An Observer Based Spread Spectrum Method for Chaotic High Secure Communications

Reza Raoufi[i], and M. B. Menhaj[ii]

ABSTRACT

This paper presents an innovative technique on the application of chaotic systems for secure communication. The inherent defect of shortage of chaotic bandwidths has been remedied by employing spread spectrum nonlinear functions and the information signal is masked with chaos based spread spectrum signal with high security. The designing state observer along with nonlinear output feedback control is the basis of the receiver structure. Lyapunov stability theory guarantees the synchronization of slave system with the master chaos driver. Meanwhile, duo to noisy communication channel, a stochastic ITO model for master system is supposed to design the state observer. The receiver extracts the information signal using the transmitted signal and the outputs of the observer. The results of numerical simulations based on the Chua circuit fully elaborate the proposed method.

KEYWORDS

The author shall provide up to 10 keywords to help identify the major topics of the paper.

1. INTRODUCTION

There have been significant interests in using chaotic dynamics to realize secure communications. There are several features in chaotic signal that make them so attractive in communication systems. Chaotic dynamics with their noise-like broadband power spectra is a good candidate to remedy narrow-band effects such as frequency-selective fading or narrow-band disturbances in communication systems. Another attractive feature of chaotic signals is their dependence on initial conditions; this in turn makes it more difficult to guess the structure of the chaotic signal generator and to predict the signal over a longer time interval. Furthermore, even infinitesimal changes in the initial conditions will lead to an exponential divergence of orbits. This feature is very interesting in cryptography, where highly complex and hard-to-predict signals are employed. Chaotic signals are deterministic in nature meaning that there is no random component in their corresponding differential equations, although their trajectories are noise-like and bounded.

Moreover, chaotic signals are aperiodic in the sense that no state ever repeats itself. Chaotic output streams will be completely uncorrelated, and the auto-correlation of a chaotic signal has a large peak at zero and decays rapidly. Thus, a chaotic system shares many properties of a stochastic process, which are the basic requirements of the spread spectrum communications. Most of the work in this area has been focused on synchronization of chaotic systems to recover the information signals [1-12]. In a typical chaotic synchronization communication scheme the information to be transmitted is carried from the transmitter to the receiver by a chaotic signal through an analog channel. The decoding of the information signal in the receiver can be carried out by means of either coherent (synchronization) or non-coherent (without synchronization) decoders [6, 7].

On the other hand, recent investigations have linked observer-based concepts to chaos synchronization, which constructs all of the state information merely from the transmitted signal [8], [13-15]. A systematic approach, which is employing a nonlinear state observer, is proposed to resolve chaotic synchronization of a class of hyper chaotic systems via a scalar transmitted signal. In most previous work in this area, there are some deficiencies and limitations like: 1) observer-based chaotic synchronization in the presence of noise in the chaos generator or transmitted signal, 2) chaotic synchronization via observer design which cannot be applied to secure

i Master student, Department of Applied Mathematics , The University of Sheffield, Sheffield S10 2TN, UK, R.Raoufi@shef.ac.uk

ii Full Professor, EE Departmentm Amirkabir University, menhaj@aut.ac.ir

communications, and finally 3) the most important is the disability of the conventional observer based synchronization for nonlinear chaos-based spread spectrum signals. It should be emphasized that although chaos is broad band, its bandwidth is not good enough for secure spread spectrum communications. Therefore, chaos-based spread spectrum techniques such as frequency hopping (FH) and direct sequence (DS) are very promising and reasonable to promote the security features of chaotic modulations. It should be noted that a pseudorandom sequence generator used in FH and DS is considered to be a special case of a chaotic system. The principal difference is that the chaotic system has an infinite number of states, while the pseudorandom generator has a finite number of states. Furthermore, the inherent periodicity of pseudorandom sequence compromises the overall security while a chaotic generator can visit an infinite number of states in a deterministic manner and therefore, it produces an output sequence which never repeats itself. So, recently, there has been much more interest in utilizing chaotic signals for spread spectrum communications. It should be pointed out that the larger the length of chaos–based random sequence is, the higher will be the security level. However, the major problem is the design of a nonlinear observer for synchronization and estimation of a noisy spread-spectrum chaotic based signal which indeed represents a much more spread and noise-like signal [16],[22].

For transmission of information by chaotic signals, many ways have been tried. The most important ones can be categorized as: chaotic masking (CM), chaos shift keying (CSK), chaos parameter modulation, chaos on-off keying (COOK) and predictive Poincare control modulation. The basic ideas of these chaotic cryptosystems are based upon using a chaotic non-linear oscillator as a broadband pseudo random signal generator. This signal is combined with the carrying message, to produce an unrecognizable signal transmitted through the insecure communication channel. At the receiver, the chaotic pseudo-random signal is regenerated so that by combining it with the received signal through the inverse operation, the original message is recovered [17-19], [21].

In chaotic masking, the chaotic signal is added to the information signal and at the receiver the masking is removed. In order for this scheme to properly work, the receiver must synchronize robustly enough as to admit the small perturbation in the driving signal due to the addition of the message. The power level of the information signal must be much lower than that of the chaotic signal in order to be buried effectively [18]. Knowing that chaos is spread to some extent and considering the fact that all chaotic and hyper-chaos generators have base-band frequency behavior, we should impose a limitation to the frequency of base-band modulated data. It is clear that this inherent chaos feature will make any chaotic secure system effective and satisfactory only for low speed modulations by guaranteeing the frequency domain security. In addition, it is possible to attack a chaotic secure system via suitable return maps when the secure system dose not employ the spread spectrum mappings for transmitted scalar signals [20].

