SECURE COMMUNICATION IN NON-LINEAR SYSTEM

Praveen Kumar Pathak[1] and Mr. Manish Sahu[2]
Department of EC , Associate Professor ,Peoples University, Bhopal
Email: praveenpathak7007@gmail.com ,manishsahu196@gmail.com

Abstract: Synchronization between chaotic systems has received considerable attention and led to communication applications. There are two major methods for coupling and synchronizing identical chaotic systems, the cascading method and the one-way coupling method. With these methods, a message signal sent by a transmitter system can be reproduced at a receiver under the influence of a single chaotic signal through synchronization. Data transmission is not safe unless it is assured that the packets will never pass through a router or a computer, over which there is no control. Traditionally, software techniques were used for data encoding. However, the ever-increasing computer power threatens Internet communication security. The study of numerical simulation and circuit simulation of chaos synchronization for chaotic systems including autonomous and non-autonomous (periodically forced) systems. Synchronization properties such as robustness and parameter sensitivity are investigated and the application in signal masking and recovery is also studied. Here a combination of the addition and inclusion methods to mask the information signal is demonstrated.

Key Words: Lorenz Attractor, observer, Rossler system.

1. Introduction

In the 1990s research on the chaotic dynamics of nonlinear sys-tem has focused on the problem of chaos control [1], on the topic of chaos synchronization [2] and on ideas for possible applications of chaos. One such application is chaos communication, where one utilizes the chaotic signals that are generated by nonlinear circuits or optical systems as carriers for information transmission. The simplicity of many chaos generators and the rich structure and broadband nature of chaotic signals are the most attractive features that caused significant interest in possible chaos communication schemes. Chaotic signals, due to the properties like limited predictability, aperiodicity, broad spectrum, and high sensitivity to parametric mismatch/initial conditions, has brought forward the idea of implementing them for secure communication and as an alternative to classical cryptography.[3] Chaotic signals can be implemented to achieve security directly at the physical level. Researchers have pointed out that there exists a very close relationship between chaos and cryptography.

Various characteristics and properties of chaotic signals such as ergodicity, mixing, randomness, complexity, unpredictably and the sensitivity to initial conditions can be connected to the well -known confusion and diffusion properties in the classical cryptography. Pecora and Carroll in 1990 [4], chaotic based communication systems have received tremendous attention. In general, various chaos related schemes have been developed for message encoding in a digital communication environment, with chaotic masking [4], chaotic shift keying [5] and chaos modulation [6] being the main three which are reviewed. The "additive chaos masking" approach was introduced in [7]. In this architecture, the message to be transmitted is first added to a chaotic signal in order to hide the information. The encrypted signal is then sent to the receiver.Synchronization [8] in general can be considered as an appearance of some relations between functional of two processes due to interaction. The choice of the functional is to some extent arbitrary and depends on the problem under consideration. Chaotic synchronization [9], however, is considered as a complete coincidence of the states. Such a regime can result from an interaction between systems or subsystems, as well as from the influence of external noisy or regular fields. Since the definition of chaos includes the rapid decor relation of nearby orbits due to the instabilities throughout phase space, synchronization among dynamical variables in different chaotic systems would appear to be almost a contradiction. In chaos communications security (i.e., privacy) is based on the complex dynamic behaviors provided by chaotic systems. Some properties of chaotic dynamics, such as complex behavior, noise-like dynamics (pseudorandom noise) and spread spectrum, are used to encode data. On the other hand, chaos being a deterministic phenomenon, it is possible to decode data using this determinism. In practice, implementations of chaos communications devices resort to one of two chaotic phenomena synchronization of chaos, or control of chaos.

Lorenz Attractor

Lorenz Attractor is a strange attractor that arises in a system of equations describing the two-dimensional flow of fluid of uniform depth, with an imposed vertical temperature difference. Lorenz system is a set of three coupled first-order differential equations given as $X^{\cdot} = \ (y - x)$
$Y^{\cdot} = \ x\,(r - z) - y$
$Z^{\cdot} = xy - bz,$

It appears to be chaotic, yet it has order of a subtle, fractal kind. The Strange Attractor can take an infinite number of different forms. All of them are fractal and demonstrate infinite self similarity.

