

MASKING OF MESSAGES USING THE DOUBLE SCROLL ATTRACTOR IN PRIVATE COMMUNICATIONS⁺

Waleed A. AL-Hussaibi*

Abstract

Message masking in private communication is described using a computer simulation of chaotic system such as double scroll oscillator. Mask of chaotic signal is added at the transmitter to the message. The received signal is used for synchronization and regenerating the masking signal at the receiver then subtracting it from the received signal to recover the original message. An analog circuit of chaotic double scroll system is described and used to demonstrate possible approach to private communication based on synchronized chaotic system and high sensitivity to initial conditions.

المستخلص

الرسائل المقنعة باستخدام تجاذب المدرجة المضاعفة في الاتصالات الخاصة تم إيضاحها باستخدام محاكاة الكمبيوتر ومن خلال نظام حركي فوضوي ناتج من هزاز المدرجة المضاعفة. يضاف قناع من إشارة فوضوية إلى الرسالة عند المرسل. الإشارة المستلمة تستخدم من أجل التزامن مع المرسل ومن أجل إعادة توليد إشارة القناع الفوضوي في المستلمة لكي يتم طرحه من الإشارة المستلمة لاستعيد الرسالة الأصلية. تم وصف دائرة كهربائية تناظرية لتوليد إشارة المدرجة المضاعفة الفوضوية ومن ثم استخدامها في الاتصالات الخاصة اعتماداً على خاصية التزامن بين الأنظمة الفوضوية وعلى الحساسية العالية للشروط الابتدائية للعمل.

Introduction

One of the most exciting recent developments in nonlinear dynamics is the realization that chaos can be useful. It is effectively unpredictable long-term behavior in deterministic system that exhibits sensitive dependence on initial conditions with noise like spectrum. Normally one thinks of chaos as fascinating curiosity at best and a nuisance at worst, something to be avoided or engineered away. But since about 1990, people have found ways to exploit chaos to do some marvelous and practical things [1,2]. One application involves *private communications* for any modulation type. Suppose you want to send a secret message to a friend or business partner. Naturally you should use a code, so that even if an enemy is eavesdropping, he will have trouble making sense of the message. This is an old problem, people have been making (and breaking) codes for as long as there have been secrets worth keeping.

Pecora and Carroll [3,4,5] reported that certain chaotic systems possess a self-synchronization property if they can be decomposed into subsystems, a drive system and a stable response subsystem and coupled with common drive signal. They showed numerically that robust synchronization occurs starting from any initial conditions if all of the Lyapunov

⁺ Received on 5/8/2004 , Accepted on 8/12/2004

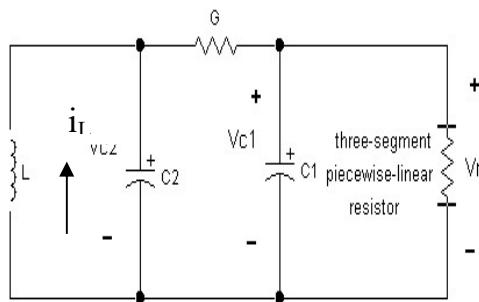
* Assit. Lacturer / Technical Colleg - Basrsh

exponents for the response subsystems are negative. Chua and Gui [6,7] found that a chaotic attractor with a macroscopic *double-scroll* structure is observed from an extremely simple autonomous electrical circuit with only one nonlinear element. Grebogi and Ott [8] discovered that the chaos could be used to transmit information. They used an electrical oscillators (*Chua's circuit*) with very simple structures to produce complex waveforms. These waveforms can be used to follow a desired symbol sequence by using small perturbations, thus allowing us to encode a message on it. Cuomo and Oppenheim [1] described an analog circuit implementation of the synchronized chaotic Lorenz system to demonstrate two possible approaches of secret communications.

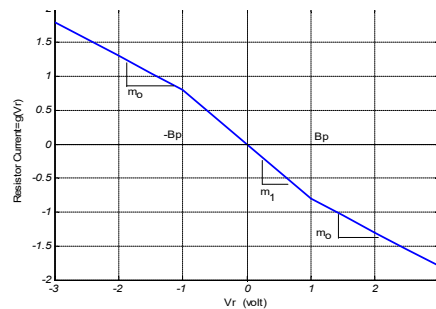
This paper is organized as follows, the next section describes the double scroll oscillator and its characteristics. In section 3, the message masking processes in transmitter and receiver are applied and in section 4 simulation results are given. Finally, some conclusions and recommendations are drawn from this paper.

