{h}(t) + \mathbf{B}m(t) \\ y_t = \mathbf{C}\mathbf{x} + d_0 m(t) \end{cases} \tag{22}$$

3.1 P Observer-Based Scheme

Using the methodology described above, a classical Luenberger type observer for the masked system Eq. (22) is given by:

$$\dot{\hat{\mathbf{x}}} = \mathbf{A}\hat{\mathbf{x}} + \mathbf{B}f(y_t) + \mathbf{h}(t) + \mathbf{K}_p(y_t - \mathbf{C}\hat{\mathbf{x}}) \tag{23}$$

where the gain $\mathbf{K}_p = \begin{pmatrix} k_1 & k_2 \end{pmatrix}^T$ is chosen such that the matrix $(\mathbf{A} - \mathbf{K}_p\mathbf{C})$ is stable. More precisely, we have:

$$\begin{cases} \dot{\hat{x}}_1 = \hat{x}_2 + k_1(y_t - \hat{x}_1) \\ \dot{\hat{x}}_2 = -y_t/4 - y_t^3 + 11\cos t + k_2(y_t - \hat{x}_1) \end{cases} \tag{24}$$

3.1.1 Results

A simulation of the above observer and the message recovery method was carried out using Matlab and Simulink. The poles of the observer were set as $p_1 = -0.1 = p_2$ so that $k_1 = 0.2$ and $k_2 = 0.01$. Therefore, $d_0 = -k_2^{-1} = -100$ In addition, we have used the following numerical values: $x_1(0) = x_2(0) = 0$, $\hat{x}_1(0) = 0$ and $\hat{x}_2(0) = 0.1$. The message consisted of a

set of a sinusoidal signal of amplitude and frequency of 0.1 V and 10 Hz, respectively. Using equations (21) and (24) the proposed scheme was simulated using Matlab Simulink as shown in Fig. 5. Fig. 6 depicts the profile of the output $y_t(t)$ of the oscillator. We can readily see that with the inclusion of the message within the oscillator, there is no longer a chaotic regime. Fig. 7 shows the attractor after including the message signal and it can be seen that the attractor of the Duffing oscillator has been totally modified and is no longer operating on a chaotic mode. Fig. 8 illustrates the original and the recovered (dotted lines) message signals. The effect of **E**m(t) given in Eq. (6) on error dynamics can readily be seen on the message recovery. This is because the term **E**m(t) is still non-zero having a real value. The best scenario would be to make **E**m(t) equal to zero, however by doing so the degree of freedom will be lost and the whole point of designing the observer will make no sense. Also, if **E**m(t) is chosen to be zero, then **A** matrix of the chaotic oscillator should itself be stable for error dynamics converging to 0. However, the effect can be minimized by choosing high value of d_0.

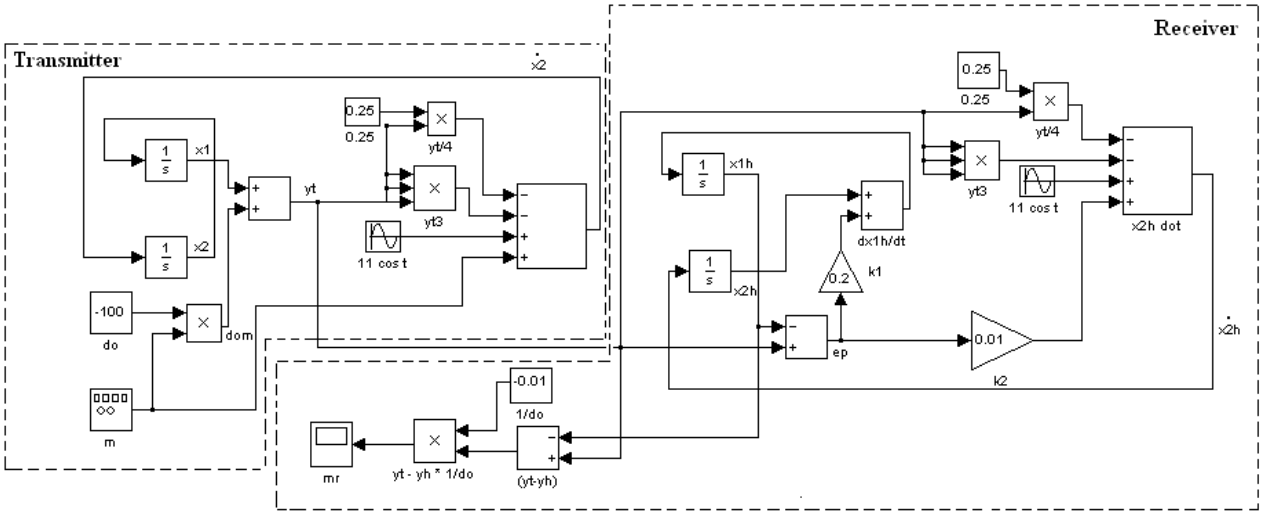


Fig. 5 A schematic Simulink block diagram of P-observer based system.