In this paper, we design a stochastic observer-based synchronization for noisy spread spectrum chaotic signals that have extremely broadband and noise-like behavior. To do so, we propose a new method of synchronization to access a high secure communication system via the CM technique. The proposed method has high security characteristics with respect to both time and frequency domains; this makes the method very attractive. Finally, the proposed approach remedies the defectiveness of low speed data modulations.

This paper is organized as follows. Section 2 presents the problem formulation and chaos-based spread spectrum techniques an n-shift ciphering algorithm. Spread-spectrum chaotic synchronization via a nonlinear state observer design will be covered in section 3. Section 4 presents high secure spread spectrum chaotic communication systems based on nonlinear state observer design in presence of channel and measurement noise. Section 5 is devoted to show the capability of proposed method by presenting an illustrative example for a secure chaotic communication in the presence of spread spectrum mapping, including the Chua circuit for analog data. Finally, section 6 concludes the paper.

The following notation will be used in the paper. $x \in R^n$ denotes an n-vector with real elements with the associated norm $\|x\| \equiv \left(x^T x\right)^{1/2}$, R^+ is the set of nonnegative real umbers. $\lambda_{\min}(A)$ $\left(\lambda_{\max}(A)\right)$ denotes the minimum (maximum) eigenvalue of a symmetric matrix. $A (A \in R^{n\times m})$ The symbol e is used for the exponential function and $E\{.\}$ denotes the expectation value.

2. CHAOS-BASED SPREAD SPECTRUM TECHNIQUES

Consider the following continuous-time chaotic dynamical system model with linear measurement.

$$\begin{cases} \dot{x} = Ax + f(x,t) \\ y = Cx \\ z = h(y) \end{cases} \qquad (1)$$

In the above, $x \in R^n$ denotes the state vector of chaotic attractor, $y \in R$ represents the system linear output measurement, A and C are constant matrices with appropriate dimensions. The pair (A,C) is assumed to be detectable and h represents a nonlinear smooth coding function which makes the output much more spread in frequency domain in order to enhance severely the complexity of $y(t)$. It should be pointed out that the function h plays a vital role in the decoding process and

will be discussed in the next subsection. Furthermore, it is assumed that f is a real analytic vector field on R^n. The system (1) has a unique solution $x(t)$ well defined over R^+. Moreover, $Ax+f(x,t)$ maps the state $x(t)$ chaotically while $f(x,t)$ satisfies the Lipschitz condition with a positive Lipschitz constant γ for $x_1,x_2 \in R^n$ and for all $y \in R$ such that

$$\|f_1(x_1,t)-f_1(x_2,t)\| \le \gamma \|x_1-x_2\| \quad ; \forall x_1,x_2 \in R^n \tag{2}$$

A. Spread Spectrum Mapping Function

A substantial problem in employing chaotic sequences as a secure encrypter signal is their bandwidth. Although the majority of chaotic dynamics have a wider bandwidth in comparison with a sinusoidal wave, they are not spread from the secure communication features point of view. Indeed, in this paper we use chaotic signals to generate a completely broadband noise-like signal via a nonlinear smooth coding function, h. Some suitable and yet efficient functionals have been introduced for h such as: Chaos-based direct sequence (CDS) and chaos-based frequency hopping (CFH) [16], [22]. It should be noted that the chaos-based FH spread spectrum hops to any frequency in the available band according to the chaotic signal $y(t)$. The CDS and the CFH mapping functions can be respectively described as follows

$$z=h(y)=y^r=(Cx)^r,(r>1:integer) \tag{3}$$

$$z=h(y)=\sin(2\pi q y(t)t),(0<q<1) \tag{4}$$

Furthermore, to achieve an extremely complex secure chaotic coding signal with respect to the above techniques, the CDS and CFH are both employed simultaneously; this in turn has an impressive impact on the frequency spectral density. Therefore, the synthetic chaos-based DS-FH spread spectrum coding function can be given by

$$z=h(y)=\sin(2\pi q(y(t))^r t) \quad ,(0<q<1,r>1:integer) \tag{5}$$

B. Multishift Cipher with Application to Secure Communication

The other method frequently used as a weak spread spectrum encrypter is the n-shift cipher algorithm. It should be noted that although this algorithm is strong enough for encryption in time domain, it can spread the chaos frequency response more restricted and weaker than the CDS or CFH techniques. This multi-shift cipher works with a chaotic cryptosystem shown in Fig.1. In this figure, the encrypter consists of a chaotic system and an encryption function $e(.)$. The key signal $k(t)$ is one of the state variables of the chaotic system. Another state variable $s(t)$ is transmitted through a public channel to the decrypter and used to synchronize the decrypter. $y(t)$ is the encrypted signal which is fed back into the chaotic system. The decrypter consists of a chaotic system and a decryption function $d(.)$. The decrypter is to find the key signal when the decrypter and the encrypter are synchronized. The encrypted signal is also recovered via synchronization. The function $d(.)$ is used to decrypt the encrypted signal. It should be noted that in the scheme shown in Fig.1, both the key signal and the encrypted signal $y(t)$ are not transmitted to the decrypter. This is different from the traditional discrete cryptosystem where both the key and the encrypted signal are transmitted to the decrypter.In figure 1, $p(t)$ denotes the data (plain text) signal, $e(p(t))$ is the encrypted signal and $\tilde{e}(p(t))$ is the recovered signal that can be done when the synchronization is achieved. We use an n-shift cipher to encrypt the plain signal. The n-shift cipher is defined by

$$\begin{aligned} e(p(t)) &= \underbrace{f_1(..f_1(f_1}_{n}(p(t),\underbrace{k(t)),k(t)),....,k(t))}_{n} \\ &= y(t) \end{aligned} \tag{6}$$