The Double Scroll Attractor

The double scroll attractor [6,7,8] has been observed in the oscillator circuit of Fig. (1-a), whose only nonlinear element is a three-segment piecewise-linear resistor with $v-i$ characteristics as shown in Fig. (1-b).



(a) Electrical schematic



(b) Characteristics of piecewise-linear resistor

Fig.(1): Chua's circuit (double scroll oscillator)

The dynamics of Chua's circuit (double scroll oscillator with more details in [6,7]) are described by:

$$\begin{aligned} C_1 (dV_{C1}/dt) &= G (V_{C2} - V_{C1}) - g(V_{C1}) \\ C_2 (dV_{C2}/dt) &= G (V_{C1} - V_{C2}) + i_L \\ L (di_L/dt) &= -V_{C2} \end{aligned} \quad \dots \dots \dots (1)$$

where G is the conductance in Fig.(1-a)

m_o, m_1 are the slope of line segments and Bp is the breakpoint in Fig.(1-b)

$g(V_{C1})$ is the piecewise-linear function in Fig.(1-b), defined by[6] as:

$$g(V_{C1}) = m_o V_{C1} + 0.5 (m_1 - m_o) | V_{C1} + Bp | + 0.5 (m_o - m_1) | V_{C1} - Bp | \quad \dots \dots \dots (2)$$

A computer simulation program (MATLAB 6.5 with signal processing toolbox / ODE23) is written to solve equation (1). With $C_1 = 1/9$, $C_2 = 1$, $L = 1/7$, $G = 0.7$, $Bp = 1$, $m_o = -0.5$, $m_1 = -0.8$ the well known double scroll attractor will be produced as shown in Fig.(2) with initial conditions: $V_{C1}(0) = 0.15264$, $V_{C2}(0) = -0.02281$, $i_L(0) = 0.3812$. Fig.(2-a) represent

the projection on (V_{C1}, V_{C2}) plan , Fig.(2-b) represents the projection on (i_L, V_{C1}) plan, Fig. (2-c) represents the time waveform of $V_{C1}(t)$ and Fig.(2-d) represent the average power spectrum of $V_{C1}(t)$.

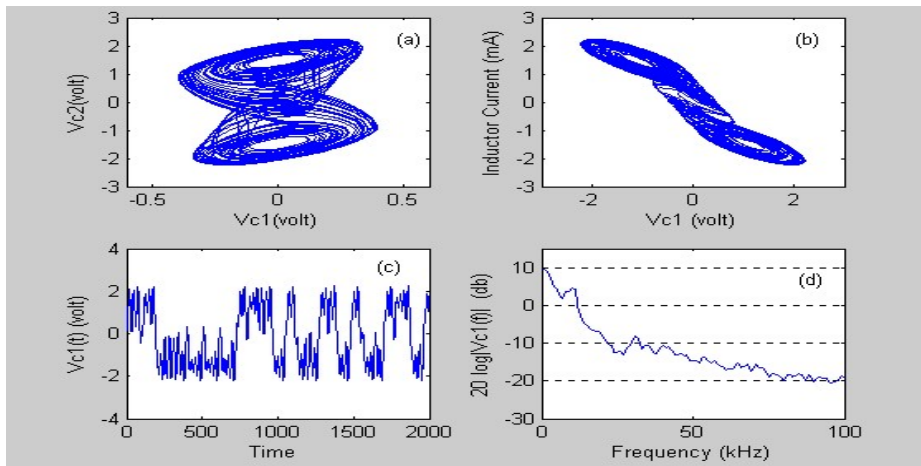


Fig.(2): Double scroll computer simulation

- (a) Attractor projection on (V_{C1}, V_{C2}) plan (b) Attractor projection on (i_L, V_{C1}) plan
(c) Waveform of $V_{C1}(t)$ (d) The average power spectrum of $V_{C1}(t)$