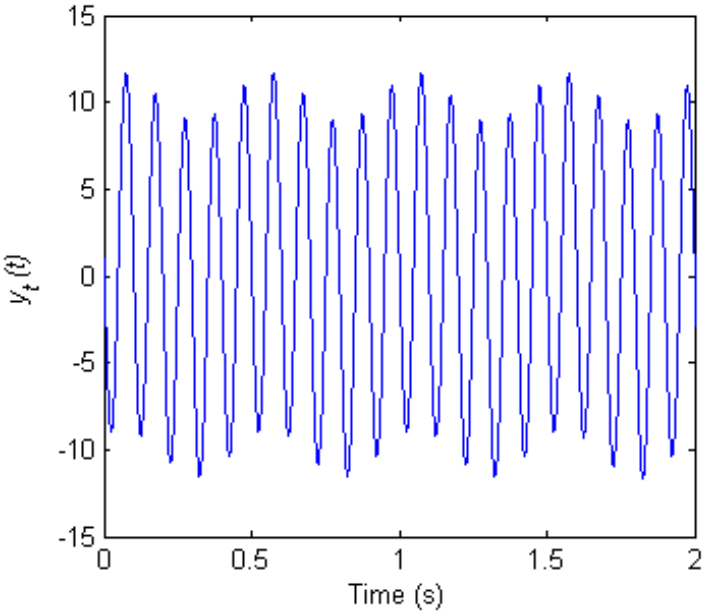


Fig. 6 Transmitter oscillator output $y_t(t)$ waveform for P-observer.

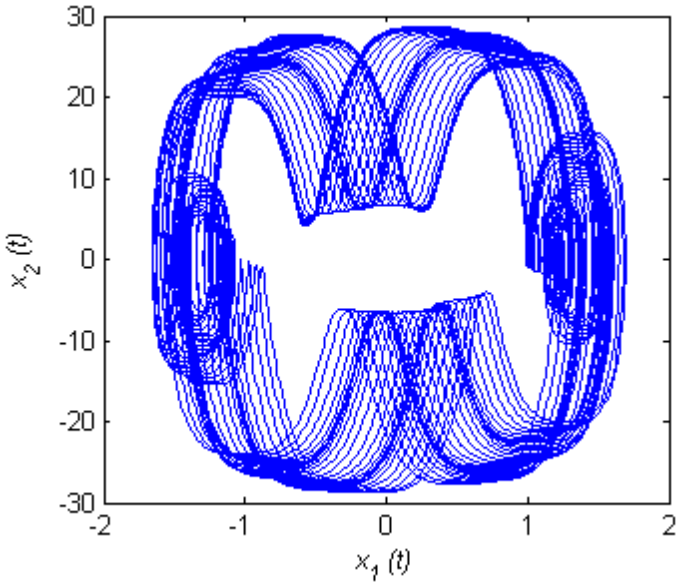


Fig. 7 Strange attractor of Duffing Oscillator with P-observer.

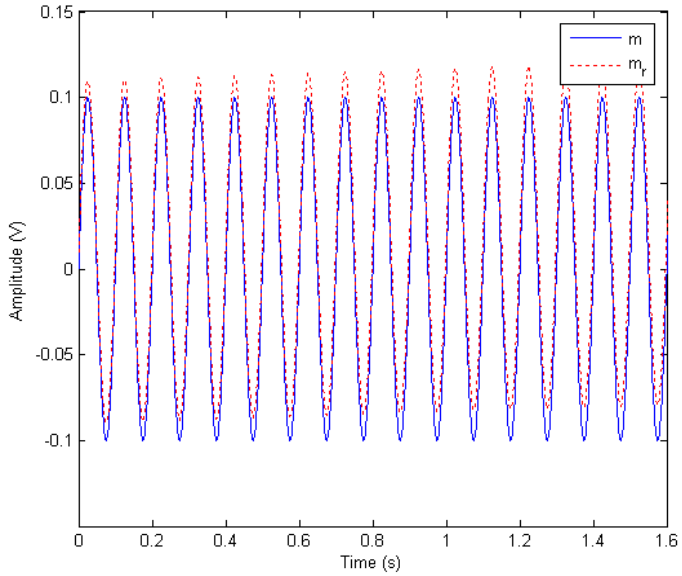


Fig. 8 Input and recovered message signals for P-observer.

