Secure communications by chaotic carrier signal using Lorenz model

Raied Kamel Jamal, Dina Ahmed Kafi

Department of Physics, College of Science, University of Baghdad, Baghdad, Iraq

E-mail: dina.hanoo83@gmail.com.

Abstract

In this paper, the generation of a chaotic carrier by Lorenz model is theoretically studied. The encoding techniques has been used is chaos masking of sinusoidal signal (massage), an optical chaotic communications system for different receiver configurations is evaluated. It is proved that chaotic carriers allow the successful encoding and decoding of messages. Focusing on the effect of changing the initial conditions of the states of our dynamical system e.i changing the values $(x, y, z, x_1, y_1,$ and $z_1)$.

<div dir="rtl">

تامين الاتصالات بواسطة الاشارات الفوضوية الحاملة باستخدام نموذج لورنز

رائد كامل جمال، دينا احمد كافي

قسم الفيزياء، كلية العلوم، جامعة بغداد، بغداد، العراق

الخلاصة

في هذا البحث، توليد الحاملات الفوضوية بواسطة نموذج لورنز تم دراسته نظريا. تقنية التشفير المستخدمة هي اخفاء الفوضى (الشواش) لأشارة جيبية (الرسالة)، انظمة الاتصالات الفوضويه البصرية لمتسقبلات مختلفة تم تقييمها. انها اثبتت ذلك الحاملات الفوضوية السماح بنجاح تشفير وفك التشفير للرسائل المستلمة. بالتركيز على تاثير تغيير الشروط الابتدائية لحالات النظام الديناميكي المستخدم، هذا يعني تغيير قيم $(x, y, z, x_1, y_1$ و $z_1)$.

</div>

Introduction

The Lorenz system is one of a few standard oscillators commonly used to explore chaos [1]. The information can be on transmitted by masking it into a chaotic signal, the amplitude of the message being added to that of the carrier [2]. Two chaotic systems can be synchronized when they are properly coupled [3]. This phenomenon has a very good application potential in transmission coding [4]. The transmission is made by using an emergent wave from a laser as a chaotic transmitter [5]. The signal is attached to a carrier wave which is of a chaotic nature and has much higher amplitude. This ensures a higher degree of difficulty in intercepting and decoding. For attaching the signal to the carrier chaotic masking, modulation and translation can be used[6]. The properties of transmission and reception of the data as well as the synchronization of the lasers can be studied by using a pair of master-slave lasers. In chaotic masking, message signal is simply added to the chaotic signal and is transmitted [7]. Schematic diagram for chaos masking is shown in Fig.1a. Receiver recovers the message signal by subtracting locally generated chaos signal from received signal as shown in Fig.1b [8]. Chaos communication is an application of chaos theory which is aimed to provide security in the transmission of information performed theory

telecommunications technologies. By secure communications, one has to understand that the contents of the massage transmitted are increasable to possible eavesdroppers [9]. In chaos communications security (i.e., privacy) is based on the complex dynamic behaviors provided by chaotic system. In the last few decades chaos become very interested field in many application: Many researchers were away of the existence of complex dynamics in well-defined system from the beginning of early 1900s. Henri Poincare (1913), prominent French mathematician he was noted the "sensitivity to initial conditions [10].

Pecora and Carroll (1990) worked on chaos synchronization, in the last two decades; various schemes have been successfully applied for chaos synchronization such as OGY method (Ott, Grebogi and Yorke, 1990) [11]. Liu (2002) proposed approaches for the synchronization for the chaotic and hyper chaotic systems in the literature. A synchronization scheme for the chaotic systems in which the last state variable of the drive system is taken as the driving scalar signal and its linear feedback gain is a function of the free parameter and the global synchronization is attained by simple linear output feedback error [12].
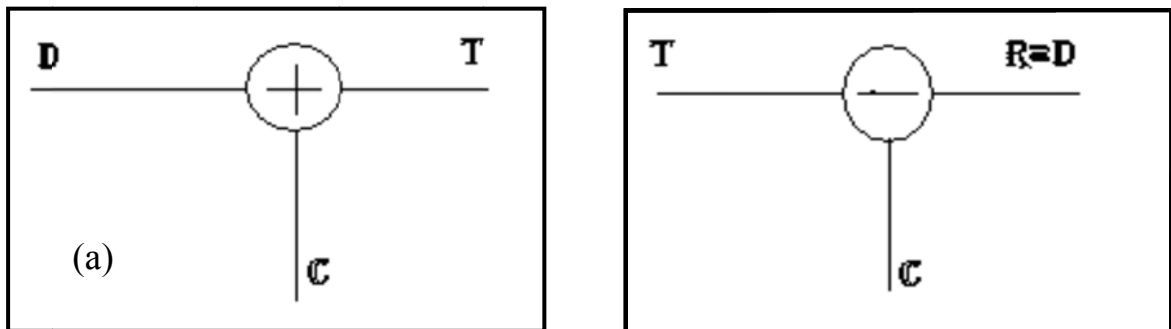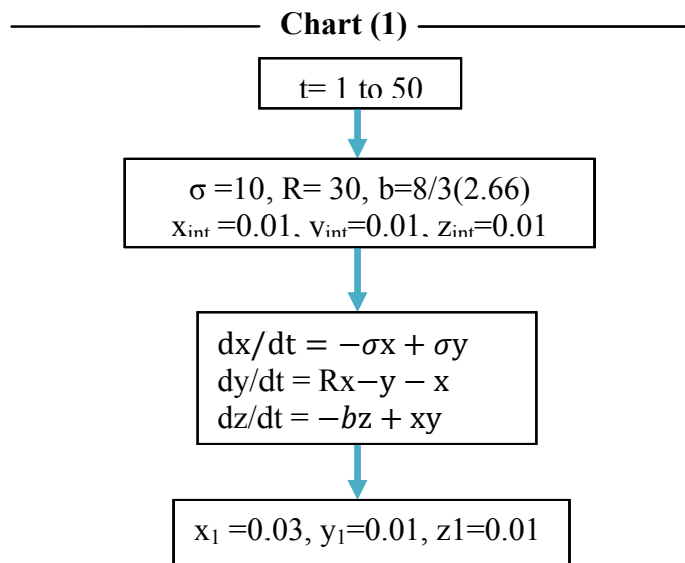

Fig.1: (a) Transmitter setup, (b) Receiver setup [13].

The dynamical model

The three Lorenz equations can be solving it numerically by using Berkeley Madonna software, as following in this chart:

──────── **Chart (1)** ────────

t= 1 to 50

σ =10, R= 30, b=8/3(2.66)
x_{inf} =0.01、v_{inf}=0.01、z_{inf}=0.01

$$dx/dt = -\sigma x + \sigma y$$
$$dy/dt = Rx - y - x$$
$$dz/dt = -bz + xy$$

x_1 =0.03, y_1=0.01, z1=0.01

Fig.2: Flow chart (1).

The first block from this flow chart Fig.2 represents the time scale of chaotic signal that generated in system and it is changeable in any range of time. Sequentially the second block represent the parameters values of Lorenz system that exhibits chaotic dynamic, where it positive and limited values. The Lorenz system equations written in the third block. Finally, the initial conditions values of the system, these values are very important to change chaotic system behavior.

