Available online at www.elixirpublishers.com (Elixir International Journal)

Computer Science and Engineering

Elixir Comp. Sci. & Engg. 38 (2011) 4496-4499

Elixir ISSN: 2229-712X

Secure chaotic modulation schemes using henon map

Dikshith Anchan and K.L.Sudha

Department of DSCE, Bengaluru.

ARTICLE INFO

Article history:
Received: 22 August 2011;
Received in revised form:
26 August 2011;
Accepted: 31 August 2011;

Keywords
Secure communication,
Chaos,
Nonlinear system,
Chaotic attractor.

ABSTRACT

Future communication should operate at higher data rates, be more reliable, and operate in increasingly crowded frequency allocations. New technologies are being tried in this direction and chaotic communication is one among them. Equivalently, chaotic signals decorrelate rapidly with themselves. The autocorrelation function of a chaotic signal has a large peak at zero and decays rapidly. Same random sequence can be obtained provided we know the exact initial condition for the process. The nonlinear, unstable and aperiodic characteristic of chaotic signals has numerous features that make it attractive for communication use. Chaotic communication is rather a new field in communication research. During the past 15 years, there has been a tremendous interest worldwide in possibility of exploiting chaos in wideband communication system. In this direction already 4 generations of chaotic communication is evolved. In this project we have implemented five different types of chaotic modulation. Demodulation is either coherent or non coherent, based on the type of modulation. For coherent demodulation we used correlator receiver and adaptive filter receiver. We have made a comparison among different types of modulation techniques.

Introduction

Chaos is a random process found in non-linear, dynamical system. Chaotic systems are characterized by "sensitive dependence on initial conditions"; a small perturbation eventually causes a large change in the state of the system. Chaotic signals have wideband power spectrum, but in the time domain, they appear "random". Thus these signals are irregular, aperiodic, uncorrelated, broadband signals which can be generated using nonlinear equations. Chaotic waveforms can be generated by very simple circuits in any frequency band and at arbitrarily power levels. Conventional modulation techniques use periodic sinusoidal signals as carriers and hence these signals are more prone to fading. Chaotic modulation schemes are evolved as a solution to this problem. In chaotic communication the digital bits or symbols are mapped onto sample functions of chaotic signals derived from chaotic attractors. To avoid periodicity, the symbols are mapped to the actual unstable, aperiodic signal outputs of chaotic circuits and not to parameters of certain known sample functions. The key difference between a conventional carrier and a chaotic carrier is that the sample function for a given symbol is unstable, aperiodic and is different from one symbol interval to the next [1]. As a result, the transmitted waveform is never the same, even if the same symbol is transmitted again and again. Because the cross correlations between pieces of chaotic waveforms are much lower than between pieces of periodic waveforms, chaotic modulation has an inherent insensitivity to multipath propagation. The output of the chaotic modulator is a wideband signal as in spread spectrum signal but there is no need of spreading and despreading processes requiring synchronization.

In chaotic modulation schemes, the digital information to be transmitted is placed directly onto a wide-band chaotic signal. Here, the nonlinear characteristic of communication devices are utilized instead of being avoided, this eliminates the complicated measures to maintain linearity. As a result, chaotic communication systems can function over a larger dynamical range, with fewer complex components and operate at higher power levels than traditional communication systems. Also Giga bits of data can be transmitted with chaotic modulation [2]. It is easier to generate strong, high-power chaotic signals than periodic signals. Chaotic signals are sensitive to initial conditions and have a noise like time series. As a result, chaotic transmissions have less risk of interception and are hard to detect by eaves droppers.

This paper is based on the project in which we have implemented 5 different types of chaotic modulation schemes and successfully demodulated them. They are Chaos Shift Keying (CSK), Differential Chaos Shift Keying (DSK), Additive Chaos Modulation (ACM), chaos on off keying (COOK) and Chaotic Pulse Position Modulation schemes. These are the modulation schemes selected from different generations. We have discussed in detail about these modulation schemes and compared their performances.