The other main problem with the P-observer is that amplitude of m(t) affect the chaotic behaviour of the oscillator which is due to the requirement to choose high value of d_0 in order to remove the influence on error dynamics. To recover back the chaotic behaviour of the oscillator, the amplitude of m(t) needs reducing significantly; more than 100 times although it is not shown here. Hence, the above communication scheme cannot operate properly in practice if a proportional observer is employed as a receiver since it enforces impractical constraint on the message to be transmitted. In the next section we show that the PI-observer is the more suitable observer for the proposed communication scheme.

3.2 PI-Observer-Based Scheme

Following the PI-observer methodology described above, we set $x_0 = \int_0^t y_t(\tau)d\tau = y_I$.

In other words $\dot{x}_0 = y_t = x_1 + d_0 m(t)$. We then have the following augmented system:

$$\begin{cases} \dot{x}_0 = x_1 + d_0 m(t) \\ \dot{x}_1 = x_2 \\ \dot{x}_2 = -y_t/4 - y_t^3 + 11\cos t + m(t) \\ y_t = x_1 + d_0 m(t) \\ y_I = x_0 \end{cases} \qquad (25)$$

The PI-observer for the above system is given by:

$$\begin{cases} \dot{\hat{x}}_0 = \hat{x}_1 + l_0(x_0 - \hat{x}_0) + k_0(y_t - \hat{x}_1) \\ \dot{\hat{x}}_1 = \hat{x}_2 + l_1(x_0 - \hat{x}_0) + k_1(y_t - \hat{x}_1) \\ \dot{\hat{x}}_2 = -y_t/4 - y_t^3 + 11\cos t + l_2(x_0 - \hat{x}_0) + k_2(y_t - \hat{x}_1) \end{cases} \quad (26)$$

Using the gains in (14), we have:

$$\begin{cases} \dot{\hat{x}}_0 = \hat{x}_1 + l_0(x_0 - \hat{x}_0) + (1-\varepsilon)(y_t - \hat{x}_1) \\ \dot{\hat{x}}_1 = \hat{x}_2 + l_1(x_0 - \hat{x}_0) \\ \dot{\hat{x}}_2 = -y_t/4 - y_t^3 + 11\cos t + l_2(x_0 - \hat{x}_0) + 1/d_0(y_t - \hat{x}_1) \end{cases} \quad (27)$$

And $(l_0 \quad l_1 \quad l_2)^T$ is chosen such that the overall error dynamics is stable.

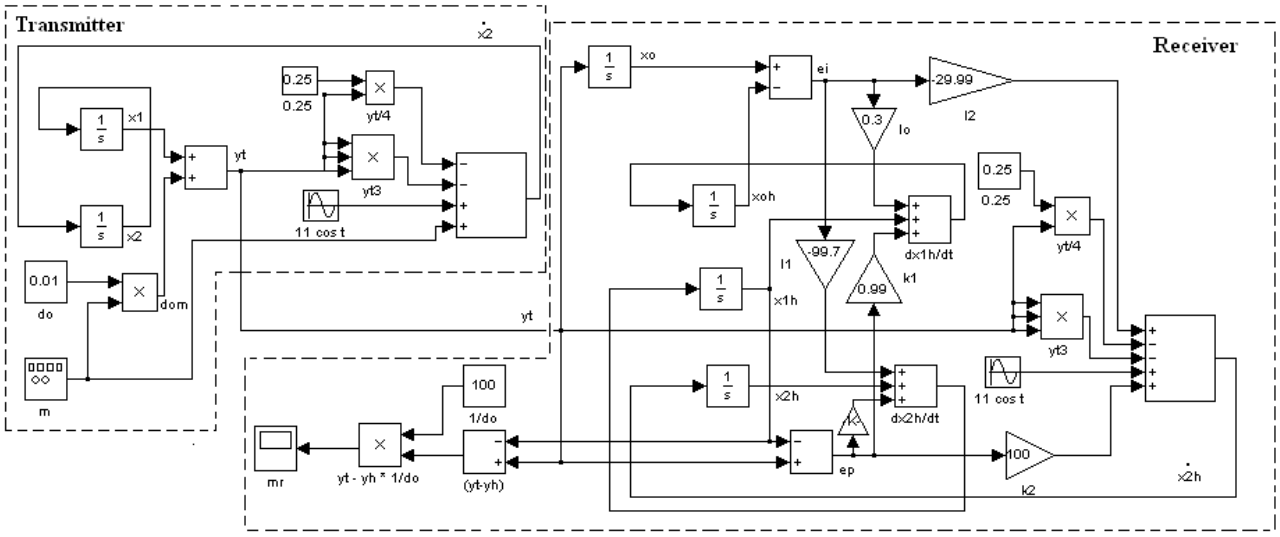


Fig. 9 A block diagram of Simulink implementation of PI-observer based system.