To study the synchronization in Lorenz model must take two Lorenz models, as shown in the flow chart (2) Fig.3 that called (transmitter and receiver part) and the term $k*(x_1-x)$ add to first equation in x scale for second Lorenz model, as show, where the second Lorenz model (receiver part) different the first one (transmitter

part) in initial conditions in (x_1) scale, moreover the term $k*(x_1-x)$ called synchronization term and the k called the coupling factor. By changing the coupling factor value gradually the full synchronization will obtain. To study the secure communications the observably program apply, after adding message like sinusoidal signal on transmitter part in y scale for Lorenz equation. This sinusoidal signal message is [m (t) =A sin (2πf t)], where A and f represent the amplitude and frequency of the message signal respectively. By this way the chaotic signal can be used as the carrier signal and this technique called chaos masking method. By changing the A and f values which can be used to study the significant of system in carrier signal, where there are limitation in A and f values.
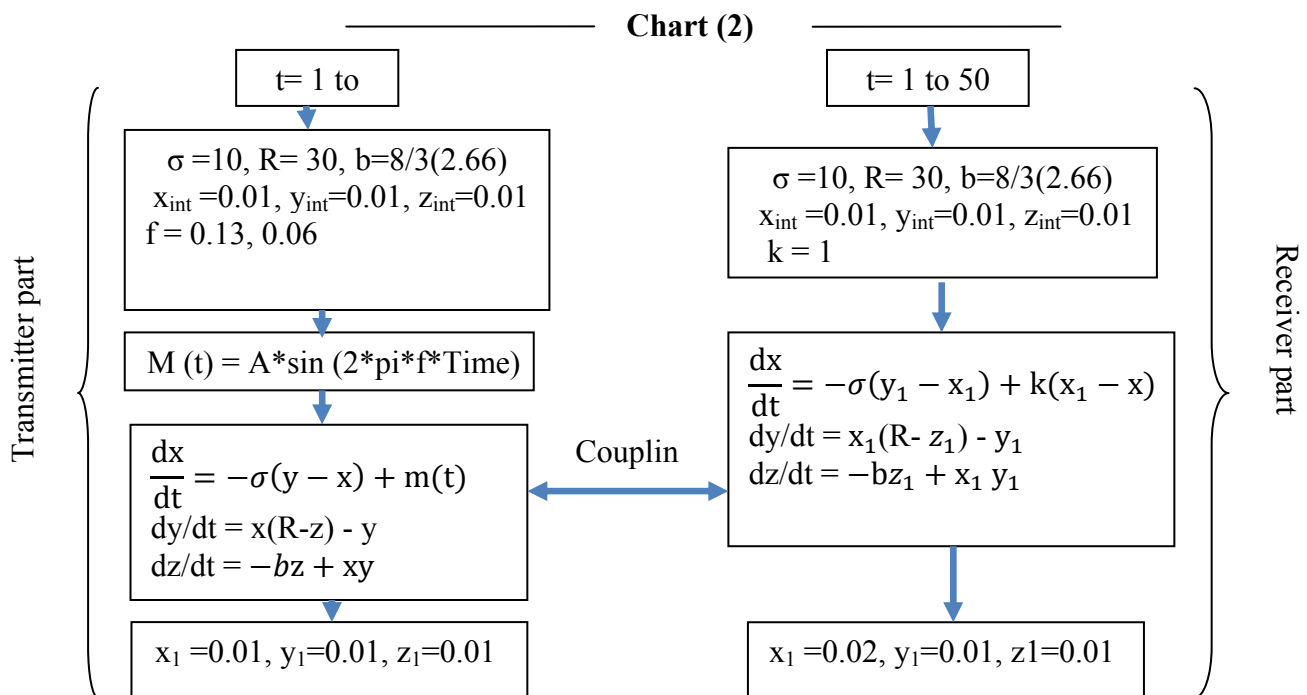
Chart (2)

Transmitter part		Receiver part

t= 1 to

t= 1 to 50

σ =10, R= 30, b=8/3(2.66)
x_{int} =0.01, y_{int}=0.01, z_{int}=0.01
f = 0.13, 0.06

σ =10, R= 30, b=8/3(2.66)
x_{int} =0.01, y_{int}=0.01, z_{int}=0.01
k = 1

M (t) = A*sin (2*pi*f*Time)

$$\frac{dx}{dt} = -\sigma(y - x) + m(t)$$
dy/dt = x(R-z) - y
dz/dt = $-b$z + xy

Couplin

$$\frac{dx}{dt} = -\sigma(y_1 - x_1) + k(x_1 - x)$$
dy/dt = x_1(R- z_1) - y_1
dz/dt = $-bz_1 + x_1 y_1$

x_1 =0.01, y_1=0.01, z_1=0.01

x_1 =0.02, y_1=0.01, z1=0.01

Fig.3: Flow chart (2).

The numerical model results

The modeling approach of chaos was investigated by programming the physical model as shown in the flow chart, where the total simulation time

chosen depends strongly on the magnitude of the temporal scales defined by three parameters R, σ and b, depending on initial conditions. To demonstrate the first property of chaos,

i.e. aperiodicity, a numerical simulation was done using Berkeley Madonna software of ordinary differential equations [14]:

$$dx/dt = -\sigma x + \sigma y$$
$$dy/dt = Rx - y - x$$
$$dz/dt = -bz + xy$$

(1)

These equations in Lorenz model describing the fluid motion and heat flow.

where X, Y, and Z are the states of the system and σ, R, and b are positive parameters (where σ is the Prandtl number, R is the Rayliegh number and b is a geometric factor), which denote physical characteristics of air flow. Typical parameter values that yields chaotic dynamics are $\sigma = 10$, $R = 30$, and $b = 8/3 = (2.66)$. For these values, the attractor generated by numerically integrating Eq. (1). To obtain a practical circuit design for the Lorenz system, it is necessary to scale the system equations.

The numerical simulation procedure to find the time series of x, y, and z coded and calculated by the forth order Runge –Kutta method. The stochastic parameters are $\sigma = 10$, R=30, and b=8/3(2.66), while the initial conditions are $x_{int} = 0.01$, $y_{int}=0.01$, and $z_{int}=0.01$. The observed intensity spectra with time for three dynamical states are shown in Figs.3, 4, and 5, where the states x, y, and z are evolving with time periodically.

The irregular behavior is also true for other variables y and z. The second property in the definition for Lorenz system is trivia. The irregular behavior in the Lorenz system is arising because of the intrinsic non-linearity of the system itself rather than the noisy parameters. The FFT for these dynamical stats are shown in Fig. 6.

The (FFT) of the chaotic signal has exponential decay shape and this is one way to distinguish noise from chaotic behavior because the (FFT) of noise has Gaussian distribution. Another nice property of chaos can be seen by plotting the variable z versus x of Lorenz system by numerically integration, see Fig. 7. The Figure shape is called the strange attractor, showing how x and z evolve against time, as well as demonstrating how a simple looking deterministic system could have extremely erratic dynamics where solution oscillate irregularly, never exactly repeating but always remaining in a bounded region of phase space. The strange attractor is not a point or a curve or even a surface, it is a fractal with a fractional dimension between 2 and 3. The same behavior, when plot between variable y versus x, is shown in Fig. 8. These figures explain the butterfly effect of the non-linear dynamical system.