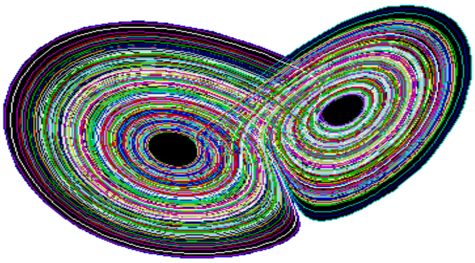


Fig : 1

The Lyapunov exponents measure quantities which constitute the exponential divergence or convergence of nearby initial points in the phase space of a dynamical system. A positive Lyapunov exponent measures the average exponential divergence of two nearby trajectories whereas a negative Lyapunov exponent measures exponential convergence of two nearby trajectories. If a discrete nonlinear system is dissipative, a positive Lyapunov exponent's quantity is a measure of chaos. Our purpose is to design and implement a Jacobian algorithm for calculating the Lyapunov exponents such that it would achieve the following three objectives:

(1) It calculates all n Lyapunov exponents of n-dimensional unknown dynamical system from observations.

(2) It achieves greater accuracy of Lyapunov exponent estimates on a relatively short length of Observations.

(3) The accuracy of the estimates is robust to the system as well as measurement noise.

PI- Observer

Chaos synchronization was originally explored and developed in systems without explicit time-dependence autonomous systems. In the first chaos synchronization scheme due to Pecora and Carroll, the system considered is an autonomous nonlinear system which can be decomposed into multiple stable subsystems. The subsystems may be cascaded so that the driving signal can be reproduced through synchronization. An observer is basically a software sensor that permits to provide an estimation of the unmeasured states variables of a system. In more precise terms, an observer is a dynamical system that uses the available measurements (inputs and outputs) to provide an estimation of the state variables that are not available to be measured. In order to design an observer for a system, we need to analyse the observability of the system. Observability is the property of a system that determines whether an observer design is possible or not.

Definition- The system (3.2) is said to be observable on a time interval [0, T] if for any two distinct initial conditions x_0, there is an input u(t) defined on [0,T] such that the output y, (x_0,u(t)),u(t)) corresponding to these initial conditions when the input u(t) is applied to the system, are also distinct. However, nothing prevents one to add an additional term to the observer that is proportional to the integral of the output observation error; that is,

$$\dot{\hat{x}}=A\hat{x}+Bf(y)+K(y - C\hat{x})+K_i\int(y-c\hat{x})\,dt$$

In such a case the observer is called a proportional integral observer; in short a PI observer.

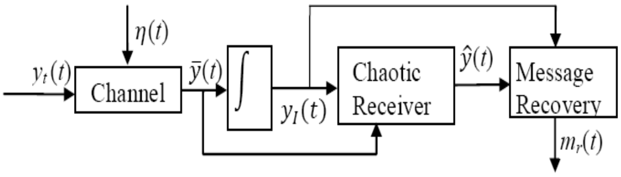


Fig:2

Chaotic masking

Chaotic masking and chaotic switching are two basic forms of chaos synchronization, they are important in secure communication applications. Chaos masking resembles a traditional sense of modulation, Chaotic masking transmitted out analog signal directly simple to realize, with high security. Chaotic switching is used digital signal modulation, compared with chaos masking signal fidelity of higher. This is one of the earlier methods to use chaotic signals for transmitting a message signal as described in and is illustrated in Fig. In this scheme, a message signal is added, i.e. masked, to the output of a chaotic oscillator at the transmitter side prior to transmission.

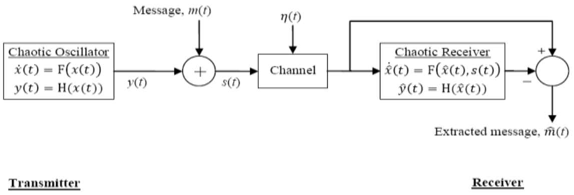


Fig: 3

Rossler System

The Rossler system is a simple model motivated by the dynamics of chemical reactions in a stirred tank. It is a set of three differential equations developed by Rossler to exhibit the simplest possible strange attractor. the three dimensional system, one of the two cascading subsystems must be two-dimensional system. Now, let's investigate all the three possible two dimensional subsystems of the Rossler system:

$$\dot{x}_1 = x_2$$
$$\dot{x}_2 = x_1+ax_2$$
$$\dot{x}_3 = c+ x_2 (x_1-b)$$

Having proved that the Lorenz system has synchronization property, one may now use this property to discuss the masking approach in sending secret messages. Since a chaotic signal is a broadband. Noise-like signal it generally cannot be deciphered when it is transmitting unless the full information about the transmitting system is available at the receiving end. From this point of view, an information bearing signal which is to be transmitted in secure way can be masked by higher power level, Noise-like chaotic signal u(t) by adding it at the transmitter to the information bearing signal m(t). Then the combined signal s (t) = u (t) + m (t), received by the receiver, can be used to regenerate the chaotic signal u,(t) through chaos synchronization. If the synchronization is successful, the u, (t) will converge to u (t) after a short initial transient and the original message can be recovered by subtracting the reproduced chaotic signal u, (t) from the received signal s (t). Assume M (t) is the recovered message then,

$$\begin{aligned} M(t) &= s(t) - u_r(t) \\ &= s(t) - u(t) \\ &= m(t) \end{aligned}$$