Where h is chosen such that $p(t)$ and $k(t)$ lie within $(-h,h)$ and $f_1(*,*)$ is the following nonlinear function

$$f_1(x,k)=\begin{cases}(x+k)+2h & ,2h \le (x+k) \le -h \\ (x+k) & ,(x+k)<h \\ (x+k)-2h & ,h \le (x+k) \le 2h\end{cases} \tag{7}$$

This function is shown in Fig.2. The corresponding decryption rule is the same as the encryption rule

$$\begin{aligned} p(t) &= d(y(t))=e(y(t)) \\ &= \underbrace{f_1(..f_1(f_1}_{n}(y(t),\underbrace{-\tilde{k}(t)),-\tilde{k}(t)),....,-\tilde{k}(t))}_{n} \end{aligned} \tag{8}$$

Where $\tilde{k}(t)$ is recovered in the receiver circuit and should approximate $k(t)$. In the n-shift cipher, the key signal is used n times to encrypt the plain signal. Since the encrypted signal is a function of $k(t)$ and $p(t)$, and since the encrypted signal is used to derive the circuit, it hides both the dynamical and the statistical characteristic of both $k(t)$ and $p(t)$ [23].

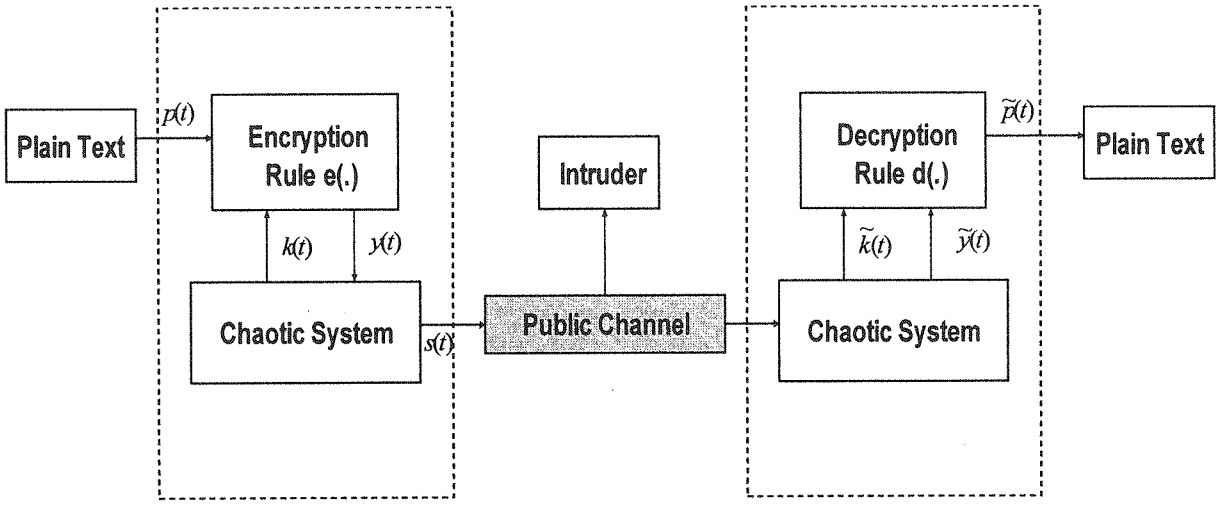

Figure 1: Block diagram of the chaotic cryptosystem

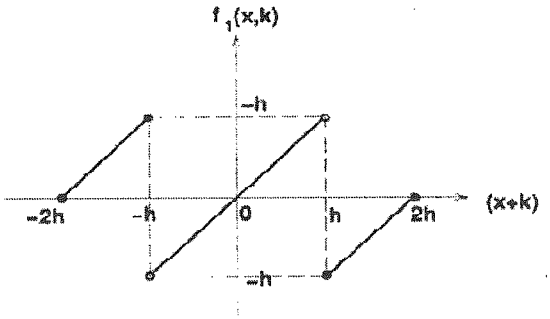

Figure 2: Nonlinear function used in continuous shift cipher

3. Observer Based Synchronization For Chaotic Spread Spectrum Systems

The receiver design for chaotic communications is a very sensitive and impressive task. Some receivers have been proposed based on Synchronization or non-coherent detection (without synchronization). The theoretical performance of chaotic communication receivers via non-coherent approach has been described in [6]. It should be noted that if synchronization can be maintained and proved theoretically from the stability point of view, it will have more potential advantage in recovery of chaotic basis functions in comparison with non-coherent detection. The chaotic synchronization techniques cited up to now are not suitable for a chaos based spread spectrum transmitted signal possessing a very noise-like and wideband characteristic. In most observer based synchronization techniques, the transmitted chaotic signals represent one state of chaos. In this paper, a new synchronization method is presented for nonlinear spread spectrum signals whose bandwidth is wide leading to a more complex behavior (high variations through times). The theoretical foundation of proposed technique is proved.