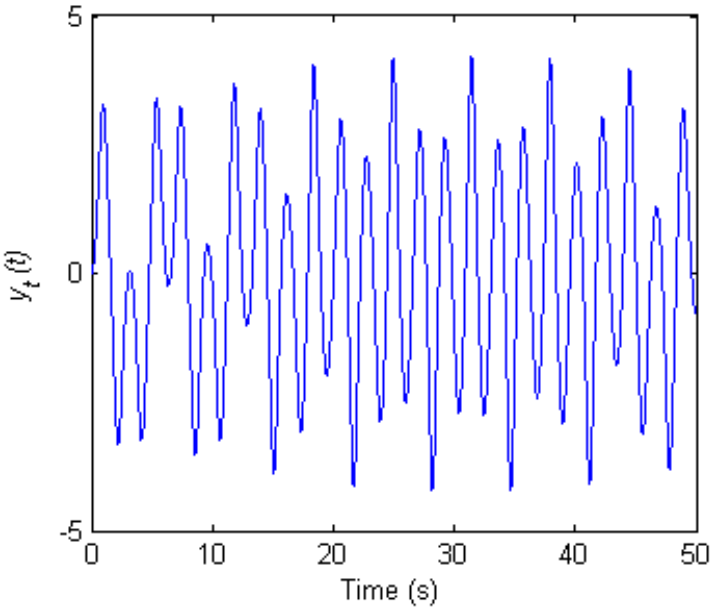


Fig. 10 Transmitter oscillator output $y_t(t)$.

3.2.1 Results

For simulation purposes we have chosen $d_0 = \varepsilon = 0.01$ so that $k_0 = 0.99$ and $k_2 = 100$. In addition $x_0(0) = x_1(0) = x_2(0) = 0$, $\hat{x}_0(0) = \hat{x}_1(0) = 0$ and $\hat{x}_2(0) = 0.1$. The poles of the observer are all set at $p = 0.1$ so that $l_0 = 0.3$, $l_1 = -99.7$ and $l_2 = -29.99$. As before, the message consisted of a set of a sinusoidal signal of amplitude and frequency of 0.1 V and 10 Hz, respectively. Equations (25) and (26) were adopted for Matlab Simulink simulation as shown in Fig. 9. Fig. 10 shows the transmitter oscillator output $y_t(t)$ waveform. Here we can see that the chaotic regime is maintained and the transmitted signal is scrambled and not discernible. Fig. 11 depicts the strange attractor of the oscillator after the inclusion of message signal illustrating how the states evolve over time in a complex and and non-repetitive pattern. Both the input and the recovered message waveforms with very little delay are shown in Fig. 12. Once the observer has completed synchronisation it estimates, with very reasonable accuracy, the message signal. The synchronization time can be predetermined for a set of design parameters and the effect of this in message recovery can be removed by transmitting the message only after this time period. It is important to note that the improved performance offered by this scheme compared to the proportional observer is due to the PI-observer that allows choosing the proportional and integral gains fairly independently. In effect, with the P-observer, the gain has to deal with the stability of the error dynamics as well as to reduce the effect of the message on the error dynamics. Hence there is too much constraints imposed on the sole proportional gain. On the other hand, with the PI-observer the integral gain is used to deal with the stability of the error dynamics while the proportional gain is used to reduce the effect of the message signal on the error dynamics.

Fig. 13 depicts the power spectral density of the recovered message at 10 Hz using P and PI observers.

The faithful recovery of the signal is evident by a low level of harmonic distortion (~50 dB). For PI-observer the output signal is marginally better than the P-observer.

Next we investigate the performance of the proposed hybrid method and PI-observer in a noisy channel. For this purpose a message signal m(t) = sin(t) is used. The chaotic carrier generated using Eq. (26) is passed through the additive white Gaussian noise (AWGN) channel having different signal-to-noise ratio (SNR) of 25, 20 and 15 dB. At the receiver, following synchronization using PI-observer given in Eq. (28), an 8^{th} order low pass Butterworth filter with a cut off frequency of 3 rad/sec is employed to reduce the noise power. To assess the synchronization behavior of a PI-observer with AWGN, we plot the state x_{1h} against the state of x_1, see Fig. 14. The perfect 45^0 line illustrates that full synchronization is still possible. This is because the integrator in the PI-observer generally tends to suppress the noise to a certain degree. Fig. 15 shows the recovered message signal for different values of SNR (i.e. 15, 20 and 25 dB). For SNR of 25 dB, there is a good match with input signal, whereas for lower values of SNR the recovered signal is rather distorted. In [19], for a practically viable chaotic cryptography scheme the recommended value of the SNR is 40 dB, whereas in [20] the value is increased to 70 dB well above what we have adopted in this work. Thus, the results presented in this paper demonstrate the potential of proposed chaotic scheme operating at relatively very low SNR. Further work is in progress to fully investigate the system performance for both analogue and digital communications.

