International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

Design Chaotic Security Communication System based on FPGA Technology

Hoang Vu Tran[1], Van Tho Nguyen[2], Thi Bich Hanh Nguyen[3]
[1]The University of Danang - University of Technology and Education, Vietnam;
[2,3]Duy Tan University;

***Abstract*- Chaotic phenomenon have been researching and applications in various fields such as biology, physics, chemistry... With many advantages such as difficult to decipher, simple hardware, easily select band; so far there have been many studies and technical applications chaos in information security, signal modulation ... This paper introduces a communication system using chaos technique, in which the information is added to chaotic signal before sending on the channel. At the receiver, it will synchronize signals and reducing travel chaos to retrieve the information. Because the characteristics of chaotic signals for an eavesdropper would like noise, this solution enhances the security of the system. We have also designed and implemented the FPGA-based communication technology that has been evaluated.**

Keywords- Chaotic; FPGA; Embedded computer; Security

I. INTRODUCTION

Chaotic phenomenon has been known since the late 19th century. Poincare was the first scientist whose observed and made important announcement regarding the status of chaos in nonlinear dynamic systems (Nonlinear Dynamical system) [1]. The publication pointed out that an important feature is the sensitive dependence of chaotic state in the initial condition. In the early 20th century, chaos in electronic circuits was detected specifical
ly in the oscillator to create the carrier of the radio communication system. At that point, chaos is considered a special status should be avoided during circuit design.

In 1963, Lorenz was analyzed the convection of the atmosphere using third-order nonlinear model [2], this analysis indicates that the parameters is defined setting of system stability is not a balance point, and nor is the status that cycle, this time the output signal of the system will diverge and will become not correlated only with very small differences of initial conditions. Is motivated by these results, the chaos status was extended researching in technical subjects as biology, chemistry, physics ... [1] [3] [4]

In the early 1990s, scientists began exploiting nonlinear dynamic and chaos characteristic and for specific applications. In signal processing, chaotic signal and noise with the same frequency band can be isolated using optimization techniques optimized to reduce noise[5] [6], the use of chaos in signal compression also have been researched [7], chaos control technique also have born [8] [9] [10]. A researching by Pecora and Carroll proved that two chaotic systems have the same set of parameter values can synchronized with each other [11]. This result has important implications for the promotion of chaos applied researching into information technology.

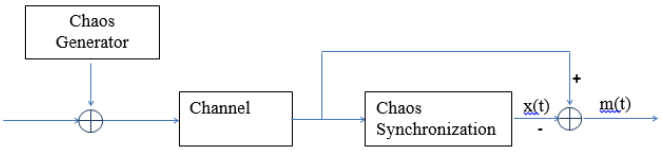
In recent years, the researching of information technology have being developed rapidly. In this information security system applicatons chaos technique, based on the characteristics of sensitive dependence of chaotic status in initial conditions [12][13][14]. The solution modulation/ demodulation technique based on chaos has also been proposed [14] [15] [16] [17].

In this paper, we introduced a communication system based on chaos technique . In this system, the message is mixed with chaotic signals before being posted to the channel. At the receiver, it will take action signals the chaos and reducing it from the received signal to recover the original information. In addition, we also proposed a chaos synchronization algorithm with reliable precision. The Runge-Kutta simulation method to prove the correctness of this solution.

This paper has been organized as follows. In section 2, we describe the security communication system and the problems of current synchronization methods when applying this model. In section 3, we propose a chaos synchronization method using sliding mode controller and analysis of the advantages of our method. Its application to secure-based communication and simulation results are show in section 4. Finally, discussion and conclusion are given in Section 5.

II. MODEL SYSTEM AND SINALS

A. *Mode system*



Figuge 1. Chaos-based Secure Communication System Model

The model of Chaos-based Secure Communication Systems is shown in figuge 1. In this model, the original message m (t) will be added to the chaotic signal x(t) before being taken up channels. Thus the signal on the channel will be:

$$s(t) = m(t) + x_1(t) \quad (1)$$

At the reciever, it have been fully the parameters of chaotic signals, it will conduct synchronized chaotic signal receiver to the transmitter side to get mixed signals in the receiver. Once synced, the system will take the received signal s (t) minus the chaotic signals have been synchronized to restore the original message.

$$m'(t) = s(t) + x_2(t) = m(t) \quad (2)$$

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

This solution enhanced the security features of the system because the message has been mixed in the chaotic signal to noise characteristics as close to an eavesdropper. Suppose that, if there are objects stolen receiver signal s (t) on the channel. Because the characteristics of chaotic signal x1 (t) is no cyclical movement should have characteristics similar to fake noise [2]. An eavesdropper do not have to be tapped by the parameters of the chaotic signal will hardly have the ability to decode the information, which helps the system has high security [12].