Chaotic theory:

Chaos is a deterministic, random-like process found in non-linear, dynamical system, which is non-periodic, non-converging and bounded. Chaotic dynamical system is one that is deterministic but appears not to be so as a consequence to its extreme sensitivity to initial conditions.[3][4] A chaotic system can be described by state space equations

$$x_{n+1}=f(x_n), \qquad n=0,1,2,3\ldots\ldots \qquad (1)$$

Chaos does not require complex equations. It can be produced by very simple ones. Consider a simple equation cx^2-1, where c is a real valued constant. Now, by iterating this equation on x, varying results can be obtained, some displaying chaos. Iterating on x means taking some starting value of x = x0, then keep putting the value of the equation back into itself, such that:

$$x_{n+1} = cx_{n2}-1 \qquad (2)$$

Tele:
E-mail addresses:

Referring to the above equation, values of c of about 1.5 and above appear to cause chaos, with the larger c, the more chaotic. Wikipedia lists around 56 different types of chaotic maps.

The Henon map is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit chaotic behaviour. The Henon map takes a point (x_n, y_n) in the plane and maps it to a new point.

$$x_{n+1} = y_n + 1 - ax_n^2,$$
$$y_{n+1} = bx_n. \qquad (3)$$

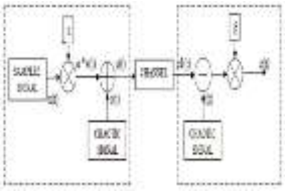
The map depends on two parameters, *a* and *b*, for which the canonical Henon map have values a = 1.4 and *b* = 0.3. For the canonical values the Henon map is chaotic. For other values of *a* and *b* the map may be chaotic, intermittent, or converge to a periodic orbit. An overview of the type of behaviour of the map at different parameter values may be obtained from its orbit diagram. The map was introduced by Michel Henon as a simplified model of the Poincare section of the Lorenz model. For the canonical map, an initial point of the plane will either approach a set of points known as the Henon strange attractor, or diverge to infinity. The Henon attractor is a fractal, smooth in one direction and a Cantor set in another.

Chaotic modulation schemes:

There are different chaotic modulation schemes suggested by research community in the last decade and four generations of chaotic communication have been reported.[3] The first generation was developed in 1993 known as *additive chaos masking* and *chaotic shift keying(CSK)*. The second generation was proposed during1993 to 1995 known as *chaotic modulation*. This generation used two different ways to modulate message signals into chaotic carriers. The first method called *chaotic parameter modulation* used message signals to change parameters of the chaotic transmitter. The second method called *chaotic non-autonomous modulation* used the message signal to change the phase space of the chaotic transmitter. The third generation was proposed in 1997 for the purpose of improving the degree of security to a much higher level than the first two generations. This generation is known as *chaotic cryptosystem*. In this generation, the combination of the classical cryptographic technique and chaotic synchronization is used to enhance the degree of security. In 1997 a brand new chaotic synchronization technology called impulsive synchronization was invented based on impulsive control theory. By applying impulsive synchronization, the fourth generation of chaotic secure communication system was presented.

Additive chaos masking (ACM):

In Additive chaos masking the message signal is added to the chaotic signal giving the transmitted signal. The chaotic system at the receiver end produces another copy of the chaotic signal which is subtracted from the transmitted signal to obtain the recovered message signal. For higher security of the message signal, Yang reported that the message signal is typically made about 10 to 100 times weaker than the chaotic signal [3].



Modulation Demodulation

Fig. 1 ACM Modulator and Demodulator

Modulated output can be expressed as

*y(t)=c(t)+α *x(t)* (4)

Where c(t)- chaotic signal x(t)- sampled input signal and α - scaling factor. Demodulated output can be otained by subtracting the chaotic signal from the received signal.