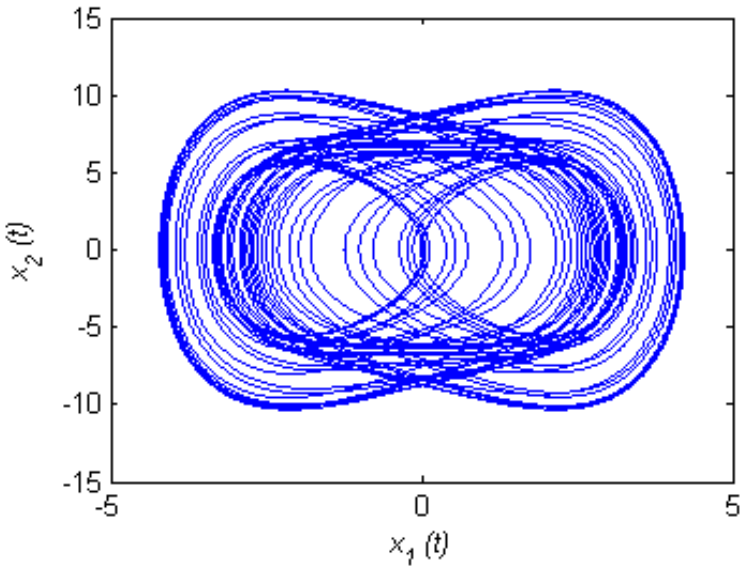


Fig. 11 Strange attractor with PI-observer.

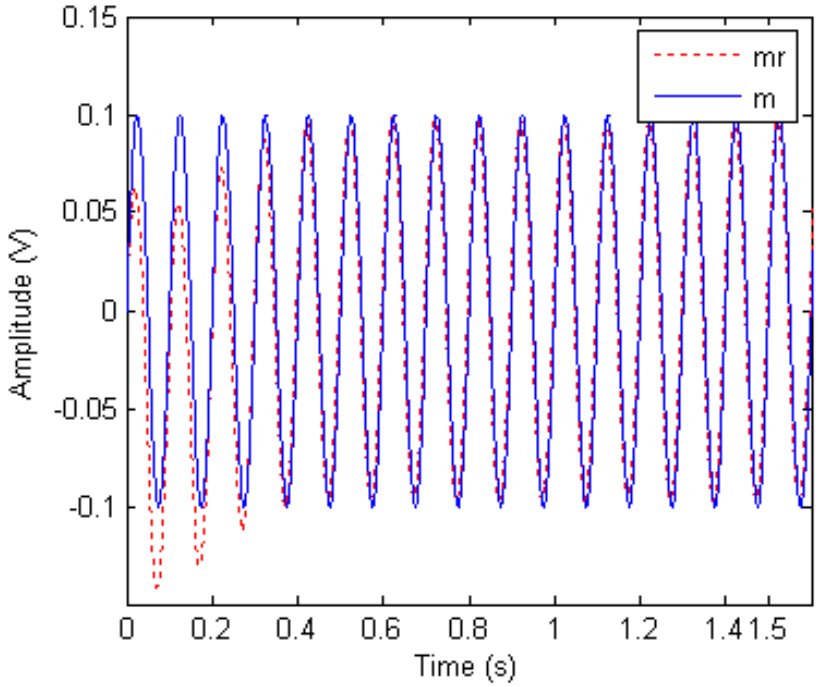


Fig. 12 Input and recovered message signals using PI-observer.