Consider the following continuous-time chaotic model wit a spread spectrum nonlinear output signal from the linear measurement. The system has a control signal in its state space model which will be employed to guarantee the stability analysis. With some modifications on the model given in (1), the following model is proposed.

$$\begin{cases} \dot{x} = Ax + f(x,t) + u(t) \\ y = cx \\ z = y + h(y) \end{cases} \tag{9}$$

where $u \in R^n$ and all other variables have the same definition described in section 2. Figure 3 illustrates the proposed synchronization scheme for the above chaotic model consisting of chaotic transmitter, spread spectrum mapping function and an observer based synchronizer in the receiver section. The transmitter is the chaotic system described by (9) and the following state estimator is employed for the receiver section.

$$\begin{cases} \dot{\hat{x}} = A\hat{x} + f(\hat{x},t) + L(z - \hat{y}) \\ \hat{y} = c\hat{x} \\ \hat{z} = \hat{y} + h(\hat{y}) \end{cases} \tag{10}$$

To investigate the convergence property of this observer, the observation error is defined as $e(t) = x(t) - \hat{x}(t)$ whose dynamic is found from (9), (10) as

$$\dot{e} = Ae + f_1(x,t) - f_1(\hat{x},t) - L(z - \hat{y}) + u(t) \tag{11}$$

It should be noted that since $A - LC$ is stable, then for any positive definite $(Q = Q^T) \in R^{n \times n}$ there exists a unique positive definite $P \in R^{n \times n}$ such that

$$(A - LC)^T P + P(A - LC) = -2Q,\ P = P^T \tag{12}$$

To investigate the stability of the system, we consider the following positive definite Lyapunov function candidate

$$V(e,t) = e^T Pe \tag{13}$$

The derivative of $V(e,t)$ evaluated along the solution of the error differential equation (11) is calculated as:

$$\dot{V}(e,t) = 2e^T P\dot{e}$$
$$= 2e^T P(Ae + f_1(x,t) - f_1(\hat{x},t) - L(z - \hat{y}) + u(t))$$
$$= 2e^T P(Ae + f_1(x,t) - f_1(\hat{x},t) - L(y + h(y) - \hat{y}) + u(t))$$
$$= -2e^T Qe + 2e^T P(f_1(x,t) - f_1(\hat{x},t)) + 2e^T P(u(t) - Lh(y))$$

Using the Lipschitz condition (2) along with (12), we will have

$$\dot{V}(e,t) \le -2\lambda_{\min}(Q)\|e\|^2 + 2\gamma\lambda_{\max}(P)\|e\|^2 + 2e^T P(u(t) - Lh(y))$$
$$= -2\|e\|^2(\lambda_{\min}(Q) - \gamma\lambda_{\max}(P)) + 2e^T P(u(t) - Lh(y))$$

It should be pointed out the above result is derived from the following fact.

$$M > 0 \rightarrow \lambda_{\min}(M)\|z\|^2 \le z^T Mz \le \lambda_{\max}(M)\|z\|^2$$

Therefore, if the offline design satisfies the following assumption

$$\frac{\lambda_{\min}(Q)}{\lambda_{\max}(P)} > \gamma \tag{14}$$

and by selecting the control signal as

$$u(t) = Lh(y(t)) \tag{15}$$

then $\dot{V}$ is semi- negative definite. This means that $V(t) \le V(0)$ or $e(t)$ is bounded in time. Also, since V is non-increasing and bounded, the state estimator will remain uniformly bounded and is convergent. So if (14) holds, finally $e(t) \rightarrow 0$ as time goes to infinity.

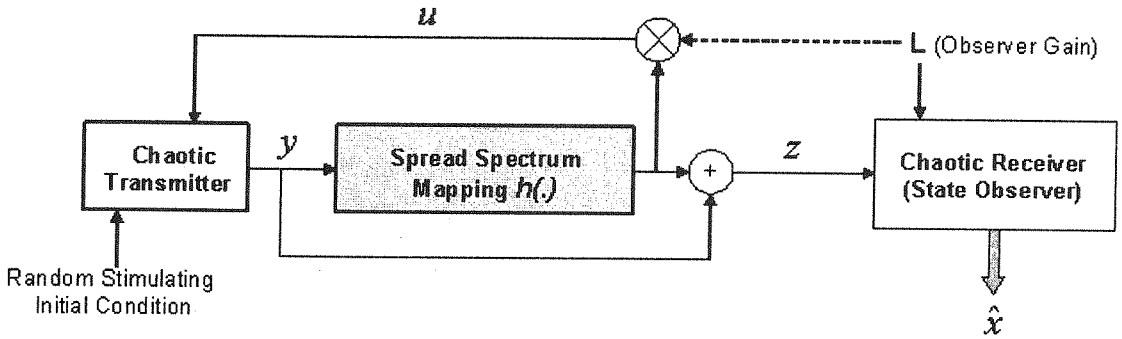

Figure 3: The proposed synchronization scheme for chaos based spread spectrum system

4. Chaos-Based Spread Spectrum Secure Communication via Observer Design For Stochastic Model

In this section, we propose a high secure communication system based on designing an appropriate observer. The proposed chaotic communication scheme basically recovers either analog or digital messages using a stochastic state estimator. It should be emphasized that we will design a robust observer owing to the Gaussian noise contaminated channel. This design mechanism via spread spectrum chaos based mappings can actually and fascinatingly make the communication system more secure because the encrypter signal with random initial conditions of the drive chaotic systems along with the complex spread spectrum functions is totally and amazingly noise-like and broadband. Meanwhile, the feedback law which is dependent on the message signal can change the chaos drive system behavior dramatically. Furthermore, considering the presence of noise in communication channel we model the chaotic drive system as stochastic state model by the Ito differential equations and we will design an observer at the receiver section. Let us consider the chaos model using Ito differential equation

$$\begin{cases} dx_t = (Ax_t + f(x_t,t))dt + u_t dt \\ dy_t = Cx_t dt \\ dz_t = (y_t + h(y_t) + s_t)dt + g(x_t)d\zeta_t \end{cases} \tag{16}$$

Where $x \in R^n, y \in R, z \in R$ are respectively the chaos states , system linear output measurement and the masking of spread spectrum chaos based signal with data in presence of noise signal. $s_t \in R$ is the unknown message signal and $u_t \in R^n$ is the control signal . Furthermore, $f: R^+ \times R^n \rightarrow R^n$ is a nonlinear Lipschitz function with the property

$$\|f(x_{t_2},t) - f(x_{t_1},t)\| \le \alpha_f \|x_{t_2} - x_{t_1}\| \tag{17}$$

and $h: R^+ \times R \rightarrow R$ represents a nonlinear smooth coding function which makes the output much more spread in frequency domain. $g: R^+ \times R \rightarrow R$ is the noise intensity function bounded by:

$$\|g(x_t)\| \le \alpha_g < \infty \tag{18}$$

and $\zeta_t \in R$ is the standard Wiener process noise independent of x_0. Meanwhile, A and C are constant

matrices with appropriate dimensions. The pair (A,C) is assumed to be detectable so that there exits a gain $L \in R^{n\times 1}$ which causes $A_0 = A - LC$ strictly Hurwitz.