Thus, the original information bearing signal is secretly masked then transmitted from one end to the other securely and finally recovered at the receiver end. Practical applications of the principle of synchronization require a certain robustness, i.e. the ability of the receiver to synchronize with the transmitter when the driving signal s(t) differs slightly from x(t), Say, s(t) = x(t) + m(t). where m(t) is the low-power message added to the much stronger chaotic masking signal x(t). If the receiver has synchronized with the transmitter, then $x_r(t) = x(t)$ and m(t) may be received as M(t) = s(t) - $x_r(t)$. If the original message signal m(t) is successfully recovered at the receiver, this kind of chaotic system can be used to send secret messages. The injecting of message in the derivate of the state changes the attractor directly at the phase space and therefore will increase the security while the adding of the message in the output will facilitate the message recovery process.

$$\dot{x}_1 = x_2$$

$$\dot{x}_2 = x_1 + ax_2$$

$$\dot{x}_3 = c + x_2 (x_1 - b)$$

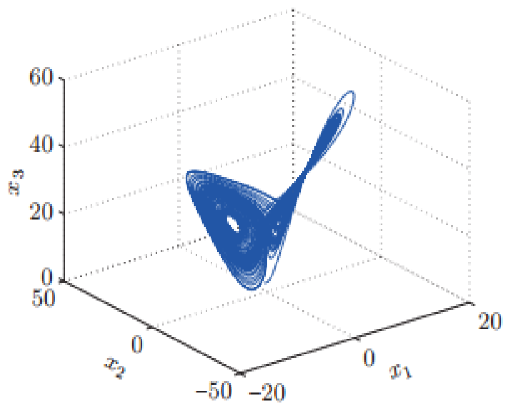
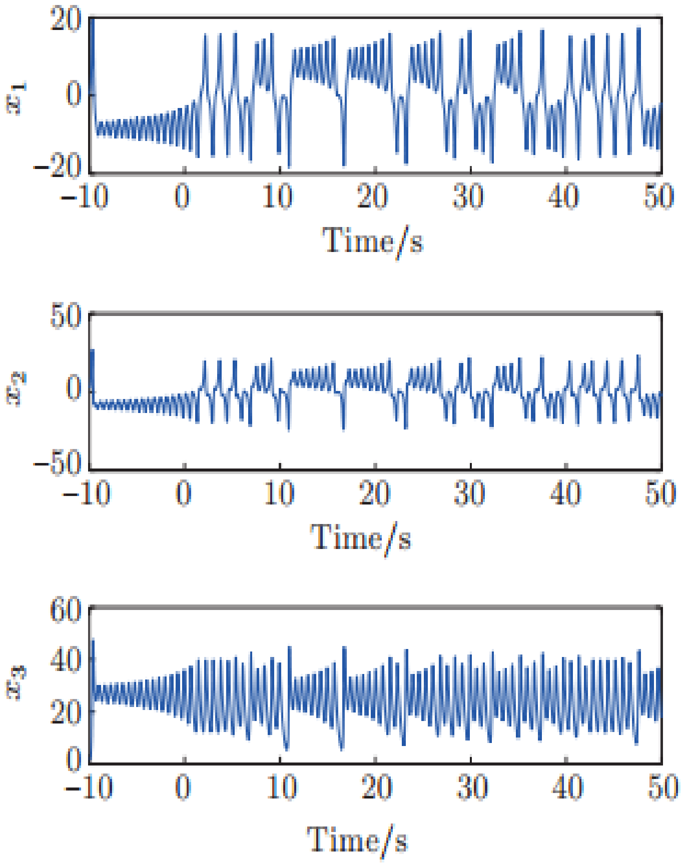


Fig:4



Cascading chaotic system

The scheme of cascading synchronized systems it is required that it can be decomposed into two cascading stable subsystems. For the three dimensional system, one of the two cascading subsystems must be two-dimensional system. The injecting of message in the derivate of the state changes the attractor directly at the phase space and therefore will increase the security while the adding of the message in the output will facilitate the message recovery process.