Using EWB 5.12 program, the physical circuit realization of equation (1) is given by [6] in Fig.(3) where the piecewise-linear resistor is replaced by (741 Op-Amp , two diodes, two 3.3 k Ohm resistors, two 46.2 k Ohm resistors, two 300 Ohm resistors, 1.25 k Ohm resistor , +15 dc power supply and -15 dc power supply) to realize the function $g(V_{C1} = V_R)$ in Fig.(1-b) . The appropriate components scaling values of $C_1=0.0055 \mu F$, $C_2=0.05 \mu F$, $L=8.2 \text{ mH}$ and $R=1/G=1.33 \text{ k Ohm}$ are used in the analog circuit to obtain the same results of MATLAB simulation in Fig.(2), So that, we will continue with the MATLAB simulations only for the next sections.

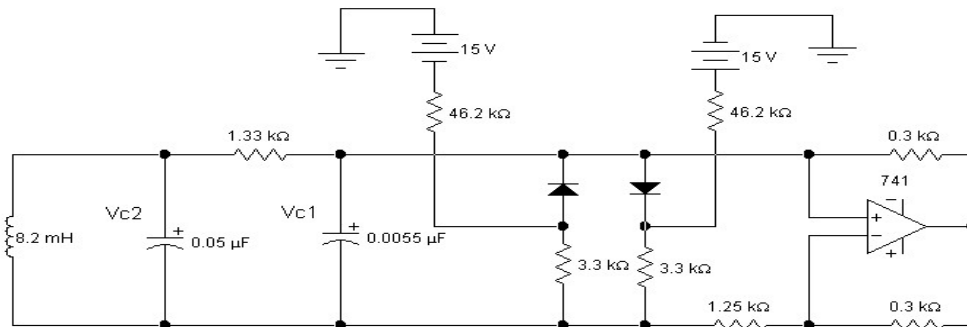


Fig. (3): Electrical circuit realization of equation (1) - double scroll oscillator

Transmitting and Receiving of Masked Messages

Many people asked : How can you make a message masking in the transmitter and then remove this mask completely in the receiver to insure private communication?

The answer is, numerical simulations are performed on the double scroll oscillator given before and here's the strategy of building on *synchronized chaos* discovery and high chaos

sensitivity to *initial conditions*: mask your message with much louder chaotic signal then send it to your partner.

The outside listener (enemy) only hears (receives) the chaos sound (signal) which is like static on the radio (meaningless noise). But if your partner has a special receiver which perfectly reproduces the chaotic mask then he can listen to the message by subtracting the mask signal.

Let us define new variables for simplicity:

$$x = Vc_1 \quad , \quad y = Vc_2 \quad , \quad z = i_L$$

Then the system of equation (1) becomes:

$$\begin{aligned} dx/dt &= (G / C_1)(y - x) - (1 / C_1) g(x) \\ dy/dt &= (G / C_2)(x - y) + z/C_2 \\ dz/dt &= -y/L \end{aligned} \quad \dots\dots\dots (3)$$

This system, which we refer to as the transmitter, can be implemented with an electronic circuit or simulated as in Fig. (3) using EWB program for example.

The proposed communication system is given in Fig. (4). The receiver system is identical to the transmitter and synchronizes (more details in [1,4] for *chaotic systems synchronization*) with it by the drive signal $x(t)$ which is used to regenerate the full-dimensional dynamics of the double scroll system.

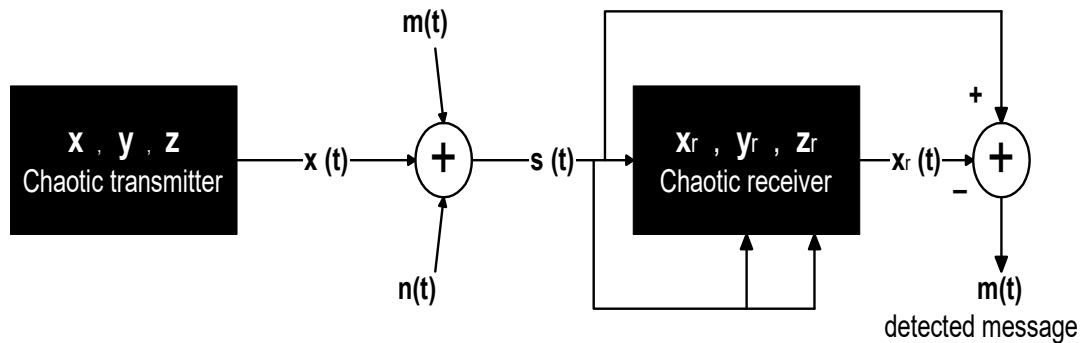


Fig. (4): Communication system using chaotic message masking

In this system a chaotic signal which is generated at the transmitter $x(t)$ is added to the information-bearing signal $m(t)$, assuming that the power level of $x(t) \gg m(t)$. The transmitted signal then is given by:

