International Journal of Engineering Research
Volume No.3, Issue No.7, Pp : 458-461
ISSN:2319-6890)(online),2347-5013(print)
01 July 2014

Chaotic Synchronization in Digital Communication

Rahul Ekhande, Sanjay Deshmukh
Department of Electronics & Telecommunication, Rajiv Gandhi Institute of Technology
ekhanderahul76@gmail.com, deshmukhsdrgit@gmail.com

Abstract— Conventional Pseudorandom signals are used for spreading of signals in wireless communication. Due to increase gain of the system the code word length need to increase but due to practical limitation and increase in complexity chaotic signals can be use as alternative to pseudorandom codes for spreading of signals. A signal masking technique based on Lorentz System is presented in this paper which uses Lorentz equation generated Chaotic Signals are used as a encryption signal by which the basic digital modulated signal is mixed at the transmitter system. The scheme recovers the information signal exactly by synchronization at receiver. The mixing property of the implemented scheme investigated by Computer Simulations showing better security performance than that of the conventional method.

Keywords— Chaotic Signals, Lorentz System, Lorentz equation, Synchronization, Lorentz Attractor

I. Introduction

Direct-sequence spread-spectrum transmissions multiply the data being transmitted by a "noise" signal. This noise signal is a pseudorandom sequence of 1 and −1 values, at a frequency much higher than that of the original signal. The resulting signal resembles white noise, like an audio recording of "static". However, this noise-like signal is used to exactly reconstruct the original data at the receiving end, by multiplying it by the same pseudorandom sequence (because $1 \times 1 = 1$, and $-1 \times -1 = 1$). This process, known as "de-spreading", mathematically constitutes a correlation of the transmitted PN sequence with the PN sequence that the receiver already knows the transmitter is using [vii]. The resulting effect of enhancing signal to noise ratio on the channel is called process gain. This effect can be made larger by employing a longer PN sequence and more chips per bit, but physical devices used to generate the PN sequence impose practical limits on attainable processing gain. With the increase in longer PN sequence increases the complexity of the system. A system which uses chaotic signals as an alternative to pseudorandom signals is proposed which shows superiority of chaotic signals over pseudo random signals by simulation analysis [viii].

This paper introduces the design of new system which will be more secure to transmit data is the main aim of this project. Chaotic Signal which are generated by Lorentz Equations are used for encryption of data which makes the transmitted encrypted signal more noise to divert or avoid an attacker to hack the data[i].

II. Material and Methodology

The Lorentz system of differential equations arose from the work of Edward N. Lorentz [i]. He came with three differential equations which produce vast different solutions for small differences in initial conditions, a characteristic as Chaos. The system of differential equations of Lorentz used

$$\dot{x} = -\sigma x + \sigma y \qquad \text{......Eq. 1(a)}$$

$$\dot{y} = rx - y - xz \qquad \text{......Eq. 1(b)}$$

$$\dot{z} = -bz + xy \qquad \text{......Eq. 1(c)}$$

Where σ; r; and b are positive parameters. The Figure1and Figure2 shows the Simulink modelling and the simulation results of the Lorentz Attractor respectively. With sigma=10; r= 28and b=8/5.The series does not form limit cycles nor does it ever reach a steady state. Instead it is an example of deterministic chaos. As with other chaotic system the Lorentz system is sensitive to initial conditions, two initial states no matter how close will diverge, usually sooner rather than later [ii].