The final diagram that shows the scenario of nonlinear dynamic behavior of system is bifurcation diagram, as shown in Fig. 9. A system transition from one type of behavior to another depending on the values for important parameters like (b) value in Lorenz equation. If (b) value is changing from 0 to maximum value 2.7 the amplitude of x scale in time series divide in three parts. The first one is curve line where b value is starting from 0 to 0.6 that called regular oscillation. The second part called period doubling that is starting from 0.6 to 0.8. Finally, the chaos behavior region is starting from 1 to 2.7, where the optimum value to get chaotic behavior at 2.7.
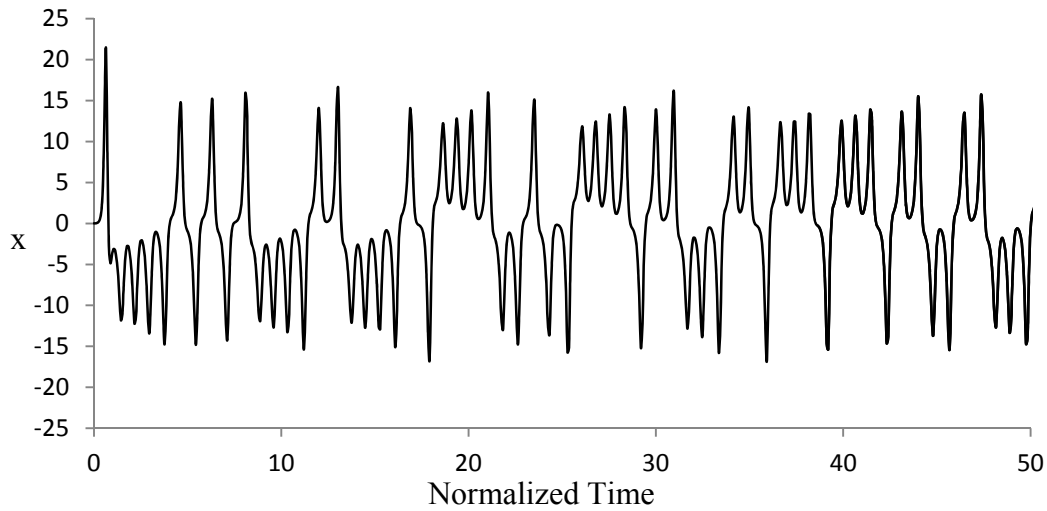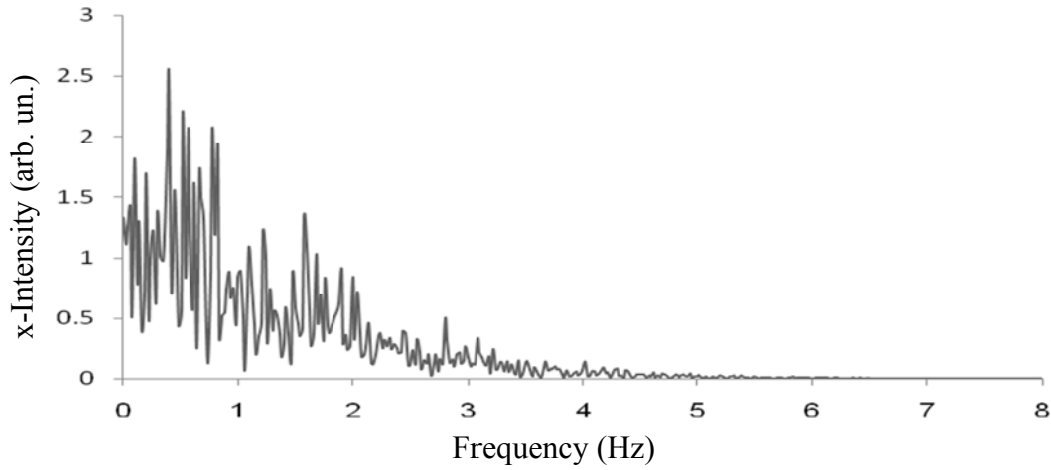
Fig. 4: The intensity of x dynamical state as function of time series when σ =10, R=30, and b=8/3(2.66) at x_{int} =0.01, y_{int}=0.01, and z_{int}=0.01.
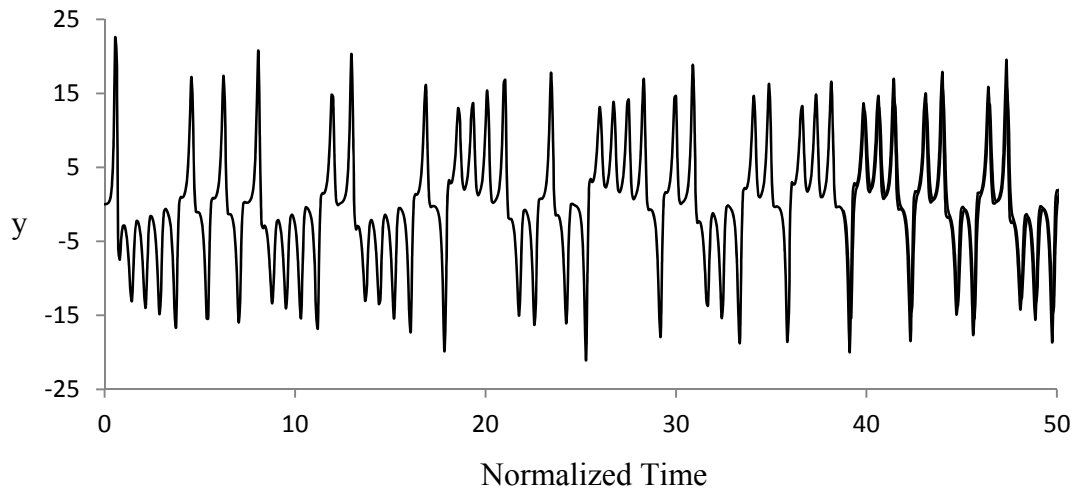

Fig. 5: The intensity of y dynamical state as function of time series when σ =10, R=30, and b=8/3(2.66) at x_{int} =0.01, y_{int}=0.01, and z_{int}=0.01.
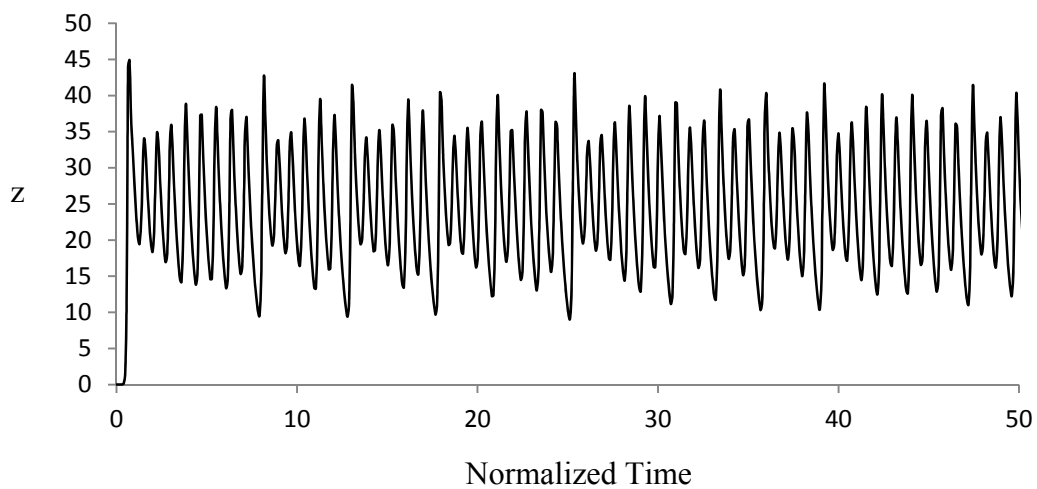
Fig. 6: The intensity of z dynamical state as function of time series when σ =10, R=30, and b=8/3(2.66) at x_{int} =0.01, y_{int}=0.01, and z_{int}=0.01.