We propose the following state estimator for the above stochastic chaos model

$$d\hat{x}_t = (A_0\hat{x}_t + f(\hat{x}_t,t))dt + Ldz_t \tag{19}$$

By defining the estimation error as $e_t = x_t - \hat{x}_t$ and using equations (16) and (19), we may have the dynamics of the estimation error as:

$$\begin{aligned} de_t = Ae_t dt + (f(x_t,t) - f(\hat{x}_t,t))dt \\ + u_t dt - Ldz_t \end{aligned} \tag{20}$$

Considering the signal z_t, we obtain

$$\begin{aligned} de_t = A_0 e_t dt + (f(x_t,t) - f(\hat{x}_t,t))dt \\ + (u_t - L(h(y_t) + s_t))dt - Lgd\zeta_t \end{aligned} \tag{21}$$

To analyze the above stochastic differential equation via Martingale-like approach [24], [26], we employ the commonly used Lyapunov candidate as $V(e_t) = e_t^T Pe_t$ where P is the solution to the Lyapunov equation $A_0^T P + PA_0 = -2Q$, and the differential operator $\bar{L}$ is defined [26] as

$$\begin{aligned} \bar{L}V(e_t) = 2\left[A_0 e + (f(x_t,t) - f(\hat{x}_t,t))\right]^T Pe_t \\ + 2(u_t - L(h(y_t) + s_t))^T Pe_t \\ + trace[GG^T P] \end{aligned} \tag{22}$$

where

$$G = -Lg$$

We use the inequalities (17), (18) along with (22) to obtain the following inequality

$$\begin{aligned} \bar{L}V(e_t) \le -2e_t^T Qe_t + 2\bar{\lambda}(P)\|e_t\|^2 \\ + 2(u_t - L(h(y_t) + s_t))^T Pe \\ + \alpha_g{}^2 \bar{\lambda}(L^T PL) \Rightarrow \\ \bar{L}V(e_t) \le -2(\underline{\lambda}(Q) - \bar{\lambda}(P))\|e_t\|^2 \\ + 2(u_t - L(h(y_t) + s_t))^T Pe \\ + \alpha_g{}^2 \bar{\lambda}(L^T PL) \end{aligned} \tag{23}$$

If the output feedback control signal is defined as

$$u_t = L(h(y_t) + s_t)$$

then the equation (23) becomes

$$\bar{L}V(e_t) \le -\tau_2\|e_t\|^2 + \tau_1$$

If we design in such a way that satisfies $\tau_1, \tau_2 > 0$ and using the Theorem 1 in [25] the following exponential bound is obtained

$$E_{e_0}\{V(e_t)\} \le V(e_0)e^{-\tau_2 t} + \tau_1\tau_2^{-1}(1 - e^{-\tau_2 t}), t \in R^+$$

Considering that $\underline{\lambda}(P)\|e_t\|^2 \le V(e_t) \le \bar{\lambda}(P)\|e_t\|^2$ we obtain

$$\begin{aligned} E_{e_0}\{\|e_t\|^2\} \le \underline{\lambda}^{-1}(P)\bar{\lambda}(P)\|e_0\|^2 e^{-\tau_2 t} \\ + \underline{\lambda}^{-1}(P)\tau_1\tau_2^{-1}(1 - e^{-\tau_2 t}), t \in R^+ \end{aligned}$$

Therefore, the above inequality guarantees the mean-square error to reach its steady state bounded by

$$\limsup_{t\to\infty} E\{\|e_t\|^2\} \le \frac{\tau_1}{\underline{\lambda}(P)\tau_2}$$

5. Example and Simulation Results

A. Chua Circuit Based Spread Spectrum Secure Communication

In this example we will show the application of the Chua circuit [27] for secure communication. Chua circuit is consisted of a nonlinear diode and four linear elements. This chaotic system is stimulated with random initial conditions along with a spread spectrum mapping function. The Chua system in presence of control signal can be given by the following equations

$$\dot{x}(t) = \begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\mu \end{bmatrix} x(t) + \begin{bmatrix} -\alpha f(x_1) \\ 0 \\ 0 \end{bmatrix} + u(t)$$

along with the linear measurement output is given by

$$y(t) = x_1(t)$$

where the nonlinear resistor in Chua circuit is modeled by

$$f(y) = \alpha x_1 + 0.5(G_a - G_b)(|y+1| - |y-1|)$$

To satisfy the design procedure proposed in section 2 and 3, we can employ the spread spectrum mapping function $h(y)$ and the transmitted chaotic signal $z(t)$ respectively as

$$h(y) = \cos(y^3 t)$$
$$z(t) = y(t) + h(y(t)) + s(t) + n(t)$$

Where $s(t)$ is the information signal defined as

$$s(t) = A\sin(2\pi ft), f = .2, A = 2$$

and $n(t)$ is the Gaussian white noise with the variance of 0.05. Regarding the procedure described in previous section, we pick the Q, P matrixes as

$$Q = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, P = \begin{bmatrix} 0.5666 & 0.5200 & -0.9237 \\ 0.5200 & 0.6860 & 0.0300 \\ -0.9237 & 0.0300 & 10.9971 \end{bmatrix}$$

The above solution for Lyapunov equation is derived with the observer gain as

$$L = [0.2 \quad 0.7 \quad 0.001]^T$$

Meanwhile, the parameter set of the Chua system is

β=15.5811 μ=0.003 α=8.29953 G_a=-1.886 G_b=-0.6590

Ultimately, figure 4 shows the chaos attractor orbits.