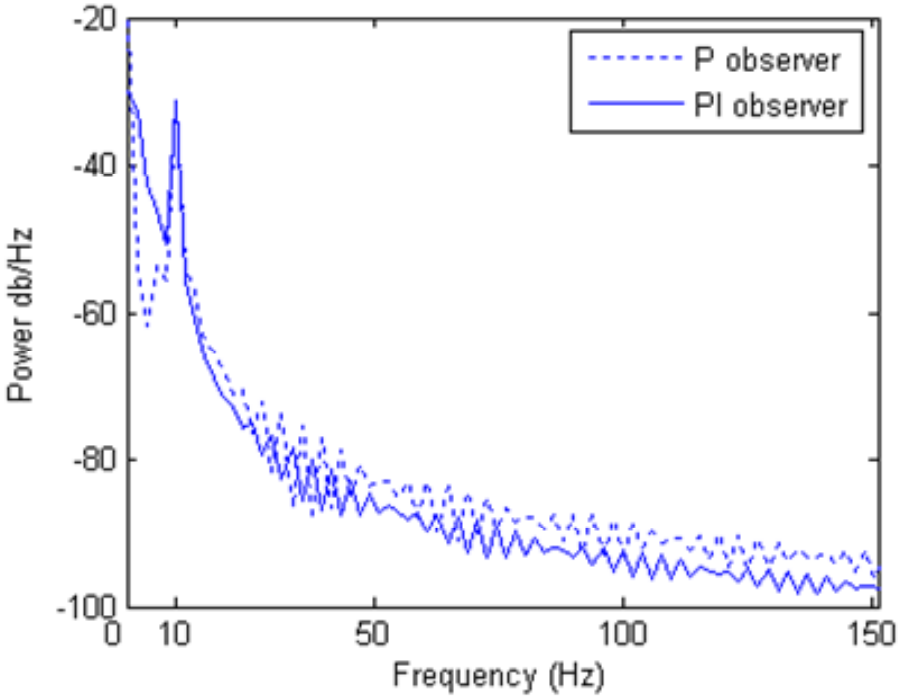


Fig. 13 Power spectral density of the recovered message for P and PI-observer.

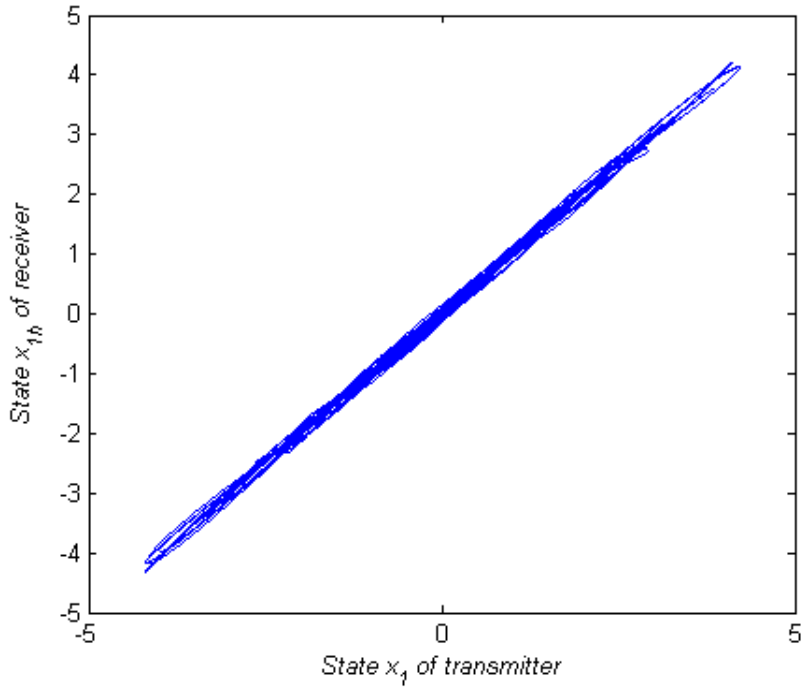


Fig. 14 Plot of states x_{1h} vs. x_1 of transmitter and receiver respectively for PI-observer in noisy channel (SNR=25 dB).