Fig. 7: The intensity as function of frequency (FFT) for x, y, and z dynamical states respectively where are these states identical.
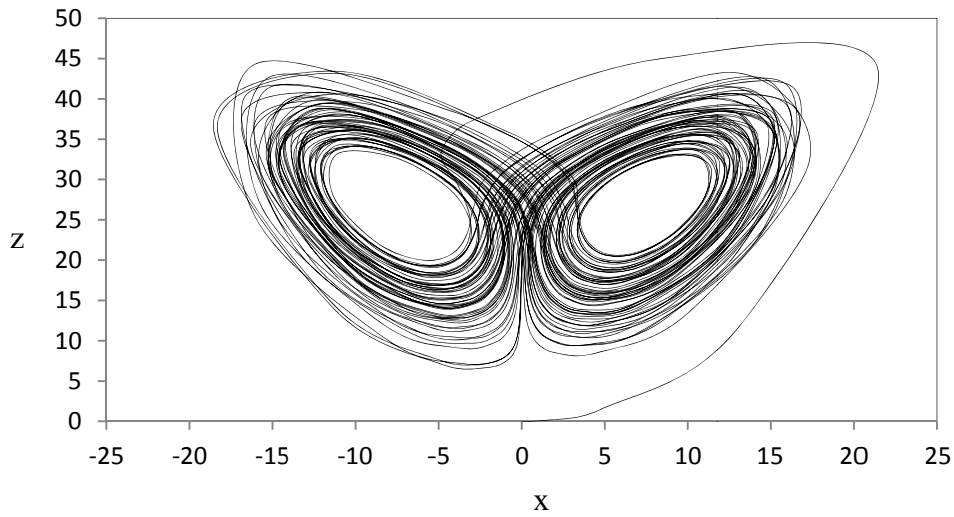
Fig. 8: Strange attractor of the Lorenz system plotting z against x by numerical integration of the system equations with σ =10, R=30, and b=8/3 (2.66), at x_{int} =0.01, y_{int}=0.01, and z_{int}=0.01.
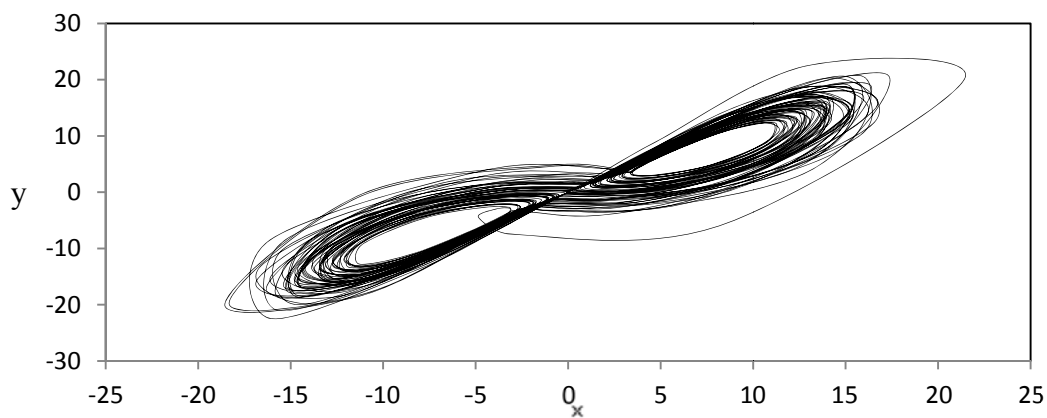
Fig. 9: Strange attractor of the Lorenz system plotting y against x by numerical integration of the system equations with σ =10, α=28, and b=8/3(2.66), at x_{int} =0.01, y_{int}=0.01, and z_{int}=0.01.