The chaos states and their estimates are depicted in figure 5. Figures 6 and 7 illustrate the bandwidth of measured Chua system output $y(t)$ and the Chua based spread spectrum signal $h(y(t))$ which is remarkably spread compared with $y(t)$; this in turn guarantees high security. The transmitted noisy chaotic signal $z(t)$ masked the information signal is shown in figure 8. Finally, the actual data and its decryption are depicted in figure 9. The accuracy of the recovered data is patent in this figure.

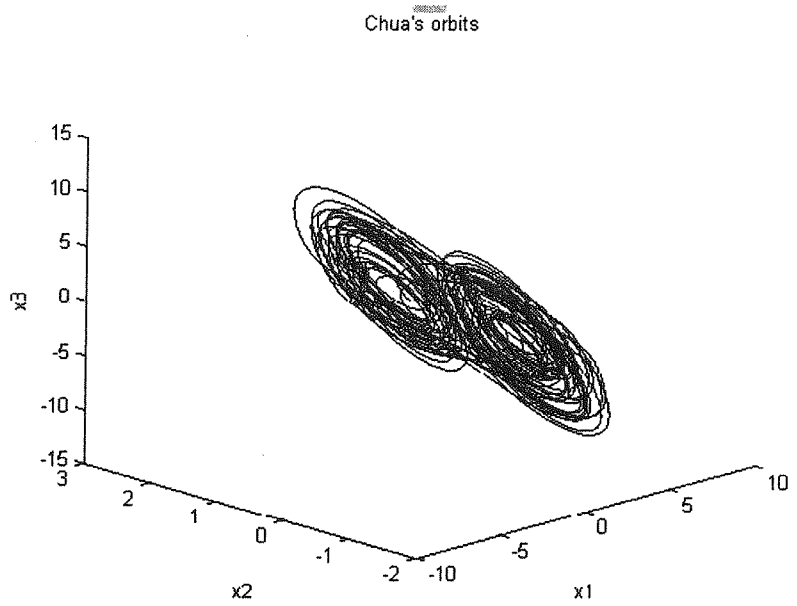

Figure 4: Chua system chaotic orbits

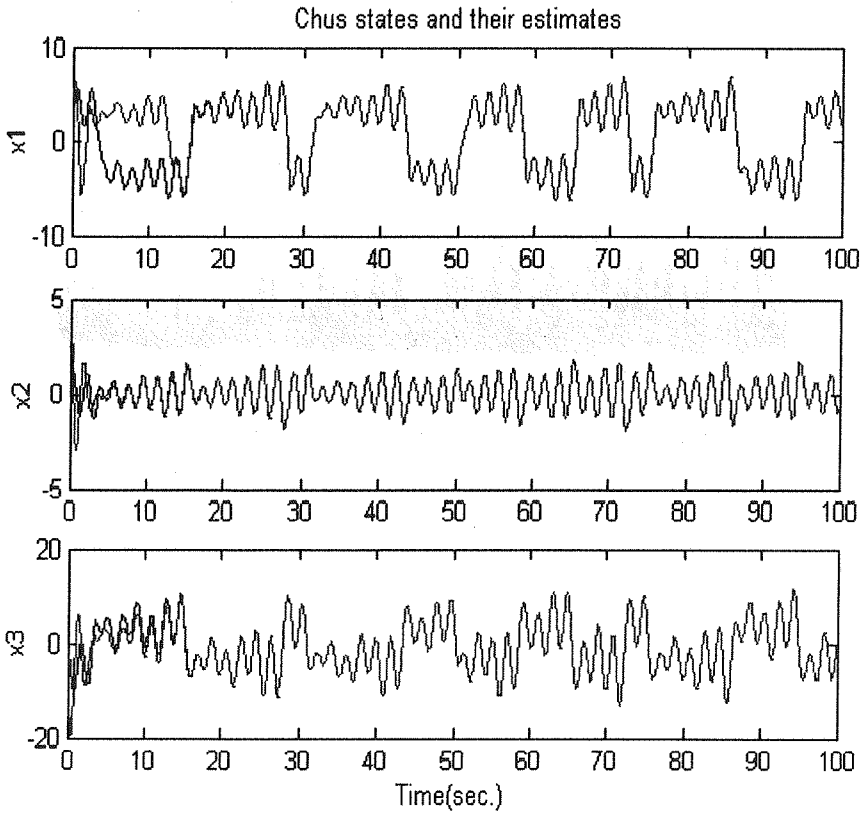

Figure 5: Chua states (black) and their estimates(red)