$$s(t) = x(t) + m(t) + n(t) \quad \dots\dots\dots (4)$$

where $n(t)$ is the AWGN noise that is coming from the channel (two wire channel in this case).

The dynamical system of the receiver is :

$$\begin{aligned} dx_r/dt &= (G/C_1)(y_r - x_r) - (1/C_1)g(x_r) \\ dy_r/dt &= (G/C_2)(s - y_r) + z_r/C_2 \dots\dots\dots (5) \\ dz_r/dt &= -y_r/L \end{aligned}$$

If the receiver has synchronized with $s(t)$ as the drive, then $x_r(t)$ is approximately equal to $x(t)$ and consequently $m(t)$ is recovered as:

$$\hat{m}(t) = s(t) - x_r(t) \dots\dots\dots (6)$$

where $\hat{m}(t)$ is the original message with a little noise that is assumed to become from the channel.

Simulation Results

To illustrate the system performance with the help of MATLAB program, a wave file containing a segment of speech (BESM ALLAH AL-RAHMAN AL - RAHEEM بسم الله الرحمن الرحيم) is taken to be used as a message $m(t)$ with 30000 sample, 16 bit resolution and sampling frequency of 11025Hz. Fig.(5-a) represents the original message while Fig.(5-b) is the chaotic signal $x(t)$. The noise power of -30 dB will be added to the transmitted signal $s(t)$ from the channel. The transmitted signal $s(t)$ is shown in Fig.(5-c) which has very slight difference from $x(t)$ because of the high chaos power compared with the message power (by experiments we take the minimum case $x(t) = 8 m(t)$, about 18 dB), we see clearly that the signal is completely buried underneath and the chaos sound is the only output from the speakers. The unmasked message at the receiver is shown in Fig.(5-d) where the original copy of speech is recovered with only a tiny amount of distortion (most visible as the increased noise on the flat parts of the speech).

We assume through this simulation that the input of the receiver is $s(t)$ given in equation (4) without any other factor from the channel.

The people who saw this experiment heard the original message, masked message and recovered message and all of them did believe that any message is there in the masked version, also all of them became very happy when they heard the recovered version despite the tiny noise (-40 dB after simple LPF used in the receiver).

In Fig(6-a) the state space of two components of the receiver system is plotted ($z_r(t)$ against $x_r(t)$), it has a little distortion compared with Fig.(2-b) coming from the message embedding in to chaotic attractor (not that this distortion depends on the power of $x(t)$ and $m(t)$ and becomes very little for high chaos power) as shown in Fig.(6-b) for this experiment. Fig.(6-c & 6-d) plots the receiver variables $x_r(t)$ and $y_r(t)$ against their transmitter counterparts $x(t)$ and $y(t)$.

The line slope of 45° indicates that the synchronization (which is proved in [1,4]) is nearly perfect and also quite stable as the initial conditions $V_{C1}(0)=0.15264$, $V_{C2}(0)= - 0.02281$ and $i_L(0)= 0.38127$ of both transmitter and receiver are the same. The line in Fig.(6-c) has a thickness more than in Fig.(6-d) because of the message amplitude. Our results are completely similar to results of Cuomo and Oppenheim in [1] where the Lorenz attractor is used.

For a difference of about 1×10^{-12} in initial conditions between the transmitter and receiver systems, decorrelation will happen in few milliseconds and then there is no recovered message at the receiver as shown in Fig.(7-a) but a chaotic signal will be received as in Fig.(7-b). Fig.(7-c & 7-d) indicates that no synchronization for this system because of initial conditions of difference.