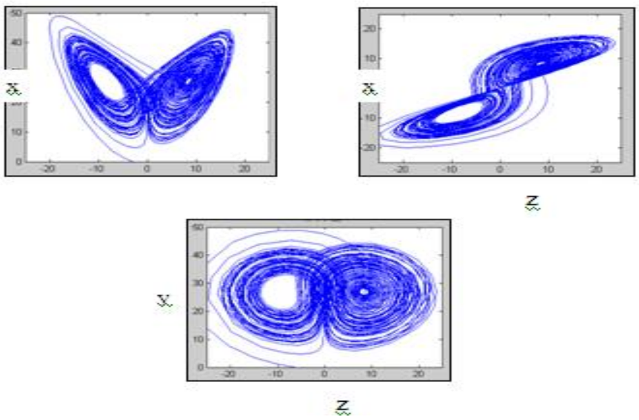

Figure 1. Phase portraits ((a) x-y, (b) x-z, (c) y-z) of the Lorentz Attractor

Block Diagram

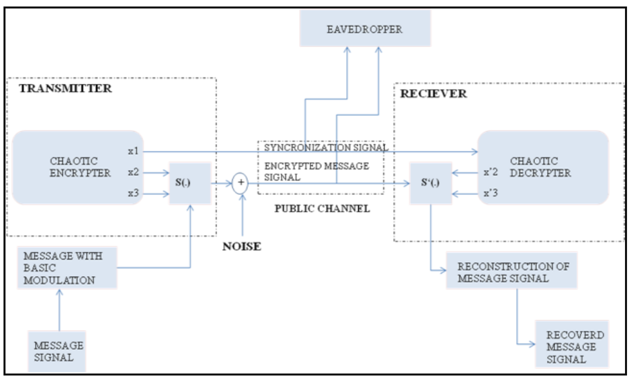

Figure 2. Block Diagram of Chaotic Modulation with Synchronization

Suppose we start with two Lorenz chaotic systems. Then we transmit a signal from the first to the second. Let this signal be the x component of the first system. In the second system everywhere we see an x component we replace it with the signal from the first system. We call this construction complete replacement. This gives us a new five dimensional compound system where we have used subscripts to label each system.

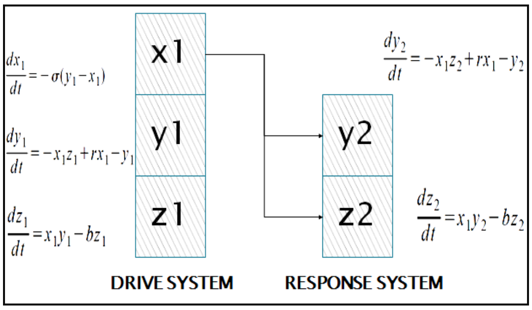

Figure 5. Drive Signal of Driver System driving the Response System

Note that we have replaced x_2 by x_1 in the second set of equations and eliminated the $x^{\cdot}_1$ equation, since it is superfluous. We can think of the x_1 variable as driving the second system. Figure 2 shows this setup schematically. We use this view to label the first system the drive and the second system the response. If we start Eq.(1) from arbitrary initial conditions we will soon see that y converges to y_1 and z_2 converges to z_1 as the systems evolve. After long times the motion causes the two equalities $y_2 = y_1$ and $z_2 = z_1$. The y and z components of both systems stay equal to each other as the system evolves. We now have a set of synchronized, chaotic systems. We refer to this situation as identical synchronization since both (y, z) subsystems are identical, which manifests in the equality of the components. Like paper [iv] the above equations will be implementated in Matlab Simulation shown below to get the exact idea of chaotic signal, its synchronization and potential of being used in communication for secure communication. Along with simulation implementation, chaotic advantages for secure communication will be studied.

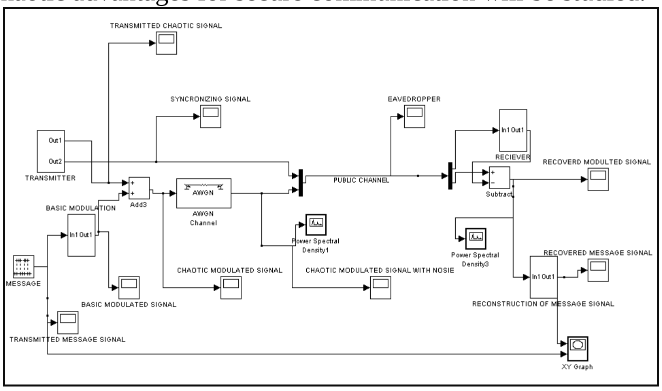

Fig. 4. Implementation of Chaotic Modulation with Identical Synchronization in MATLAB Simulink

III. Results and Tables

The result of above MATLAB simulation is shown below. Fig.5 (a) is the input given to the transmitter, Fig.5 (b) is the output of basic modulation sub block which is the on- off keying of the input message signal. Fig.5(c) is the transmitted chaotic signal used for chaotic modulation. Fig.5 (d) is the synchronizing signal used for synchronizing the receiver.Fig.5 (e) shows the chaotic modulated signal which is then passed through AWGN channel whose output is 5(f). Fig. 5(g) is the signal seen by the intruder or eavesdropper in the public channel. Fig 5(h) is the recovered basic modulated signal after receiver synchronization which is then given to reconstruction of original message signal whose output is shown in Fig 5.(i)