To exhibt the sensistive dependence of system on initial condition, the simulation is performed a gain as shown in flow chart. Two identical systems (transmitted and received) are taken with same parameters but strating from different initial conditions (nearly howerver identical). The difference in intital 0.03. Fig. 10 depicats the time series of variable x_{int} and x_{1int} for two Lorenz systems (transmitted and reciver). After some period, the two variables are diverging from each other even though they started from identical initial conditions. To check the identical chaotic signal between these two systems must plot between amplitude of x scale versus amplitude of x_1 scale, as shown in Fig.11. It shown diffusion distribution in (x-x_1) plane with great accumulate point in (0, 0) point. Synchronization in chaotic systems occurs by using synchronization term $C=k(x_1-x)$ where transmitted and received are connected to each other, Where Fig. 12 show the series plot of variables x and x_1 for coupling factor k=15.
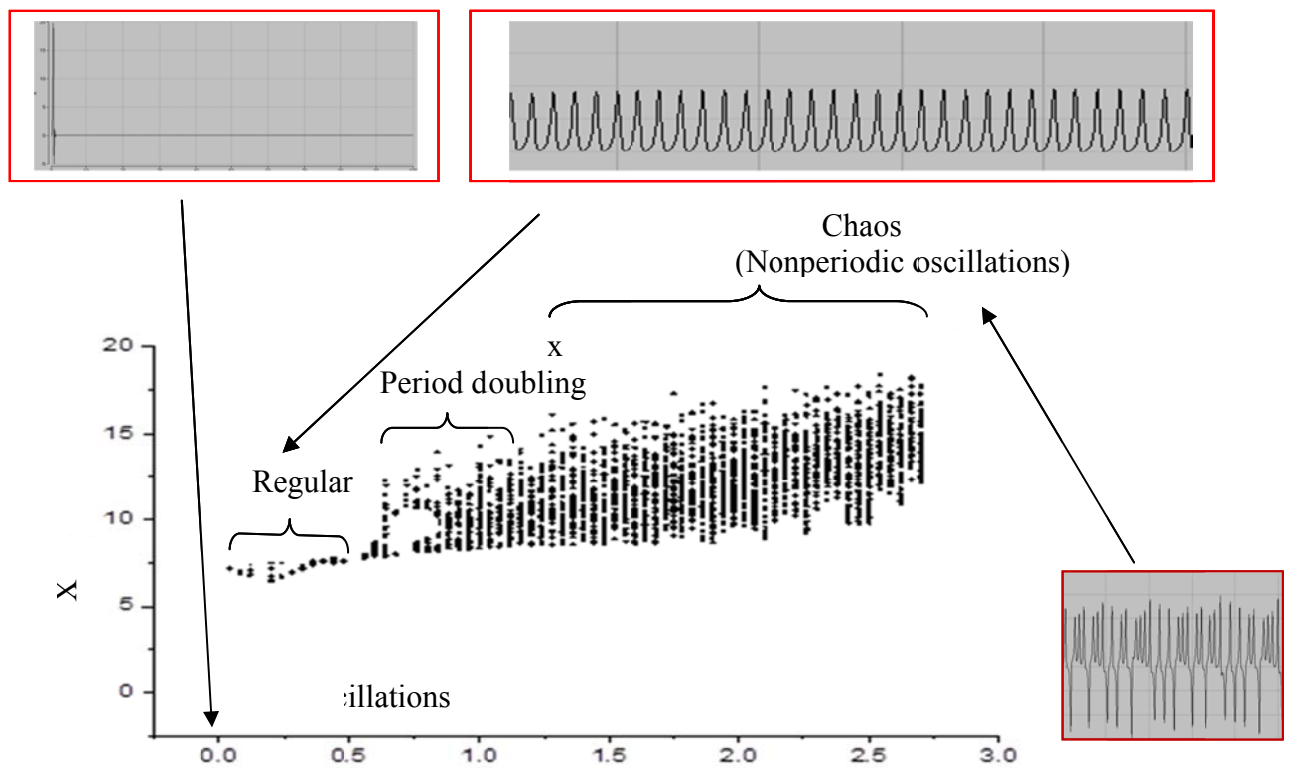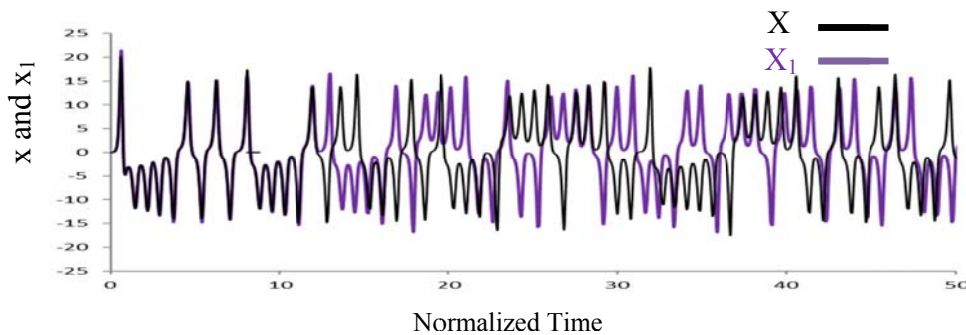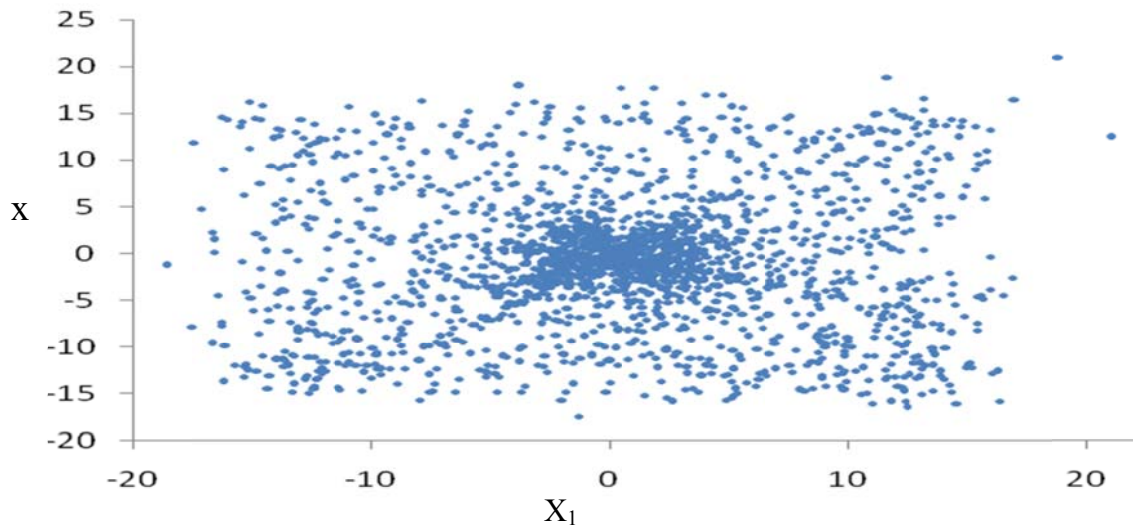

Fig. 10: Bifurcation diagram.

Normalized Time

Fig. 11: Time series plot of variable x and x1 of two similar Lorenz system starting from a nearly identical initial conditions (x_{int}=0.01, and x1int=0.03).

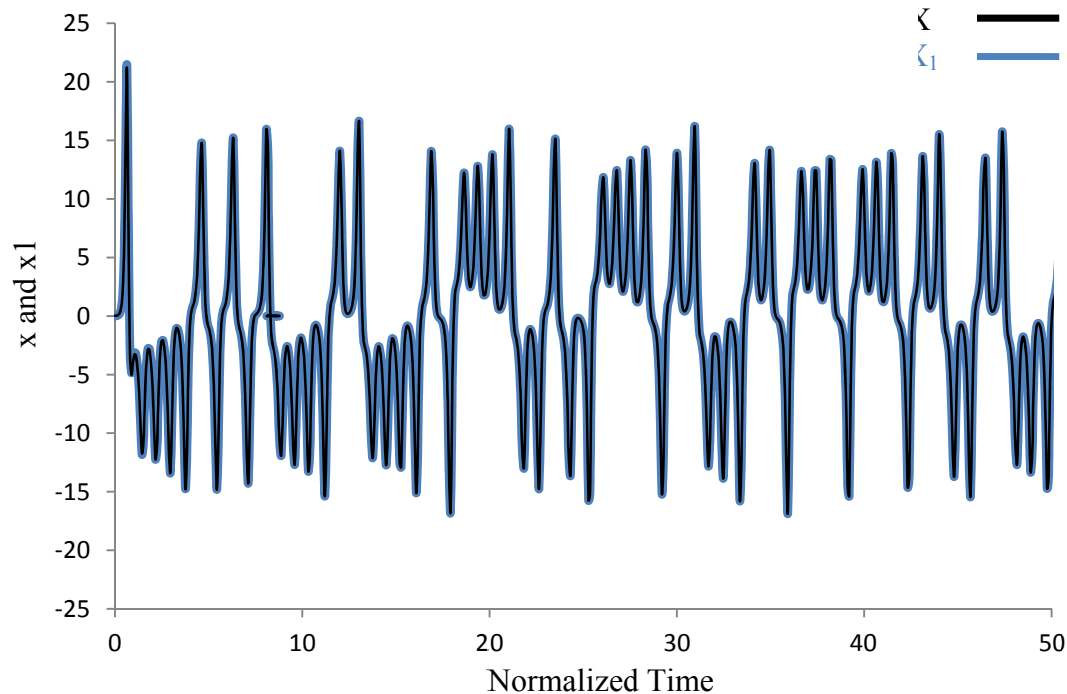**Fig.12: x vs. x1, of two similar Lorenz system at xint=0.01, x1$_{int}$=0.03, and k=0 without synchronization.**

It´s shown from Fig.12 got full synchronization between the transmitter and receiver system where the coupling factor was k=15.