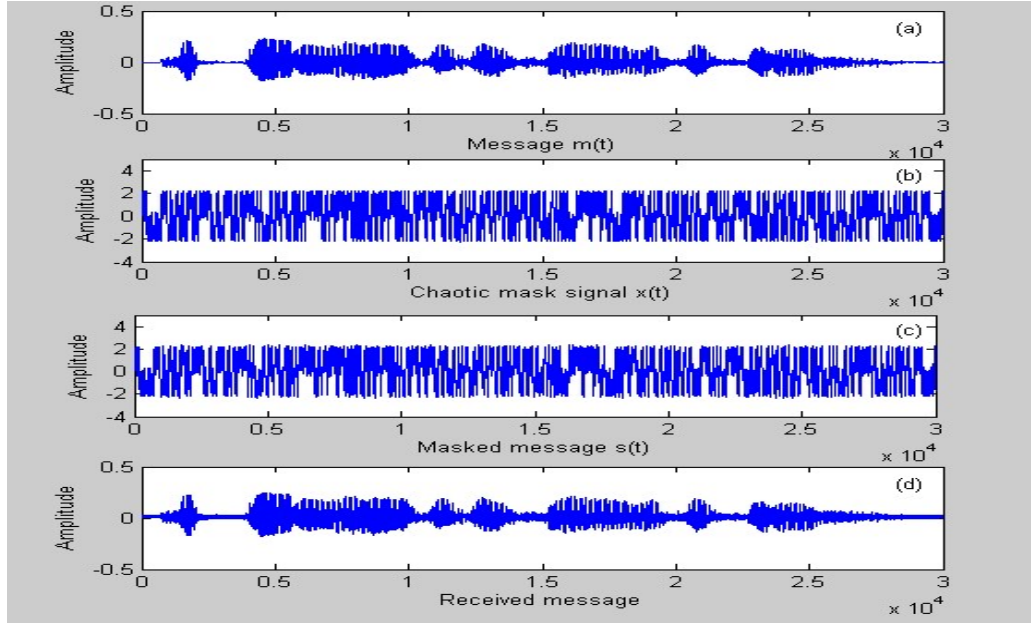


Fig. (5): Data of synchronized communication system using chaotic message masking: (a) Original speech signal (b) Chaos mask (c) Masked message (d) Received message

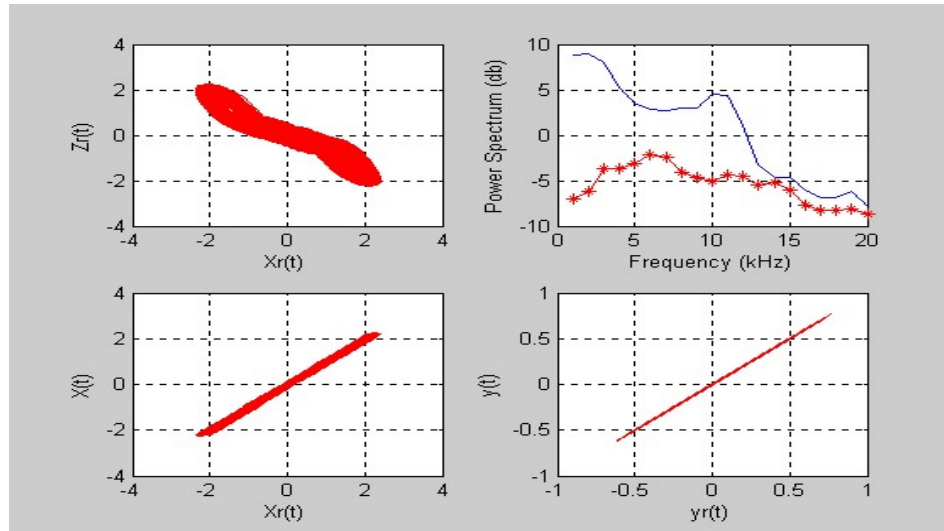


Fig.(6): Data of synchronized communication system using chaotic message masking: (a)Receiver state space (b) Power spectrum of the speech message and the chaos (c) Transmitter and receiver signals $x(t)$ carrying message verses $x_r(t)$ (d) Transmitter and receiver signals $y(t)$ verses $y_r(t)$