However, no cycle characteristics of chaotic signals also cause enormous difficulties in the synchronization signal between the receiver and tranmitter. Therefore, the system can only be viable if solving the problem of synchronized chaotic the system. In this paper, we propose a method of chaos synchronization with satisfactory precision to ensure the the feasibility of the system model.

b.Chaotic Signals

Consider the Lorenz dynamic continuous 3D system is shown by the following difference equation:

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y-x) \\ \frac{dy}{dt} &= x(r-z)-y \\ \frac{dz}{dt} &= xy-bz \end{aligned} \qquad (3)$$

Where x, y, z is the state variables; σ, r, b is the system parameters. With the parameter σ = 10, r = 28, b = 8/3, Lorenz system into a state of chaotic activity.

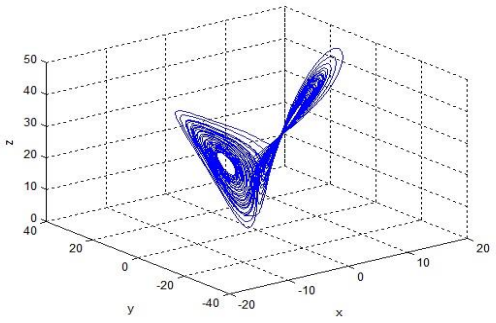


Figure 2: The orbit of the phase on the Lorenz chaotic system

Figure 2 shows the orbit of the phase on the Lorenz chaotic system above. In this figure, we can see clearly that movement system does not cycle, as the time approaches infinity, the line express in phase space do not go to any fixed point or periodic orbit. Besides, this orbit is always remain in a defined domain of phase space and never move out of this area.

Figure 3 shows the components x, y, z of the system with the initial conditions are very small differences (1, 3, 4) and (-1.001, 3, 4). We notice that the system is very sensitive to initial conditions, the trail comes from the initial conditions is different very small (nearly 0) will split very quickly create entirely different orbit.

Although, the Lorenz system is no cyclical movement but it is not a random process. Lorenz chaotic system is a defined system, it is expressed by the equation system with specific parameters, no statistical parameters. We can identify the system at any time t.

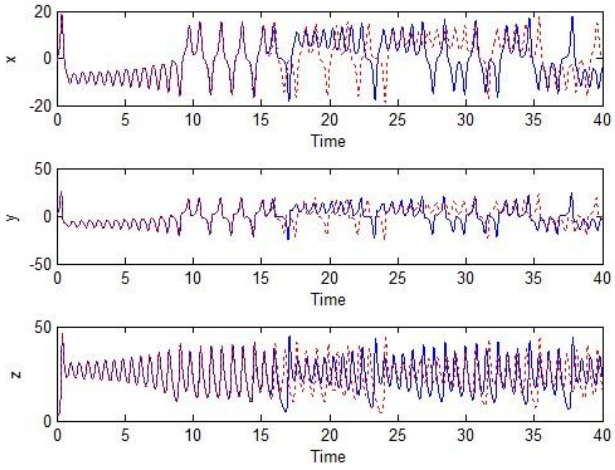


Figure 3: Variable over time of Lorenz chaotic system with the initial conditions are very small differences (-1,3,4) and (-1.001,3,4) và

In the next section, we will present a chaotic synchronization method that can allow for increasing the power of the embedded information signal without affecting the synchronization process.

III. SYSCHRONIZATION

1. *Describe the method*

Consider the Lorenz system includes 1master system and 1 response system are described respectively as follows:

$$\begin{aligned} \frac{dx_1}{dt} &= \sigma(y_1-x_1) \\ \frac{dy_1}{dt} &= rx_1-y_1-x_1z_1 \\ \frac{dz_1}{dt} &= x_1y_1-bz_1 \end{aligned} \qquad (4)$$

$$\begin{aligned} \frac{dx_2}{dt} &= \sigma(y_2-x_2)+u_1 \\ \frac{dy_2}{dt} &= rx_2-y_2-x_2z_2+u_2 \\ \frac{dz_2}{dt} &= x_2y_2-bz_2+u_3 \end{aligned} \qquad (5)$$

In that u_i (i = 1,2,3) are control laws that should be identified to ensure the response system synchronized with master system.