Drawn the attractor for x-x$_1$ of two similar Lorenz systems (transmitter and receiver), at full synchronization (k=15) show linear relation between them, as shown in Fig. 13, where the slope of curve was 1.


Fig.13: Time series plot of variable x and x1 of two similar Lorenz system at x$_{int}$=0.01, x1$_{int}$=0.03, and   k=15 (full synchronization).

Chaotic signals in secure communication systems

On might feel that since the signal generated from chaotic system irregular in nature, therefore, these types of signals cannot have any practical application and should be avoided. However, the properties of the chaotic signal can in fact be used in different fields of communication engineering particularly; spread spectrum applications to achieve chaotic synchronization, there had to be some sort of coupling present between the two chaotic systems. If we consider unidirectional coupling, then a signal from one chaotic (transmitter system) is being transmitted to another chaotic (receiver system). This is analogous to communication systems where a carrier signal is modulated by a massage signal prior to transmission. Therefore, the chaotic signals can be used as the carrier signal. Using the chaotic masking method; that is one of the earlier methods to use chaotic signal for transmitting a massage signal. In this scheme, a massage signal is added i.e., masked to the output of a chaotic oscillator at the transmitter side prior to transmission, as shown in Fig. 14.
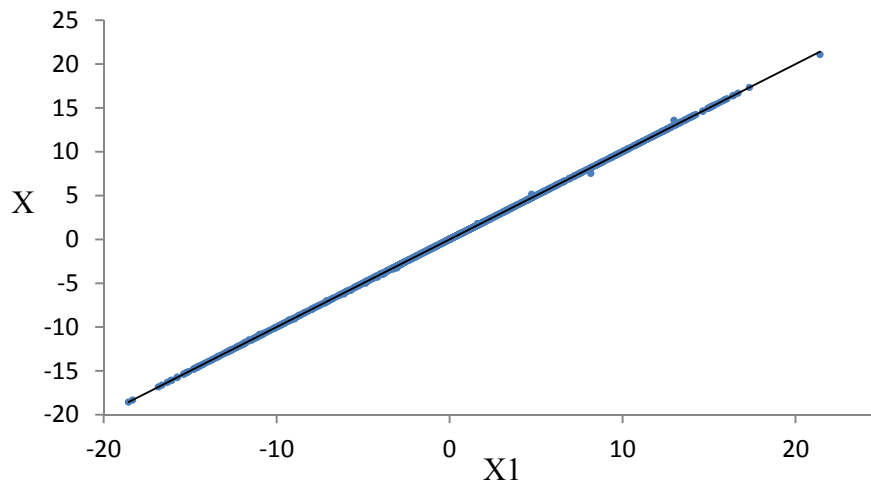
Fig. 14: x vs. x1, of two similar Lorenz system at xint=0.01, x1$_{int}$=0.03, and k=15 (full synchronization).

In Fig. 15 with information message signal m (t) =A sin (2πf), four different amplitudes A=1, and 11 are studied, whose frequency 0.13, 0.06 Hz, as shown in Figs. 15, 17, and 19 respectively. It is represent the transmitted signal, input and output sinusoidal signal message, where the recovered message signal is (green line) and input massage signal (red line). Few things are worth mentioning regarding the implementation of the chaotic communication system which will also be helpful in our result. One point worth pointing out is, the chaotic signals really broadband, since, the basic idea was to hide the narrow band message spectrum within the wide band of chaotic signals, therefore the chaotic signals being used as the carrier should have a wide spectrum. However, the power spectrum (FFT) of the output signal from the Lorenz oscillator illustrate that the spectrum hardly exceeds beyond 4-5Hz as shown in Figs. 16, 18, and 20.

Therefore a message signal e.g. a sinusoidal signal with a frequency of 5Hz after being masked with that chaotic signal will be easily detected

from the observed spectrum of the masked signal. Also, the power of the massage signal should be considerably lower than the power of the chaotic carrier; otherwise once again the message signal will be clearly visible in the spectrum, this is illustrated in FFT Figs. 16, 18, and 20. So the fundamental frequency for massage signal becomes more evidentially by increasing the amplitude of the input massage signal. This result led us to conclude that the spectrum of chaotic signal must be larger than spectrum of input massage. By the same observably manner, when changing the input signal frequency from 0.13 Hz to 0.06 Hz obtain the Fig. 19. The fundamental frequency for signal massage is evident again in this state, so the secure communication was failed this as shown in Fig. 21.
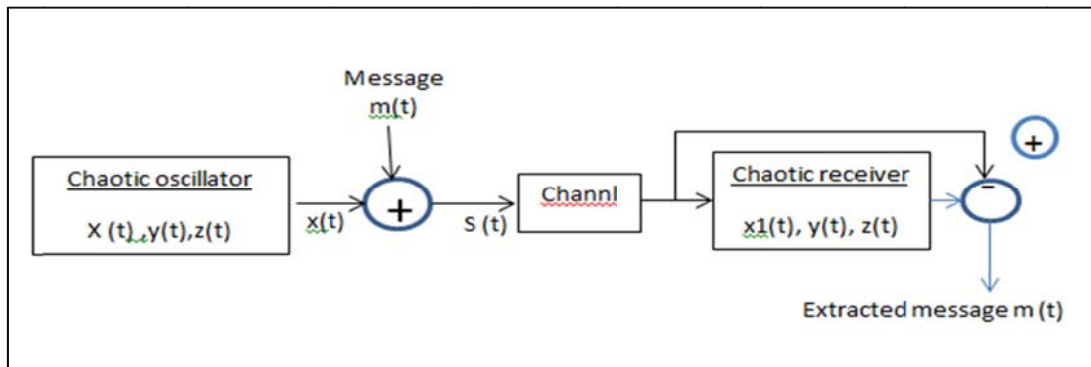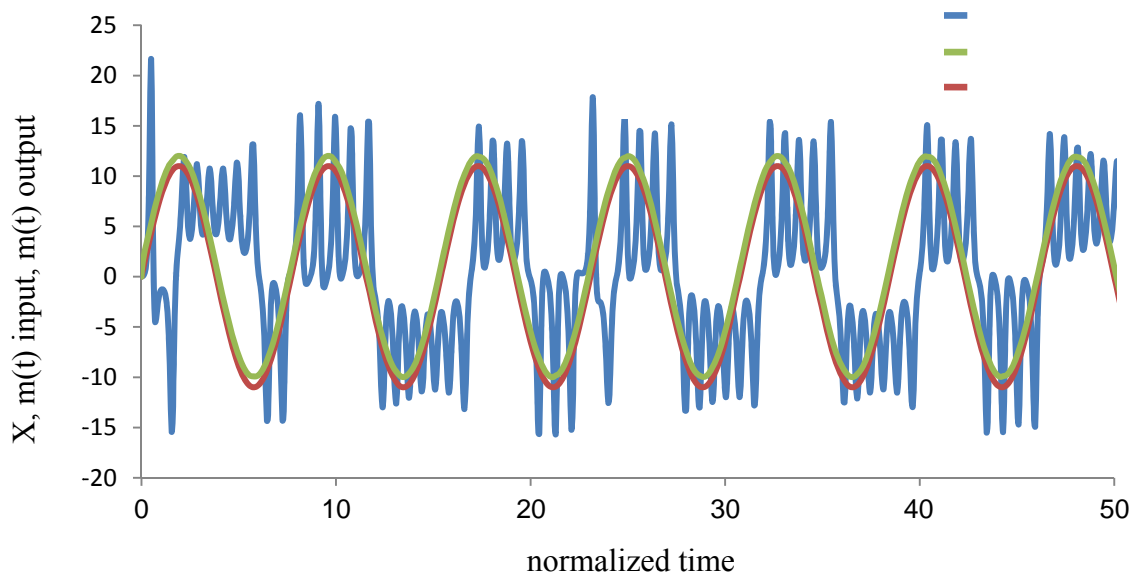