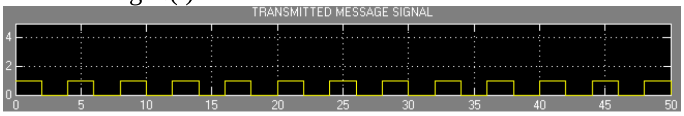

Figure 5. (a) Transmitted Message Signal

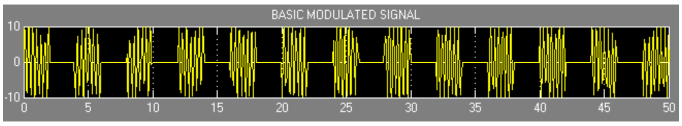

Figure 5. (b) Basic Modulated Signal

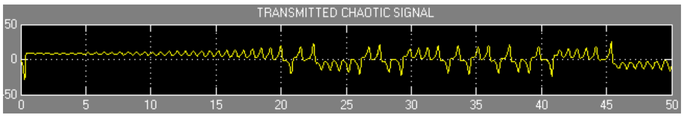

Figure 5. (c) Transmitted Chaotic Signal

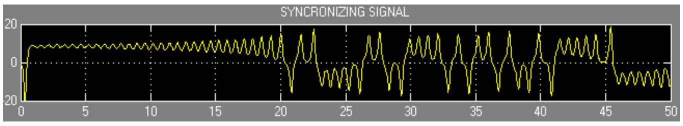

Figure 5. (d) Synchronizing Signal

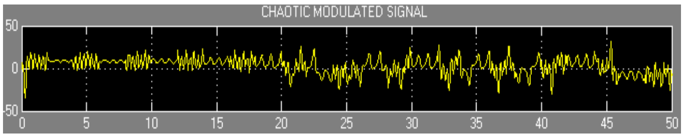

Figure 5. (e) Chaotic Modulated Signal

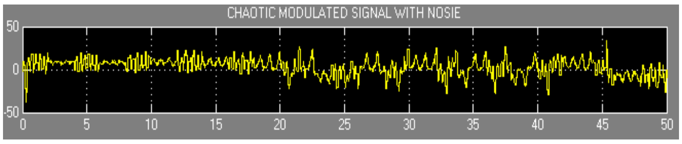

Figure 5. (f) Chaotic Modulated Signal with noise

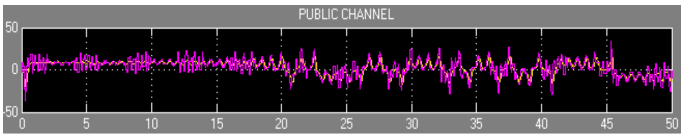

Figure 5. (g) Signal through Public Channel

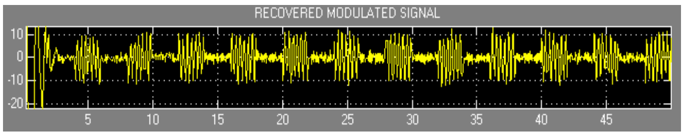

Figure 5. (h) Recovered Modulated Signal

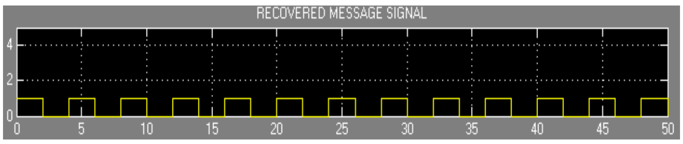

Figure 5. (i) Recovered Message Signal

International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.3, Issue No.7, Pp : 458-461 01 July 2014

Synchronization:

Identical synchronization, also known as Pecora-Carroll synchronization, assumes a specially conditioned pair of chaotic circuits (strongly parameter matched) where the state of the receiver converges asymptotically to the state of the transmitter [xi]. More precisely, given a dynamical system at the transmitter with current state x, x˙ = f(x), and a (nearly) identical replica of this dynamical system with current state x0, x˙0 = f(x0), identical synchronization occurs when

$$\lim_{t\to\infty} ||x'(t) - x(t)|| = 0 \quad \text{......Eq. 2}$$

For any combination of initial states x(0) and x(1)[v]. These synchronization mechanisms rely significantly on underlying circuit and transmission channel assumptions and fail to support robust synchronization as required for practical communications.