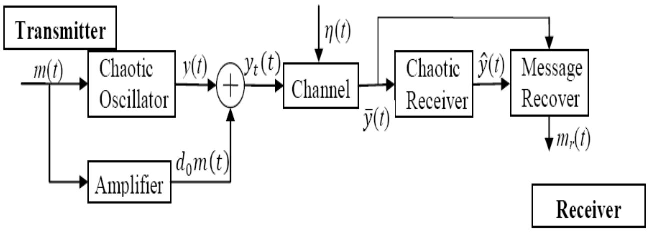
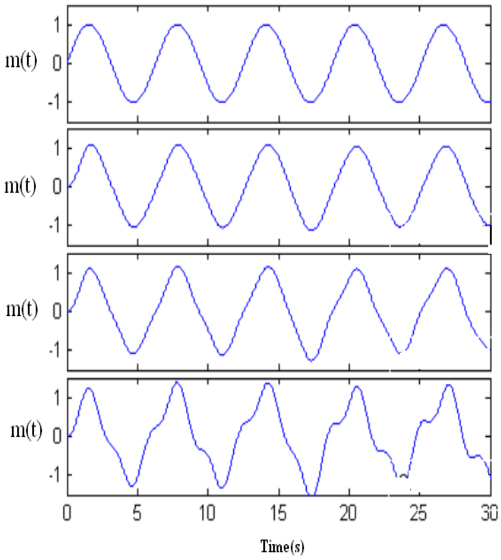


Fig: 5

RESULTS

It is important now to compare the improved performance achieved by the proposed scheme versus the chaotic system.A sinusoidal message signal s = sin (t) is utilized and the algorithm's response is then evaluated under a noisy channel environment. The chaotic carrier signal obtained i.e.y_t is passed through the additive white Gaussian noise (AWGN) channel. The process is repeated by setting signal-to-noise ratio (SNR) to 20, 15, 10 and 5 dB. At the receiver, a low pass filter is used in order to reduce the noise power.



When SNR is 15 dB, both the recovered message and input signals are matched very well, but for lower values of SNR the recovered signal is somewhat distorted. The approach recommended a SNR (value) of 25 dB, whereas results obtained by the proposed chaotic system here outperforms with much lower SNR values.

CONCLUSION

The objective of paper was to explore techniques to exploit the properties of chaotic signals to implement secure communication. The facts that chaotic signals were a periodic, broadband and sensitive to initial conditions/parameters mismatches were important for them to be utilized in security. Therefore the chaotic parameters acted some sort of hardware key and hence same dynamical system was necessary for the transmitter and the receiver with proper chaotic synchronization techniques.

The advantages of proportional observer (PI-observer) including flexibility on the choice of observer gains, this approach is employed in the design of the receiver, which is a non-linear chaotic system based on the Rossler proposition. However, in order to verify the theoretical presentation, simulations were run and the results clearly demonstrate that the desired performance is possible at SNR >= 15 dB While, minimum SNR for the model is 25 dB.

REFRENCES

[1] E. Ott, C. Grebogi, J. A. Yorke, Controlling chaos, Phys. Rev. Lett. 64 (1990) 1196 { 1199.

[2] H. Fujisaka, T. Yamada, Stability theory of synchronized motion in coupled-oscillator systems, Prog. Theor. Phys. 69 (1983) 32 { 47.12}

[3] V. S. Afraimovich, N. N. Verichev, M. I. Rabinovich, Stochastic synchronization of oscillation in dissipative systems. Radio physics and Quantum Electronics (English Translation of Izvestiya Vysshikh Uchebnykh Zavedenii, Radiozika) 29 (1986) 795{ 803.

[4] L. M. Pecora, T. L. Carroll, Synchronization in chaotic systems, Phys. Rev. Lett. 64 (1990) 821 { 824.

[5] B. Sklar, Digital communications : fundamentals and applications, Prentice-Hall, Englewood Clis, NJ, 1988.

[6] G. M. Maggio, N. Rulkov, L. Reggiani, Pseudo-chaotic time hopping for uwb impulse radio, IEEE T. Circuits-I. 48 (12) (2001) 1424{1435}.

[7] C. C. Chen, K. Yao, K. Umeno, E. Biglieri, Design of spread-spectrum sequences using chaotic dynamical systems and ergodic theory, IEEE T. Circuits-I. 48 (9) (2001) 1110{1114}.

[8] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, A. R. Volkovskii, Digital communication using chaotic-pulse-position modulation, IEEE T.Circuits-I. 48 (12) (2001) 1436{1444}.

[9] L. E. Larson, J.-M. Liu, L. S. Tsimring (Eds.), Digital Communications Using Chaos and Nonlinear Dynamics, Institute for Nonlinear Science,Springer, 2006.