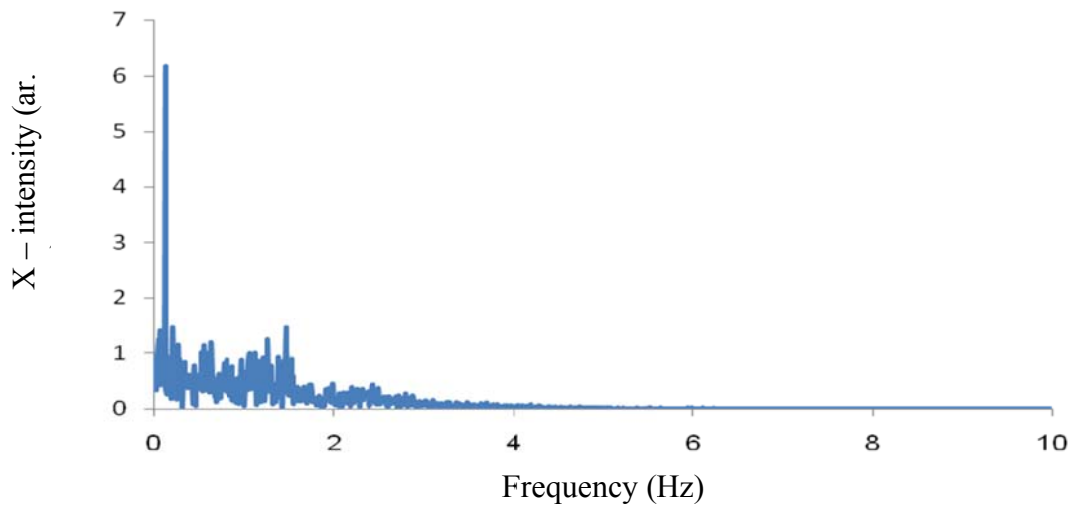*Fig. 15: Chaotic communication scheme based on chaotic masking.*
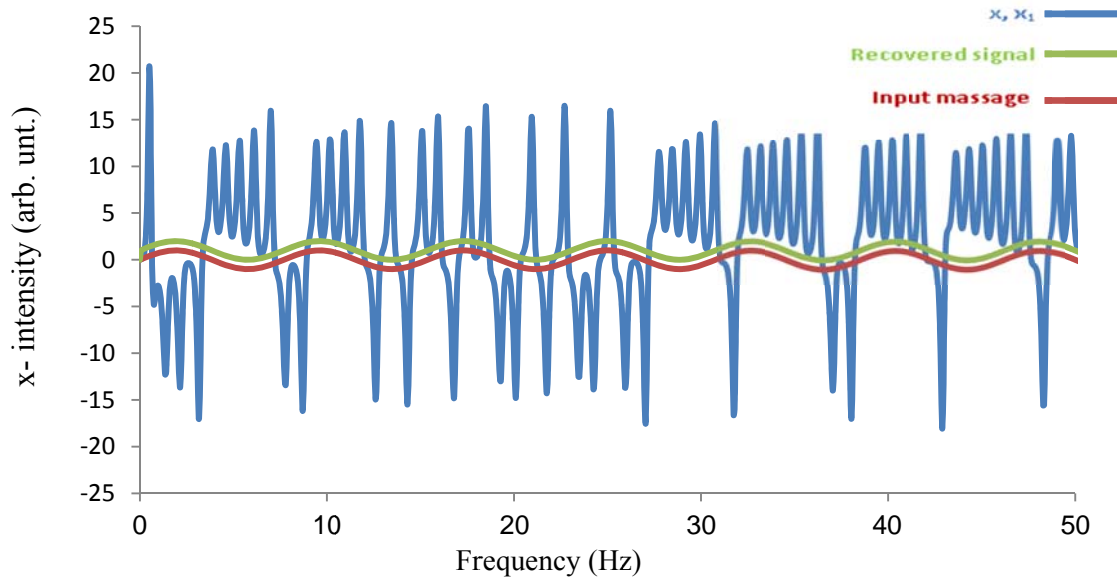
Fig. 16: FFT spectrum at [x_{int}=0.01, $x1_{int}$=0.03, k=15, A=1 and f=0.13Hz].
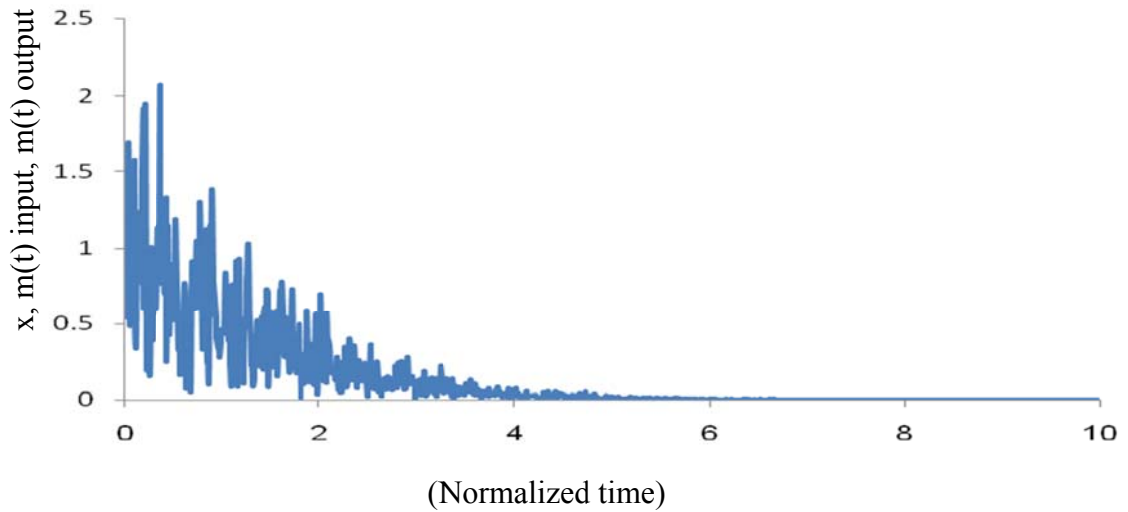
(Normalized time)

Fig. 17: x, m (t) input and m (t) output vs. normalize time, at x_{int}=0.01, $x1_{int}$=0.03, k=15, A=1 and f=0.13Hz.

normalized time

Fig. 18: x, m(t) input and m(t)output signal vs. normalized time, at x_{int}=0.01, $x1_{int}$=0.03, k=15, A=11 and f=0.13Hz.