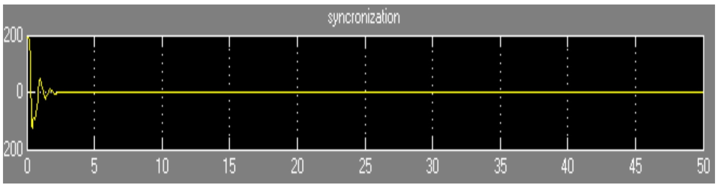

Figure 5. (j) Synchronization of Transmitted & received Signal

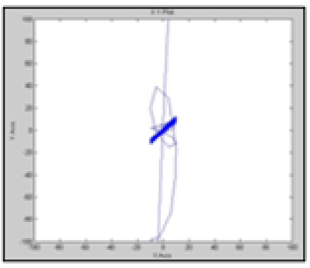
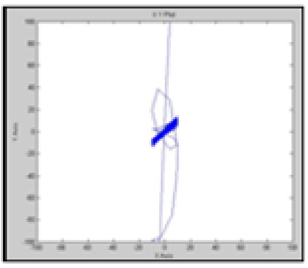

Fig.6. (a) Variance=1 Fig.6. (b) Variance=2

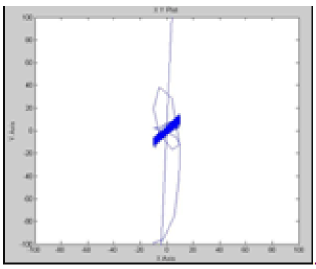
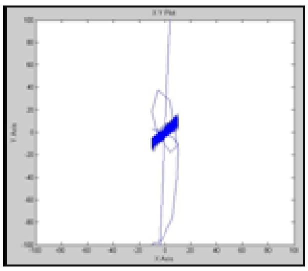

Fig.6. (c) Variance=3 Fig.6. (d) Variance=5

With the increase in AWGN noise the synchronization becomes more complex which varies decision rule complexity at the reconstruction of original signal

BER comparision:

Below figure 7 shows the BER vs. Signal to noise ratio for various modulation schemes, which show the implemented chaotic modulation scheme is better as compare to DPSK, PSK.8 PAM, FSK, and OPQSK for noise level above 10 dB.

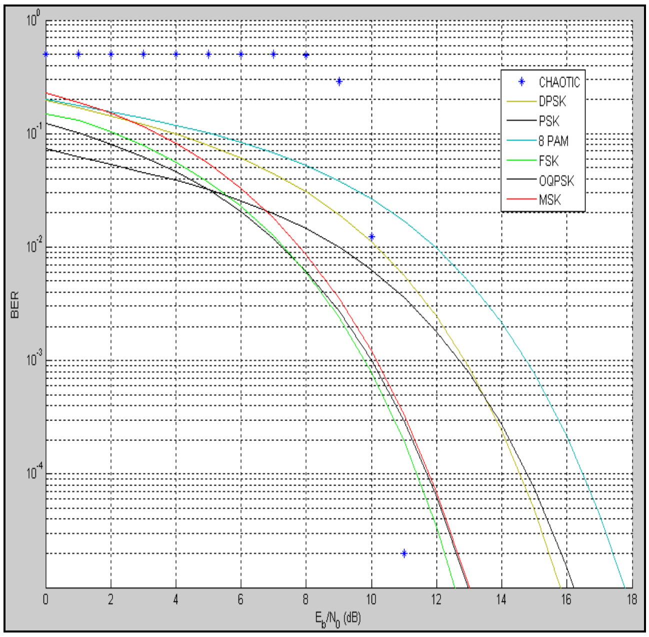

Fig.7. Comparison of BER of Proposed Chaotic Modulation With DPSK, PSK, PAM, FSK &OPQSK

Autocorrelation of chaotic signal and cross correlation of two chaotic signals is shown below in Fig. 7.(a) and (b). The impulse correlation and the wide-broad spectrum fig 7.(c) of chaotic signal makes them perfect for their use in MIMO system is spreading message signal in digital communication[x].