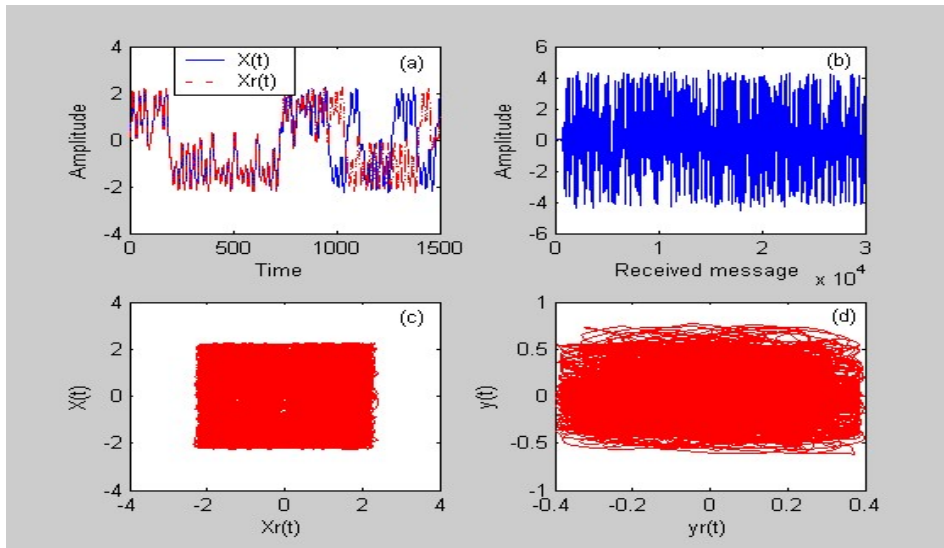


Fig.(7): Data of unsynchronized communication system using chaotic message masking
(a) Signals of $x(t)$ and $x_r(t)$ for i.c. difference of 1×10^{-12} (b) Received message (only Chaos)
(c) Transmitter and receiver signals $x(t)$ carrying message verses $x_r(t)$
(d) Transmitter and receiver signals $y(t)$ verses $y_r(t)$

Conclusions

One can use the chaos, which is very sensitive to initial conditions and has robust synchronization property to build a secret communication system with identical transmitter and receiver circuits and same password (initial conditions).

There is no way to lose your messages if any one tries to steal only and only if you gave him the password. Good results are obtained from the simulation figures and the wave sounds files using the double scroll oscillator.

Two-wire channel is used for simplicity. Perfect synchronization between the transmitter and receiver is achieved as it is proved by Cuomo and Oppenheim. Reduction of -10 dB in noise power is achieved by the use of simple LPF in the receiver.

As a result of 18-dB difference between the mask and message power level we have a good system performance.

Our recommendation is to use the double hook oscillator in another research.

References

- 1- Steven H. Strogatz. *Nonlinear Dynamics and Chaos with Applications to Physics, Biology, Chemistry, and Engineering*. Addison-Wesley Publishing Company, second printing, November , 1995.
- 2- Waleed A. Al-Hussaibi, " Effects of Low Pass Filtering on Chaotic Signals of Boost Switching Regulators ", *The 8'Th Scientific Conference for Foundation of Technical Education*, pp. 69-75 , 2002.
- 3- L. M. Pecora and T. L. Carroll, " Synchronization in Chaotic Systems " , *Physical Review Letters*, Vol. 64, pp. 821-824 , 1990.
- 4- Pecora. L. M and Carroll. T. L, " Self Synchronization in Chaotic Systems by Decomposition " , *Physical Review Letters*, Vol. A 44, pp. 2374-2378 , 1991.
- 5- Pecora. L. M and Carroll.T. L , " Circuit Implementation of Synchronized Chaos with Application to Communication " , *Physical Review Letters*, Vol. 71, pp. 65-72, 1993.
- 6- Leon O. Chua and Gui-Nian Lin, " Canonical Realization of Chua's Circuit Family " , *IEEE Transaction. Circuits and Systems*, Vol. 37 , pp. 885-902 , July 1990.
- 7- Leon O. Chua and Gui-Nian Lin, " Intermittency in a Piecewise – Linear Circuit " , *IEEE Transaction., Circuits and Systems*, Vol. 38 , pp. 510-520 , 1991.
- 8- Celso Grebogi and Edward Ott, " Communicating with Chaos " , *Physical Review Letters*, Vol. 70, pp. 3031-3035, 1993.