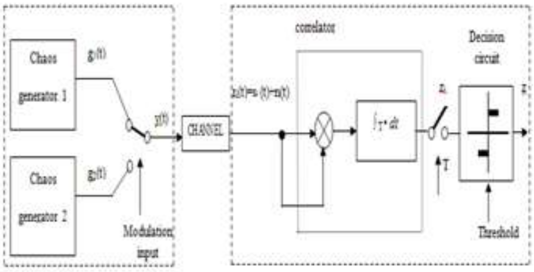
i.e. *z(t)=β *(z1(t)-c(t))* (5)

where *z1(t)=y(t)+n(t), n(t)* - noise signal added in the channel and *β* - scaling factor.

The scaling factor α is multiplied with the input signal x(t) to make it less energetic compared to chaotic signal c(t). Then at the reciever the recovered o/p is again multiplied by a scaling factor β to get back the original input signal.

Chaos Shift Keying

In Chaos Shift Keying (CSK) modulation, chaotic signals carrying different bit energies are used to transmit the binary information [4][1]. Chaotic signals having different bit energies can be generated by different chaotic circuits or they can be produced by the same chaotic circuit if the output is multiplied by two different constants. The demodulator determines the bit energy. Because the information is carried by nonperiodic chaotic signal segments, the received energy per bit appearing at the input of the decision circuit is a random variable, even in the noisefree case. Demodulation is done at the receiving end by measuring the energy over the bit interval and making the decision. The major disadvantage of the CSK system is the threshold level required by the decision circuit depends on the SNR.



Modulation Demodulation

Fig. 2. CSK Modulator and Demodulator

CSK Modulation for M-ary signaling can be described mathematically as

$$y(t) = \begin{cases} g1(t), & if \quad m(t) = m1 \\ g2(t), & if \quad m(t) = m2 \\ \dots\dots\dots \quad \dots\dots\dots & \dots\dots\dots \quad \dots\dots\dots \\ \dots\dots\dots \quad \dots\dots\dots & \dots\dots\dots \quad \dots\dots\dots \\ gn(t), & if \quad m(t) = mn \end{cases}$$

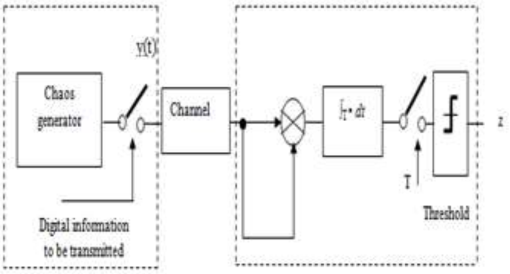
Demodulated signal can be obtained by squaring the received signal as given below

$$z = \int_T r_i^2(t)\,dt = \int_T [s_i(t) + n(t)]^2\,dt \qquad (6)$$

$$= \int_T s_i^2(t)\,dt + 2\int_T s_i(t)\,n(t)\,dt + \int_T n^2(t)\,dt$$

Chaotic On-Off-Keying

In *Chaotic On-Off-Keying* (COOK), the chaotic signal in the modulator is switched off and on according to symbols ‘0’ and ‘1’ respectively. The noise performance of the COOK scheme is superior compared to CSK because the distance between the elements of the signal set is greater than that with CSK. The threshold level in COOK is also dependent on SNR.[1]



Modulation Demodulation

Fig 3. COOK Modulator and Demodulator

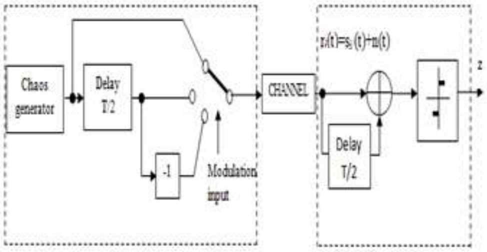
$$y(t) = \begin{cases} 0, & if \quad m(t) = m1 \\ x(t), & if \quad m(t) = m2 \end{cases}$$

$$z = \int_T r_i^2 (t)\, dt = \int_T [s_i (t) + n(t)]^2\, dt$$

$$= \int_T s_i^2 (t)\, dt + 2 \int_T s_i (t)\, n(t)\, dt + \int_T n^2 (t)\, dt \qquad (7)$$