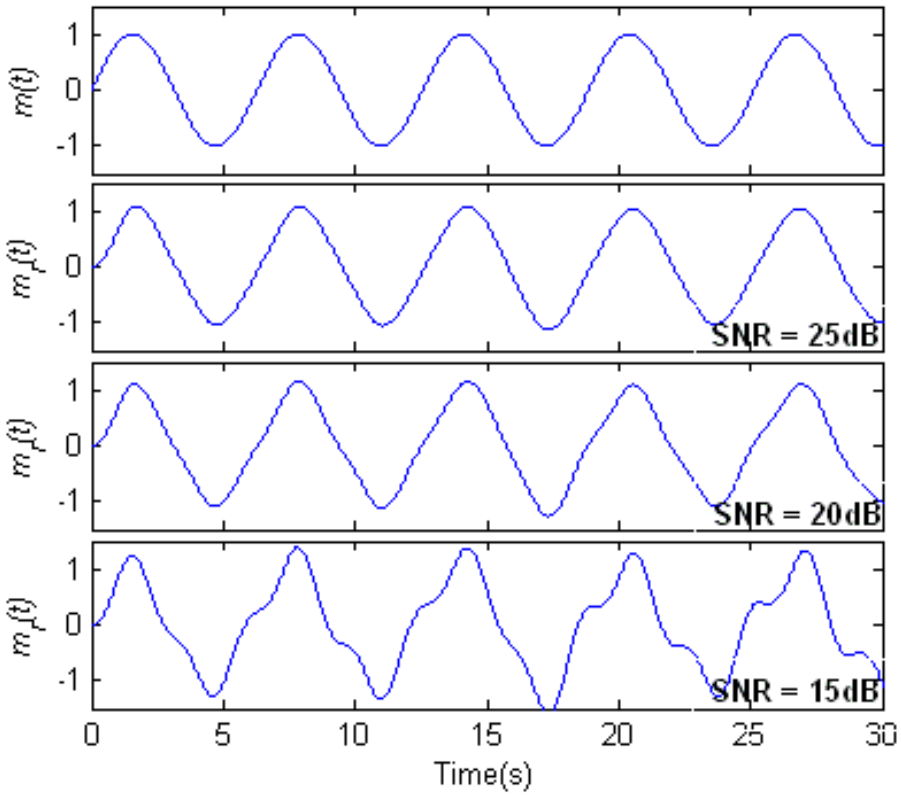


Fig. 15 Input and recovered message signals using PI-observer at different values of SNR.

4 Conclusions

In this paper we have proposed a new chaos-based communication scheme based on the observers. The main novelty lies in the masking method employed. It uses a combination of the addition and inclusion method to mask the message mainly to facilitate the recovery of the message signal. We have compared two observers employed as a receiver for the proposed communication scheme namely: the proportional observer (P-observer) and the proportional integral observer (PI-observer). We have shown that the P-observer is not suitable for the proposed communication scheme since it imposes unpractical constraints on the messages to be sent if the communication has to be kept secure. On the other hand, we have shown that the PI-observer is the best solution since it allows greater flexibility in choosing the gains of the observer and it does not impose any unpractical restriction on the message signal. This is mainly due to the fact that, with the PI-observer, the integral gain is used to deal with the stability of the error dynamics while the proportional gain is used to reduce the effect of the message on the error dynamics. Finally, it is also shown that the proposed scheme can perform with an SNR >= 25 dB, thus demonstrating its practically feasibility.

References

[1] Li S., Alvarez G., Li Z. and Halang W. A., "Analog Chaos-based Secure Communications and Cryptanalysis: A Brief Survey," *International IEEE Scientific Conference on Physics and Control (PhysCon)*, Potsdam, Germany, arXiv:0710.5455v1 [nlin.CD], 2007.

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

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

[4] Johnson P. and Busawon K., "Chaotic synchronisation for secure communication using PI-observers," *IFAC Conference on Analysis and Control of Chaotic Systems*, Reims, France, pp 205-210, 2006.

[5] Milanovic V. and Zaghloul M. E., "Improved masking algorithm for chaotic communication systems," *Electronics Letters*, Vol. 32, pp. 11-12, 1996.

[6] Yeh J. P. and Wu K. L., "A simple method to synchronize chaotic systems and its application to secure communications," *Mathematical & Computer Modelling*, Vol. 47, pp. 894-902, 2008.

[7] Parlitz U., "Transmission of digital signals by chaotic synchronization," *International Journal of Bifurcation and Chaos*, Vol. 2, pp. 973-977, 1992.

[8] Yang T. and Chua L. O., "Secure Communication via parameter modulation," *IEEE Transaction on Circuit and Systems-I: Fundamental Theory And Applications*, Vol. 43, pp. 817-819, 1996.

[9] Itoh M., Murakami H. and Chua L. O., "Communication systems via chaotic modulations," *IEICE Transaction Fundamentals*, Vol. E77-A, pp. 1000-1006, 1994.

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

[11] L'Hernault M., Barbot J. P. and Ouslimani A., "Sliding mode observer for a chaotic communication system: Experimental Results," *IFAC Conference on Analysis and Control of Chaotic Systems*, pp. 411-416, 2006.

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

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

[14] Huang X., Xu J., Huang W. and Lu Z., "Unmasking chaotic mask by a wavelet multiscale decomposition algorithm," *International Journal of Bifurcation and Chaos*, Vol. 11, pp. 561-569, 2001.

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

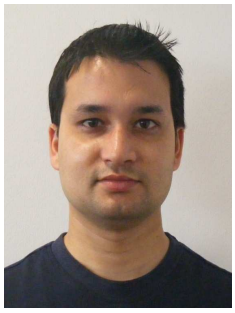
[16] Barbot J. P., *Observability bifurcations: applications to cryptography In: Chaos in Automatic Control,* Taylor and Francis, 2005.

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

[18] Busawon K. and Kabore P., "Disturbance attenuation using proportional integral observers," *International Journal of Control*, Vol. 74, pp. 618-627, 2001.

[19] Alvarez G. and Li S., "Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems," *International Journal of Bifurcation and Chaos*, Vol. 16, pp. 2129-2151, 2006.