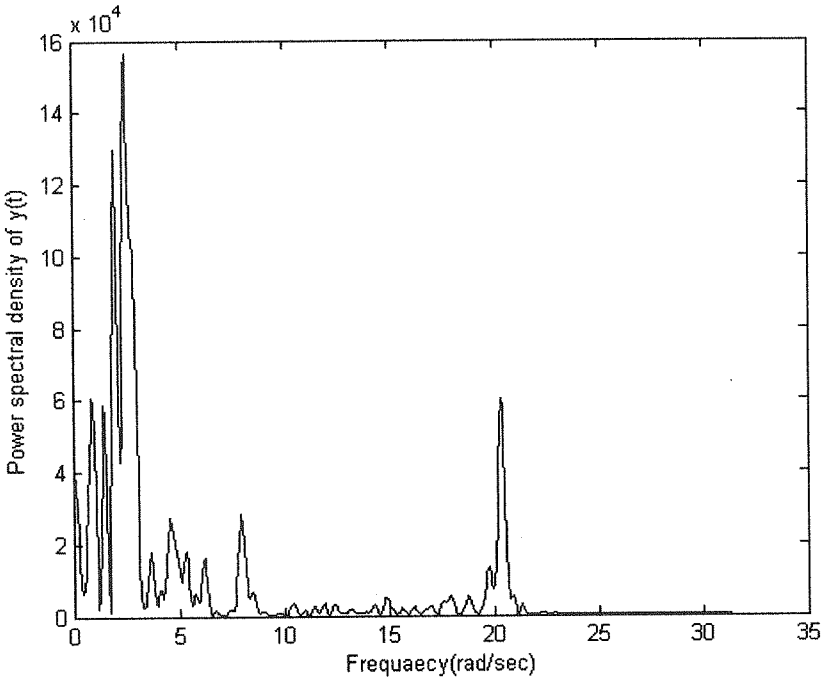

Figure 6: Frequency bandwidth of the signal y(t)

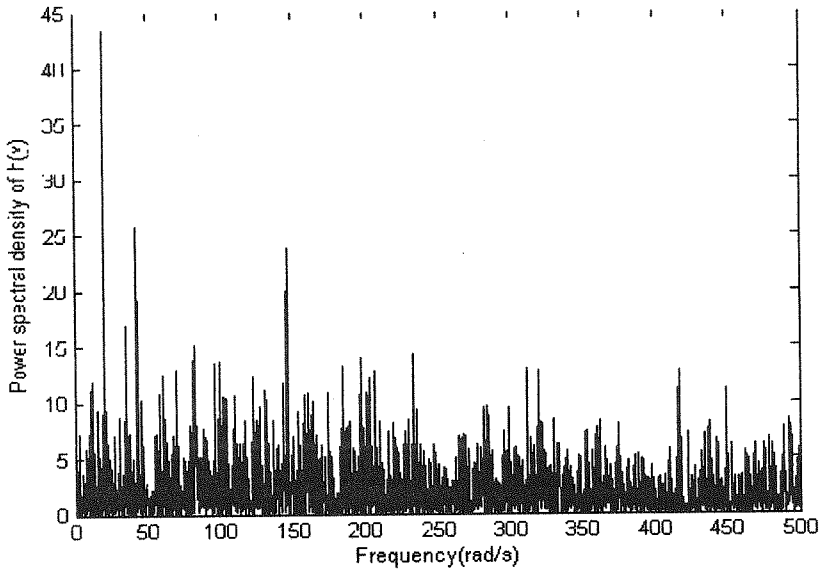

Figure 7: Bandwidth of chaos based spread spectrum function

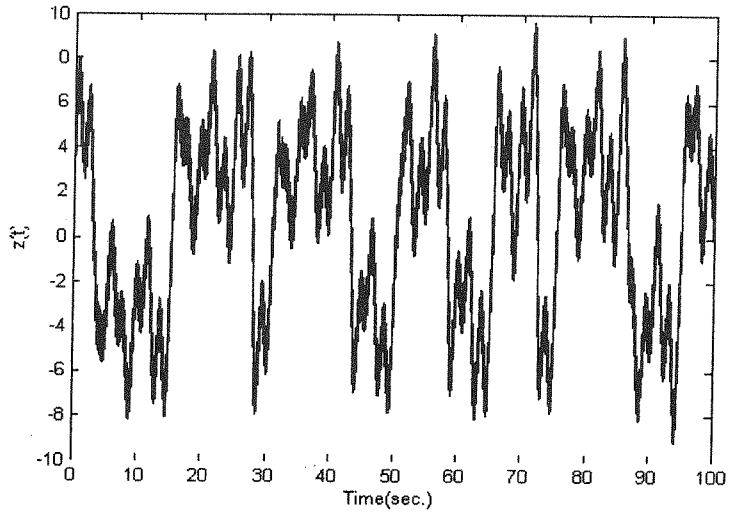

Figure 8: Transmitted secure signal thorough the insecure channel

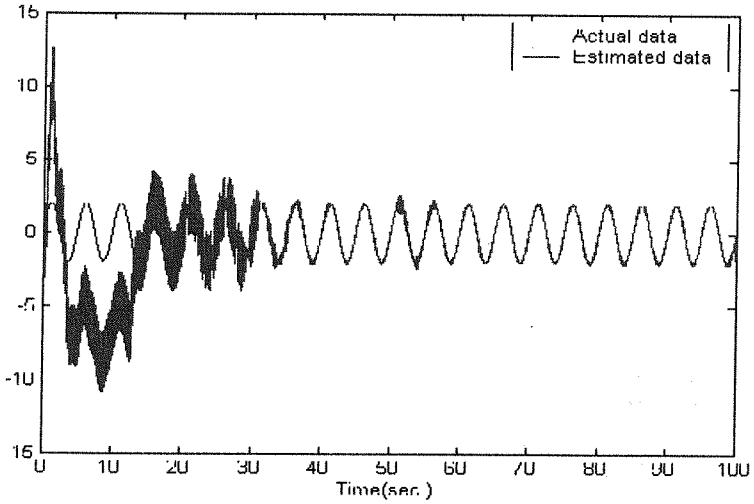

Figure 9: Actual data and its estimate

6. CONCLUSION

In this paper a new chaos based spread spectrum secure communication scheme has been presented. We have used spread spectrum mapping functions to expand the chaos bandwidth. The basic structure of the receiver section is consisted of an observer with feedback control for stochastic model of the sender chaotic section. We have used Lyapunov stability theory to complete the proof of synchronization. The impressive effect of chaotic signal as the input of the spread spectrum mapping functions is in turn really remarkable.