Frequency (Hz)

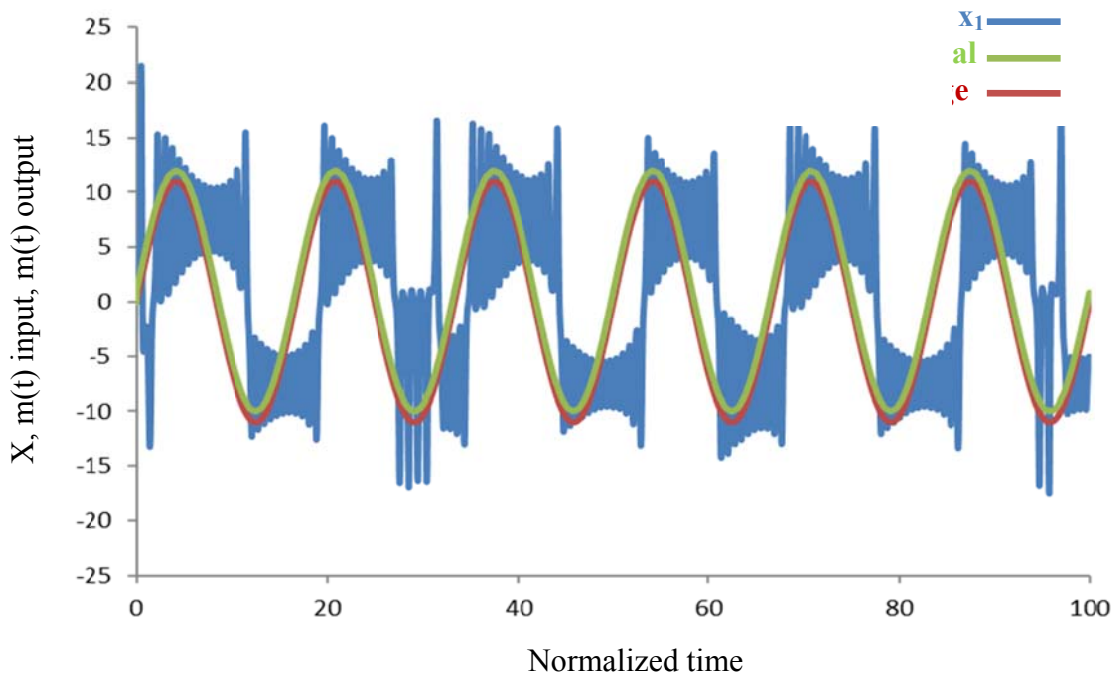***Fig. 19: FFT spectrum at [x_{int}=0.01, $x1_{int}$=0.03, k=15, A=11 and f=0.13Hz].***

Fig. 20: x, m (t) input and m (t) output signal vs. normalized time at xint=0.01, x1$_{int}$=0.03, k=15, A=11 and f=0.06 Hz.
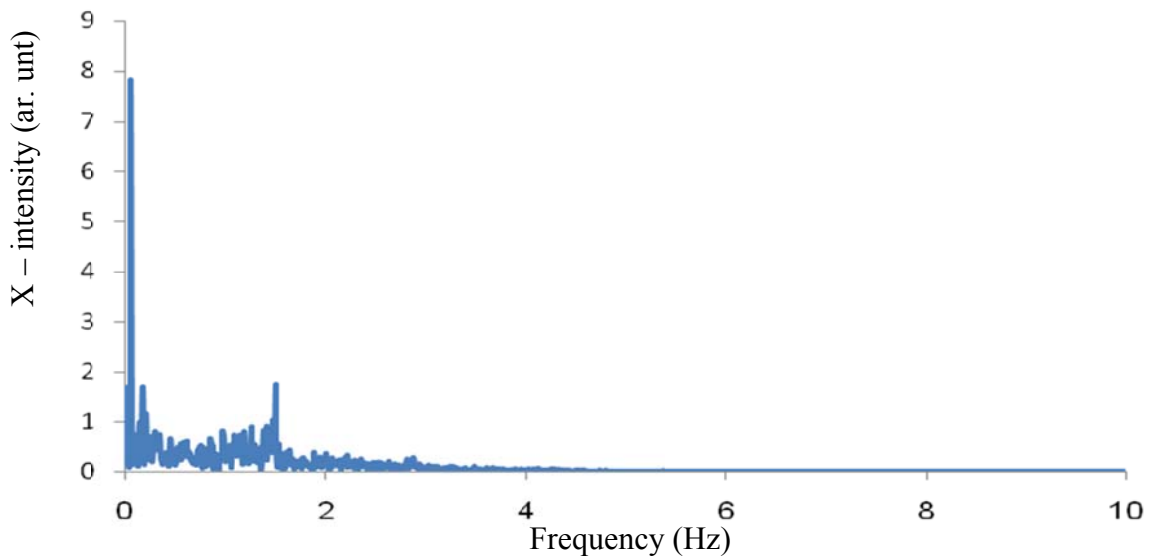

Fig. 21: FFT spectrum at x$_{int}$=0.01, x1$_{int}$=0.03, k=15, A=11 and f=0.06 Hz.

Conclusions

This work demonstrates the feasibility of a simple method to synchronize two Lorenz systems with different parameters and then extend it to the recovery of the information signal, which is originally inserted into a chaotic signal, with satisfactory precision. To keep the communication more secure, the peak of power spectrum of the information signal had better be as indistinguishable from these of the neighboring frequencies of the masking variable as possible, that is "almost hidden" in the spectrum of the transmitted signal.

References

[1] J. M.T.Thompson and H.B Stewart, "Nonlinear Dynamic and chaos" Wiley, New York, (1986).

[2] S. Hayes, C. Grebogy, E. Ott, Phys. Rev. Lett. 70, 20 (1993) 3031-3034.

[3] Jiin-Po Yeh, Kun-Lin Wu "ASimple method to synchronize chaotic system and its application to secure communications ", Mathmatical and computer modelling, vol.47, (2008).

[4] R.Lang and K.Kobayashi, IEEE Journal of Quantum Electronics, 16 (1980) 347-355.

[5] E.N.Lorenz, W. Kinzel, A. Englert and I. Kanter, J. Atoms. Sci. 20, 2 (2010) 130-141.

[6] L. M, Pecora and T. L. Caroll, Phys. Rev. A 44, 4 (1991) 2374 - 2383.

[7] Bindu M. Krishnai, Manu P. John, V. M. Nandakumaran, Pramana Journal of Physics, 74, 2 (2010) 224-243.

[8] C. Mirasso, J. Mulet, C. Masoller, IEEE Photonic Technology Letters, 14, 4 (2002) 456-458.

[9] K. Ikeda and K. Mastomoto, Physical D, 222 (1987) 310- 321.

[10] J. Ohtsubo, "Semiconductor Laser Stability, Instability and Chaos", 3rd Edition. Springer, 2013.

[11] L. M. Pecora, T. L. Carroll. Phys. Rev. Lett. 64 (1990) 821-824.

[12] S. Tang A. I. Mees and L. O. Chua, IEEE Trans. Circuits, 30, 620 (1983) 220-310.

[13] K. Al-Naimee, F. Marino, M. Ciszak, R. Meucci, T.F. Arecchi, New J. Phys., 11 (2009) 1-3.

[14] E. N. Lorenz, Journal of Atmospheric Sciences, 20 (1963) 130-141.