Differential Chaos Shift Keying:

The basic idea of DCSK [5] is that every information bit to be transmitted is represented by two chaotic sample functions. The first sample function serves as a reference while the second one carries the information. Bit "1" is sent by transmitting a reference signal provided by a chaos generator twice in succession, while for bit "0", the reference chaotic signal is transmitted, followed by an inverted copy of the same signal. The two sample functions are correlated in the receiver. A positive autocorrelation indicates that bit "1" has been received while a negative peak indicates bit "0". Because a differential technique is used, the threshold level required by the decision circuit is zero and is independent of the SNR at the input to the receiver. The distance between the elements of the signal set is maximum, in this case. This is why DCSK and COOK gives the best and second best noise performance respectively. The noise performance of DCSK and COOK is comparable to that of conventional noncoherent modulation techniques.



Modulation Demodulation

Fig. 4. DCSK Modulator and Demodulator

$$s1(t) = \begin{cases} x(t) & t\,k \le t < tk + T/2 \\ + x(t - T/2) & t\,k + T/2 \le n \end{cases}$$

$$s2(t) = \begin{cases} x(t) & t\,k \le t < tk + T/2 \\ - x(t - T/2) & t\,k + T/2 \le n \end{cases}$$

$$z = \int_{T/2} r_i (t)\, r_i (t\text{-}T/2)\, dt$$

$$= \int_{T/2} [s_i (t)\, n(t)]\, [s_i (t) + n(t\text{-}T/2)]\, dt$$

$$= \int_{T/2} [s_i^2 (t) dt + \int_{T/2} s_i (t) [\, n(t) + n(t\text{-}T/2)]\, dt$$

$$+ \int_{T/2} n(t)\, n(t\text{-}T/2)\, dt \qquad (8)$$

Chaotic Pulse Position Modulation system:

In [6], N. F. Rulkov proposed transmission of information with chaotically timed pulse sequences rather than continuous chaotic waveforms. Each pulse has identical shape, but the time delay between them varies chaotically. The information can be encoded in the pulse train by alteration of time position of pulses with respect to chaotic sequence. Since the information about the state of the chaotic system is contained *entirely* in the timing between pulses, the distortions that affect the pulse shape will not significantly influence the detection of information in noisy channel. Fig. 5 and 6 shows the block diagram for CPP modulator and demodulator respectively.

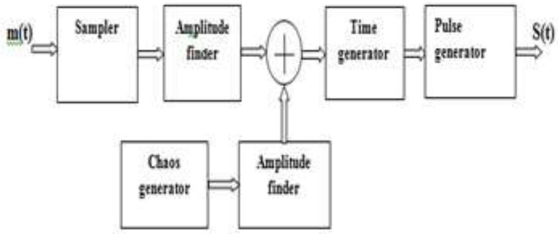


Fig 5. CPP Modulator

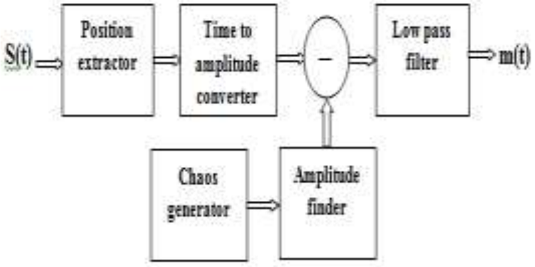


Fig. 6. CPP Demodulator

Simulation Results for Different Modulation Techniques:

In this part we provide MATLAB simulation results for previously discussed chaotic communication techniques such as CSK, COOK, DCSK, ACM & PPM.