[20] Cherrier E., Boutayeb M. and Ragot J., "Observers based synchronization and input recovery for a class of nonlinear chaotic models," *IEEE Transaction on Circuit and Systems*, Vol. 53, pp. 1-10, 2006.



Rupak Kharel received his Masters degree in Optoelectronic and Communication Systems from Northumbria University, Newcastle Upon Tyne, UK in 2007. He is currently working toward the Ph.D. degree in Electrical and Electronic Engineering, specializing in chaotic communication, at the same university. His research interests are in the field of nonlinear dynamical systems especially chaotic synchronization and its application to secure communication.

Dr. Krishna Busawon is a Reader in the School of Computing, Engineering and Information Sciences at Northumbria University. Before joining Northumbria University in the year 2000, he was a Lecturer in the Department of Mechanical and Electrical Engineering (FIME) at the University of Nuevo León, Mexico. He was also appointed as a Research Fellow at Simon Fraser University in 1997. Prior to that, Dr. Busawon did his Ph.D. research in Control Systems Engineering at the CNRS (Centre National de Recherches Scientifiques) research laboratory - LAGEP, (Laboratoire d'Automatique et de Génie des Procédés) at the University of Lyon, France. Dr. Busawon research interests are in nonlinear control systems theory in general, with principal interest in nonlinear observer design. He has applied his research to various industrial applications including power, bioprocesses and communication systems.

Professor Zabih Ghassemlooy, B.Sc. (Hons), M.Sc., Ph.D., C.Eng., Fellow of IET, Senior Member of IEEE, Received his B.Sc. (Hons) degree in Electrical and Electronics Engineering from the Manchester Metropolitan University in 1981, and his M.Sc. and Ph.D. in Optical Communications from the University of Manchester, Institute of Science and Technology (UMIST), in 1984 and 1987, respectively with Scholarships from the Engineering and Physical Science Research Council, UK. From 1986-87 he worked as a Demonstrator at UMIST and from 1987 to 1988 he was a Post-doctoral Research Fellow at the City University, London. In 1988 he joined Sheffield Hallam University as a Lecturer, becoming a Reader in 1995 and a Professor in Optical Communications in 1997. He was the Group Leader for Communication Engineering and Digital Signal Processing Subject Division, and also head of Optical Communications Research Group until 2004. In 2004 he moved to the University of Northumbria at Newcastle as an Associate Dean for Research in the School of Engineering and Technology. In 2005 he became Associate Dean for Research and Head of Northumbria Communications Research Laboratories in the School of Computing, Engineering and Information Sciences. In 2001 he was a recipient of the Tan Chin Tuan Fellowship in Engineering from the Nanyang Technological University in Singapore to work on the photonic technology. In 2006, he was awarded one of the best Ph.D. research supervisors at Northumbria University. He was a visiting professor at the Ankara University, Turkey and Hong-Kong Polytechnic University, and is currently a visiting Professor at the Technological University of Malaysia. He is the Editor-in-Chief of The Mediterranean Journals of Computers and Networks, and Electronics and Communications. He serves on the Editorial Committees of IEEE Communications Letters, International Journal of Communication Systems, and the EURASIP Journal of Wireless Communications and Networking, Contemporary Engineering Sciences, Research Letter in Signal Processing, and also has served on the Publication Committee of the IEEE Transactions on Consumer Electronics, the editorial board of the Inter and the Sensor Letters. He is the founder and the Chairman of the International Symposium on Communication Systems, Network and Digital Signal Processing, a committee member of the International Institute of Informatics and Systemics, and is a member of technical committee of a number of international conferences. He is a College Member of the Engineering, and Physical Science Research Council, UK (2003-2009), and has served on a number of international Research and Advisory Committees. His research interests are in the areas of photonic networks, modulation techniques, high-speed optical systems, and optical wireless communications. He has received a number of research grants from UK Research Councils, European Union, Industry and UK Government. He has supervised more 27 Ph.D. students and has published over 300 papers. He is a co-editor of an IET book on "Analogue Optical Fibre Communications", the proceedings of the CSNDSP '08', '06, CSDSP'98, and the 1st Intern. Workshop on Materials for Optoelectronics 1995, UK. He is the co-guest editor of a number of special issues: the IET Proceeding Circuit, Devices and Systems, Feb. 2008 and August 2006, the Mediterranean J. of Electronics and Communications on "Free Space Optics–RF", July 2006, the IET Proceeding J. 1994, and 2000, and Inter. J. Communications Systems 2000. From 2004-06 he was the IEEE UK/IR Communications Chapter Secretary, and currently is the Vice-Chairman. He is also Vice-Chairman of IET Northumbria Branch, UK..