Error between two chaotic systems are defined:

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

$$e_1 = x_2 - x_1$$
$$e_2 = y_2 - y_1 \quad (6)$$
$$e_3 = z_2 - z_1$$

Take the derivative 2 side of the equation (4) we have system error Differential equations as follows:

$$\frac{de_1}{dt} = \sigma(e_2 - e_1) + u_1$$
$$\frac{de_2}{dt} = -e_2 + x_2 z_z - x_1 z_1 + u_2 \quad (7)$$
$$\frac{de_3}{dt} = -re_1 - x_2 y_2 + x_1 y_1 + u_3$$

The task of the control law is to ensure the synchronization between the master system (4) and the response system (5) so that errors (6) towards 0.

Select Control Act:

$$u_1 = -\sigma e_2$$
$$u_2 = -be_1 + x_2 z_2 - x_1 z_1 \quad (8)$$
$$u_3 = -x_2 y_2 + x_1 y_1$$

Get equations (7) minus (8) we have:

$$\frac{de_1}{dt} = -\sigma e_1$$
$$\frac{de_2}{dt} = -e_2 \quad (9)$$
$$\frac{de_3}{dt} = -re_3$$

Equations (9) has a solution $e_1 = e^{-\sigma t}; e_2 = e^{-t}; e_3 = e^{-rt}$

When t towards ∞, the e_1, e_2, e_3 toward 0

Select the Lyapunov function to ensure the stability of the Lorenz chaotic system

$$V(e) = \frac{1}{2}(e_1^2 + e_2^2 + e_3^2) \quad (10)$$

Take the derivative 2sides of the equation (8) we have:

$$\frac{dV(e)}{dt} = e_1 \frac{de_1}{dt} + e_2 \frac{de_2}{dt} + e_3 \frac{de_3}{dt} \quad (11)$$

Substitution (7) to (9) we have: $\frac{dV(e)}{dt} = -ae_1^2 - e_2^2 - re_3^2$ (12)

We found that V(e) is a positive function in R^3 and V '(e) is a negative function in R^3, ie stable system at equilibrium point (0,0,0), according to Lyapunov stable theory [13], we may conclude control law in equation (8) will ensure stability for Lorenz chaotic system

2. Analysy and simulation.

For testing, we conducted simulating synchronous control law above by the Runge-Kutta method with parameters σ = 10, r = 28, b = 8/3 and the initial conditions for the master system was $x_1(0)=1$; $y_1(0)=3$; $z_1(0)=4$, the initial condition for response system was $x_2(0)=12$; $y_2(0)=13$; $z_2(0)=-26$.

The simulation results in Figure 4 shows the response system will synchronize with master system after about 1 seconds, in which x component will sync after about 0.3s (Figure 4.a) and 99.91% accuracy.

Accuracy also be simulated by the formula

$$F = \left(1 - \frac{\frac{1}{N}\sum_{i=1}^{N}(x1_i - x2_i)^2}{\frac{1}{N}\sum_{i=1}^{N}(x1_i)^2}\right) x100$$

where N is the number of samples.