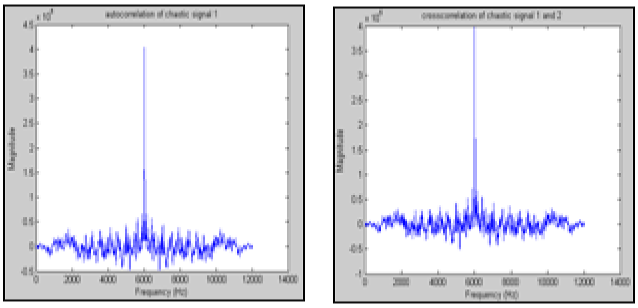

Fig.7. (a) & (b) Autocorrelation and Cross correlation of Chaotic Signals

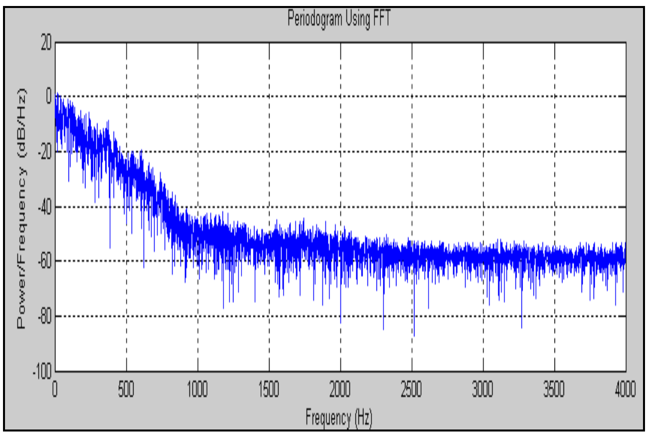

Fig.7. (c) Spread Spectrum of Chaotic Signal

IV. Conclusion

This paper focuses on the Lorentz Attractor's chaotic oscillator circuits and their synchronization used for the applications in signal masking communications. Chaotic signal masking circuits with Identical Synchronization of Transmitter and receiver were realized using Matlab-Simulink and related figures 5(a)-(j) point out that Matlab-Simulink output proves the same conclusions. We have demonstrated in simulations that chaos can be synchronized and applied to secure communications. Figure.5(g) modulated Signal and the synchronizing signal in the public channel appear noisy in nature and makes difficult for eye dropper or hacker to distinguish between the information containing signal and noise, which makes this system more secure .All simulations results performed on Lorentz chaotic system are verified the applicable of secure communication .

Acknowledgement

I would like to thank the respected Dr. Udhav Bhosle and Prof. S. D. Patil for supporting and giving immense guidance.

References

i. *E. N. Lorenz, Deterministic non-periodic flow, J. Atmos. Sci., 20, 130–141, 1963*

ii. *L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems", Phys. Rev. Lett, 64(8):821–5, 1990..*

iii. *Oppenheim, A.V. & Cuomo, K.M. "Chaotic Signals and Signal Processing" Digital Signal Processing Handbook Ed. Vijay K. Madisetti and Douglas B. Williams Boca Raton: CRC Press LLC, 1999*

iv. *Ihsan PEHLIVAN,, Yılmaz UYAROGLU, M. Ali YALÇIN ve Selçuk COSKUN "Design and Simulations of the Arneodo Attractor's Chaotic Oscillator and Signal Masking Circuits", 5th International Advanced Technologies Symposium (IATS'09), May 13-15, 2009, Karabuk, Turkey*

v. *Taejoo Chang, Iickho Song, Jinso Bae, Hong-Gil Kim "Chaotic Signal masking based on Lorentz System"*

vi. *Louis M. Pecora, Thomas L. Carroll, Gregg A. Johnson, and Douglas J. Mar" Fundamentals of synchronization in chaotic systems, concepts, and applications"Received 29 April 1997; accepted for publication 29 September 1997*

vii. *Sneha Venkateswar, Gargi Rajadhyaksha, Jinal Shah "Analysis Of Chaotic Signals As An Alternative To Pseudo-Random Sequences In Ds-Cdma"Canadian Journal on Computing in Mathematics, Natural Sciences, Engineering and Medicine Vol. 4 No. 2, April 2013*

viii. *Nguyen Xuan Quyen, Vu Van Yem, and Thang Manh Hoang, "A Chaos-Based Secure Direct Sequence/Spread-Spectrum Communication System", Hindawi Publishing Corporation Abstract and Applied Analysis Volume 2013, Article ID 764341, 11 pages* http://dx.doi.org/10.1155/2013/764341

ix. *I. Pehlivan and Y.Uyaroğlu, "Simplified chaotic diffusionless Lorentz attractor and its application to secure communication systems", IET Commun., 2007, 1(5):1015-1022, 2007.*

x. *Louis M. Pecora, Thomas L. Carroll, Gregg A. Johnson, and Douglas J. Mar," Fundamentals of synchronization in chaotic systems, concepts,and applications"*