ACM:

Here, the message signal is added to the chaotic signal generated with Henon map to get the modulated output. The result is depicted in the Fig.7. It is clear that the output, in no way resembles the input and look like a random signal. This not only makes signal to achieve LPI property but also increases the secrecy in the transmission.

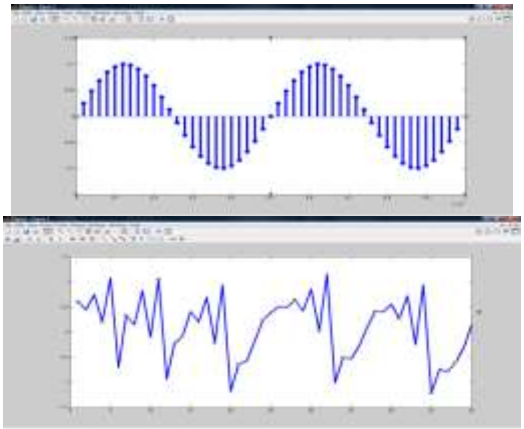
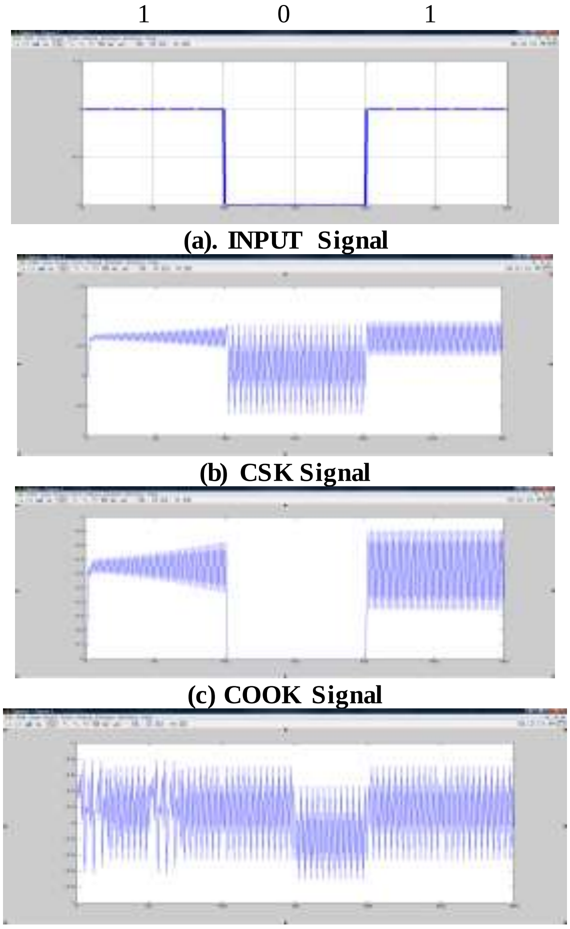


Fig. 7. Sampled Input Signal and ACM output

CSK:

As explained in modulation/demodulation techniques for chaotic shift keying, the bit sequence 0's and 1's are mapped to chaotic signals generated using two different chaotic generators. In our simulation we have used same Henon map with different initial conditions to represent 1 and 0. The result of simulation is depicted in Fig. 8.b. with respect toinput signal shown in Fig. 8.a.



(a). INPUT Signal

(b) CSK Signal

(c) COOK Signal

(d) DCSK Signal

Fig. 8

COOK:

A special case of CSK is the chaotic on off keying (COOK). It uses one chaos generator, which is switched on or off according to a binary message symbol to be transmitted. The bit sequence 0’s and 1’s are mapped to chaotic signal, such that chaos generator is switched on for bit ‘1’ and turned off for bit ‘0’. The result of simulation is depicted in Fig. 8.c.

DCSK:

As explained in modulation/demodulation techniques for differential chaotic shift keying,’1’ is sent by transmitting a reference signal provided by a chaos generator twice in succession, while for bit ‘0’, the reference chaotic signal is transmitted, followed by an inverted copy of the same signal. The result of simulation is depicted in Fig. 8.c.