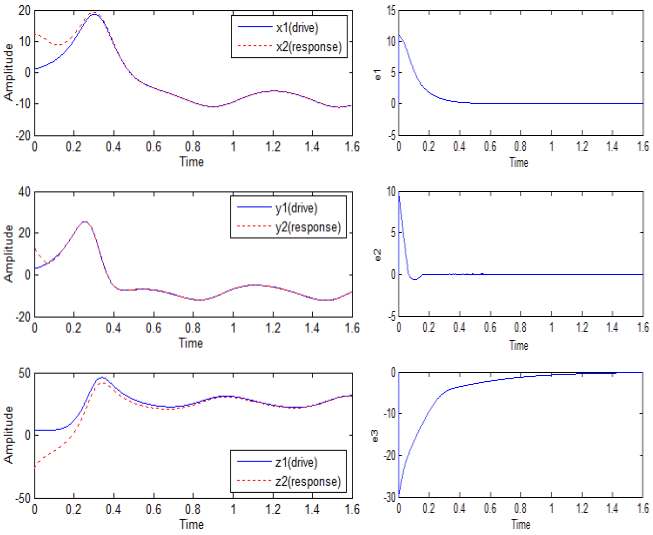


Figure 4.a) Chaos synchronization for all states.
b) Estimated for all state

IV. DESIGN CHAOTIC SECURITY COMMUNICATION SYTEM BASE ON FPGA TECHNOLOGY

Next, we apply this synchronization method to the security communication model described above. In Fig 5, the source signal is the binary bit that is go into the BPSK modulator before being embedded in the chaotic signal. It is then tranmited to the channel. At the receiver, it sync and removal chaotic signals. Then, it is go into the BPSK demodulator to recover binary information.

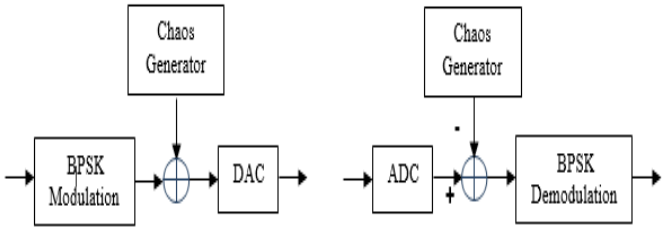


Figure 5. Comunication system model

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 04, April-2019

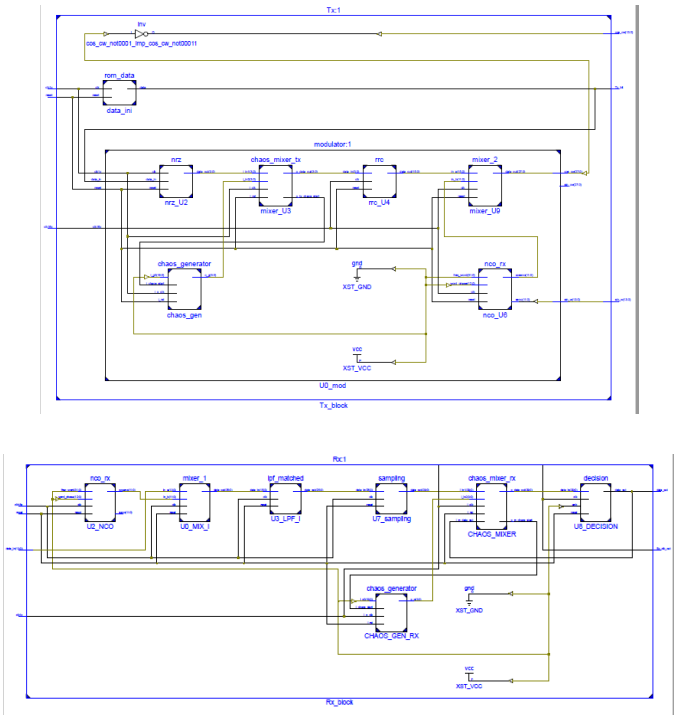


Figure 6. a. Tranmiter schematic b. Receiver schematic

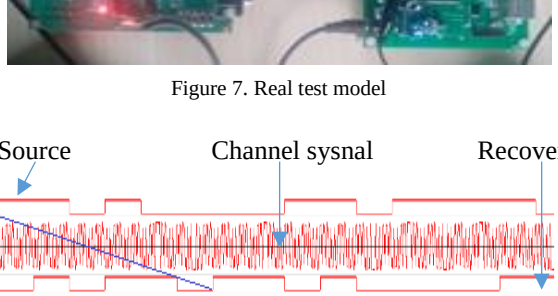


Figure 7. Real test model

Figure 8 . Measurement results on oscilloscope

Transmitters and receivers are designed and implemented based on FPGA technology. Figure 6.a is the transmitter block diagram, Figure 6.b is the receiver block diagram. We used an FPGA-embedded computer [19] that we designed to implement the test. Figure 7 is the actual image deployed

The test results are shown in Figure 8. The measurement results on osciloscope show that the receiver has been decoded correctly.