7. REFERENCES

[1] L.M. Peccora, T.L. Carroll, "Synchronization in Chaotic Systems," Phys. Rev. Lett., vol.64, pp. 821-824, Feb. 1990.

[2] L. Kocarev, K.S. Halle, K. Eckert and L.O. Chua, "Experimental demonstration of secure communication via chaotic synchronization," Int.J.Bifurcation & Chaos, vol. 2, pp. 709- 713, 1992.

[3] Tao Yang and L.O. Chua, L.O, "Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication," Circuits, and Systems I: Fundamental Theory and Applications. vol. 44, pp. 976- 988, Oct. 1997.

[4] M. Hasler and Y. Maistrenko, "An Introduction to the Synchronization of Chaotic Systems: Coupled Skew Tent Maps," IEEE Trans. Circuits and Sys., vol 44, pp. 856-866, Oct. 1997.

[5] H. Nijmeijer, and I.M.Y. Mareels, "An observer looks at synchronization," Circuits and Systems I: Fundamental Theory and Applications, vol. 44, pp. 882-890, Oct. 1997

[6] G. Kolumban, M. P. Kennedy and L. Chua, "The Role of Synchronization in Digital Communications Using Chaos-Part II: Chaotic Modulation and Chaotic Synchronization," IEEE Trans. Circuits and Sys., vol. 45, pp. 1129-1139, Nov.1998.

[7] V. Rubezic, and R. Ostojic, "Synchronization of chaotic Colpitts oscillators with applications to binary communications," Proceedings of ICECS '99. vol. 1, pp. 153 -156, Sept. 1999.

[8] A. Azemi and E. Yaz, "Sliding Mode Adaptive Observer Approach to Chaotic Synchronization," ASME J. Dyn. Sys. Meas. Contr., vol. 122, pp. 758- 765, 2000.

[9] So Hayes , C. Grebogi, and E. Ott, "Communicating with chaos," Phys. Rev. Lett. vol. 70, ppo 3031-3034, 1993o

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

[11] M. Lakshmanan and K. Murali, Chaos in Nonlinear Oscillators: Controlling and Synchronization, World Ventific: Singapore, 1996.
[12] K. Murali and M. Lakshmanan, "Transmission of signals by synchronization in a chaotic Van der Pol-Duffing oscillator," Phys. Rev. E, vol. 48, pp. 271-350, 1993.
[13]] Teh-Lu and Nan-sheng Huang, " An Observer-based Approach for Chaotic Synchronization with Application to Secure Communications," IEEE Transaction on Circuits and Systems, vol. 46,pp. 1144-1150, No. 9, 1999.
[14] G. Grassi and S. Mascolo, "Nonlinear Observer Design to Synchronize Hyperchaotic Systems via a Scalar Signal," IEEE Trans. Circuit System, vol. 44, pp. 1011-1014, Oct. 1997.
[15] A. L. Fradkov, H. Nijmenijer and A. Yu. Markov, "On Adaptive Observer-Based Synchronization for Communication," 14th World Congress of IFAC, pp. 461-466, 1999.
[16] M. Itoh, "Spread spectrum communication via chaos," Int.J. Bifurcation & Chaos, vol. 9, pp.155-213,1996.
[17] H. Dedieu, M.P. Kennedy and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic character using self-synchronizing Chua's circuits," IEEE Trans. Circuits & Syst-II, vol.40, Phys. Rev. E, vol. 48, pp. 271-350,1993.
[18] K.M. Short, "Unmasking a modulated chaotic communication scheme," Int. J. Bifurcation & Chaos, vol.6, pp. 367-375,1996.
[19] T. Yang, "Recovery of digital signals from chaotic switching," Int.J.Circuit Theory & Appln.. vol. 23, pp.611-615, 1995.
[20]] G. Perez and H.A. Cerdeira, "extracting messages masked by chaos," Phys. Rev. Lett., vol.74,pp. 1970- 1973,1995.
[21] G. Alvarez, F. Montoya, G. Pastor, M. Romera, "Chaotic cryptosystems," IEEE Transaction, Int. J. Bifurc. Chaos, pp. 332-338, 1999
[22] H. Yu, H. Leung, "A comparative study of different chaos based spread spectrum communication systems," IEEE Transaction, pp. 213-216, 2001
[23] Tao Yang, Chai Wah Wu and Leon Chua, "Cryptography Based on Chaotic Systems," IEEE Trans. On Circuits and Systems, vol.44, pp.469-472, May 1997.
[24]]E. Yaz, and A. Azemi, "Observer design for discrete and continuous non-linear stochastic systems," Int. J. Systems Sci., vol.24, no.12, pp.2289-2302, 1993.
[25] M. Zakai, "On the Ultimate Boundedness of Moments Associated with Solution of Stochastic Differential Equation," SIAM Journal on Control,-, 1967.
[26] P. F. Lorchinger, "Lyapunov Techniques for Stochastic Stability," SIAM J. on Control and Optim., vol.33, pp.1151-1169, 1995.
[27] Leon O. Chua, C. Wu, A. Hung, and G. Zhong "A universal circuit for studing and generating chaos-part I: routes to chaos," IEEE transaction Circuits ans Systems, I: Fundom. Theory Appli., vol.40, pp. 732-744, 1993.