Secured PPM using Chaos:

In this technique, we first took the samples of the given information signal. Signal with Henon map is generated and sampled. Samples of information signal and chaotic signal are added and time proportional to this amplitude is generated. Pulse generator is used to generate pulses with position determined by the time calculated as above.

At the receiving end, the same chaotic sequence is generated with Henon map for the same initial condition. From the received ppm signal, the position information is extracted and the amplitude proportional to this is generated. Chaotic sample is subtracted to get the original samples. LPF is used to extract the original signal. The result of simulation is depicted in Fig. 9.

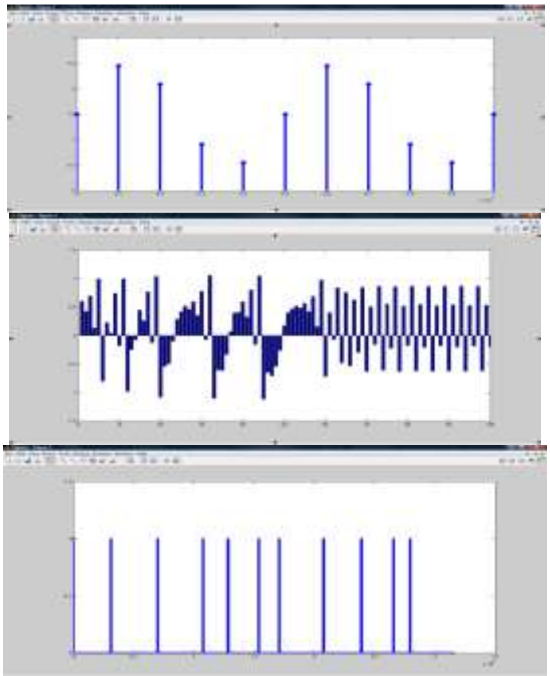


Fig. 9. Sampled Input Signal, Chaotic Signal and CPPM

Conclusion:

Chaotic modulation schemes are gaining importance these days because they inherit the property of randomness and these modulation schemes are more secured compared to conventional modulation systems. In this paper, we have discussed in detail about 5 different types of chaotic modulation schemes ACM, CSK, COOK, DCSK and CPPM. All these modulation schemes are implemented in MATLAB. ACM and CPPM changes some parameters of information signal while in CSK, COOK, DCSK, chaotic waveforms are used as carriers instead of conventional sinusoidal signals. We tested the transmission of these signals through AWGN channel and are able to get back the original signals.

References

[1] *Michael Peter Kennedy Giza Kolumbdn, Gdbor .Kas, and Zoltdn Jdkd* “Recent advances in communicating with chaos” 0-7803-4455-3/98- 1998 IEEE

[2] Anjam Riaz and Maaruf Ali “Chaotic Communications, their Applications and Advantages over Traditional Methods of Communication” 978-1-4244-1876-3/08 ©2008 IEEE Proceedings - 21 - CSNDSP08

[3] Tao Yang, “A survey of chaotic secure communication systems” International Journal of Computational Cognition (http://www.YangSky.com/yangijcc.htm) Volume 2, Number 2, Pages 81–130, June 2004 Publisher Item Identifier S 1542-5908(04)10205-4/$20.00

[4] M. P. Kennedy and H. Dedieu, “Experimental Demonstration of Binary Chaos Shift Keying Using Self-Synchronizing Chua’s Circuits”, in Proc. 1993 NDES,Dresden, pp.67-72

[5] G. Kolumbbn, B. Vizvbi, W. Schwarz, and A. Abel,“Differential chaos shift keying: A robust coding for chaotic communication”, in Proc. 1996 pp 37-92,NDES, Seville.

[6] N. F. Rulkov and A. R. Volkovskii, “Synchronization of pulse-coupled chaotic oscillators,” in *Proceedings of the Second Experimental Chaos Conference*. Singapore: World Scientific, 1993, pp. 106–115.