V. CONCLUSIONS

In this paper introduced and demonstrated the feasibility of information systems applications chaos technology to strengthen security capabilities. We also presented a chaotic synchronization method with satisfactory accuracy to provide the ability to recover the original signal correctly. We have also designed an FPGA-based communication system to prove the feasibility of the system With characteristics as difficult to decipher, simple hardware and easily select the frequency [18], the chaotic information system entirely capable of practical application.

ACKNOWLEDGMENTS

"This research is funded by Funds for Science and Technology Development of the University of Danang under grant number B2017-ĐN06-09"

REFERENCES

[1] S. H. Strogatz, *Nonlinear Dynamics And Chaos: With Applications To Physics, Biology, Chemistry, And Engineering*.: Westview Press, 2001

[2] E. N. Lorenz, "Deterministic nonperiodic flow," *Journal of the Atmospheric Sciences*, vol. 20, pp. 131-140, 1963

[3] R. C. Hilborn, *Chaos and Nonlinear Dynamics: An introduction for Scientists and Engineer*.: The Clarendon Press Oxford University Press, 2001.

[4] M. P. Kennedy, R. Rovatti, and G. Setti, *Chaotic Electronics in Telecommunications*.: CRC Press, 2000

[5] Z. Jákó and G. Kolumbán, "Carrier generation for chaotic communication by fourth-order analog phase-lock loop," in *International Symposium on Nonlinear Theory and its Applications (NOLTA'98)*, Crans-Montana, Switzerland, 1998, pp. 827-830

[6] E. J. Kostelich and T. Schreiber, "Noise reduction in chaotic time series data: A survey of common methods," *Physical Review E*, vol. 48, pp. 1752-1763, 1993

[7] H. Dedieu and M. J. Ogorzalek, "Nonlinear approach to signal coding and compression," in *European Conference on Circuit Theory and Design (ECCTD'99)*, Stresa-Italy, 1999, pp. 58-61

[8] G. Chen, "Chaos, bifurcations, and their control," in *Wiley Encyclopedia of Electrical and Electronics Engineering*, J. G. Webster, Ed. New York: Wiley, 1999, pp. 194-218

[9] Z. Galias, C. A. Murphy, M. P. Kennedy, and M. J. Ogorzalek, "A feedback chaos controller: Theory and implementation," in *IEEE International Symp. on Circuits and Systems (ISCAS'96)*, Atlanta, 1996, pp. 120-124

[10] M. Ogorzalek, "Observation of stochastic resonance in a ring laser," *Physical Review Letters*, vol. 60, 1998

[11] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821-824, 1990

[12] Ming H B and Sheng Y Z, "Data encryption algorithm based on chaotic parameter modulation", Circuits and Systems, 2009, pp. 34-38.

[13] Victor Hugo Pereira Rodrigues and Tiago Roux Oliveira, *Chaos Synchronization Applied to Secure Communication via Sliding Mode Control and Norm State Observers*, 13th IEEE Workshop on Variable Structure Systems, VSS'14, June 29 -July 2, 2014, Nantes, France.

[14] S. Vaidyanathan and S. Sampath, "Sliding mode controller design for the global chaos synchronization of Coullet systems," Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol. 84, pp. 103-110, 2012.

[15] L. Kocarev, K. Halle, K. Eckert, and L. O. Chua, "Experimental demonstration of secure communication via chaotic synchronization," *International Journal of Bifurcation and Chaos*, vol. 2, no. 3, pp. 709-713, 1992

[16] G. Kolumbán, M. P. Kennedy, and L. O. Chua, "The role of synchronization in digital communications— Part II: Chaotic modulation and chaotic synchronization," *IEEE Transactions on Circuits and Systems I*, vol. 45, no. 4, pp. 1129–1140, 1998

[17] Yang, Y. Chen and F. Zhu, "Singular reduced-order observer-based synchronization for uncertain chaotic systems subject to channel disturbance and chaos-based secure communication," Applied Mathematics and Computation, vol. 229, pp. 227-238, 2014.

[18] A. Abel and W. Schwarz, "Chaos communications-principles, schemes, and system analysis," Proceedings of the IEEE, vol. 90, no. 5, pp. 691–710, 2002

[19] Tran Hoang Vu, Nguyen Van Tho, Do Thanh Bao Ngoc, "Design and implementation solutions for real-time embedded computer integrated FPGA technology", Journal of Science and Technology-The University of Danang, JST-UD, Vol 2, no 11(132), pp. 97-101, 2018