암호통신 응용을 위한 마이크로 컨트롤러 기반 로렌츠 카오스 시스템

차민드라[1] · 강보경[1] · 알라딘[1] ·박용수[2] · 송한정[1]

[1]인제대학교 나노융합공학과 · [2]충청대학교 전자정보과

Microcontroller based Chaotic Lorenz System for secure communication applications

Chamindra Jayawickrama[1] · Bogyeong Kang[1] · AlaaDdin Al-Shidaifat[1] · Yongsu Park[2] · Hanjung Song[1]

[1]Department of Nanoscience and Engineering, Inje University, Gimhae 50384, Korea.

[2]Faculty of Electrical & Electronic Engineering, Chung cheong University, Cheongju 28171, Korea.

E-mail : chaminjayaw@gmail.com

요 약

본 연구에서는 암호통신 응용을 위한 카오스 로렌츠 시스템을 다룬다. 암호통신에 필요한 카오스 신호 생성에 PIC18F 기반 마이크로 컨트롤러가 사용되며, 마이크로컨트롤러 프로그램에 XC8 컴파일러가 사용된다. Matlab 및 Preteus 프로그램을 사용하여 모의실험을 실시하였다. 모의실험 결과, 카오스 신호 파형 및 2차원 및 3차원 카오스 어트랙터를 얻었고, 생성된 카오스 신호를 이용하여 암호통신 적용 결과, 성공적으로 카오스 송, 수신 특성을 보였다.

ABSTRACT

This paper presents chaotic Lorenz system implementation for secure data communication applications. In this work chaotic signal is generated by a PIC18F family based microcontroller, XC8 compilers have been utilized for the compilation of C code of microcontroller program. For simulation work Matlab and Proteus platforms were utilized and finally, chaotic time waveforms, 2D and 3D chaotic attractor were obtained and secure communication waveforms were achieved successfully.

키워드

Lorenz system, Chaos, Secure communication, Microcontroller

Ⅰ. Introduction

Since the Lorenz chaotic system was discovered by Ed. Norton Lorenz in 1963, the investigation of chaotic behavior in nonlinear systems has been given great attention [1-4]. Besides the Lorenz system, chaotic circuits and their applications have received a great deal of attention in various fields today. There is a strong interest among researchers in the hardware implementation of chaotic generators by using electronic circuits, including discrete type and fully integrated type, for applications such as secure communications [2-7], data encryption applications. There is two type of chaotic signal oscillators, one is analog circuit based chaotic signal generator and another one is digital chaotic waveform generator in analog chaos signal generator generates analog signal output. disadvantage of analog chaotic waveform generator is, if there is any requirement to change analog signal output waveform pattern, it is required that to change some resistor component values of the internal analog circuitry. And other hands there are many advantages of microcontroller-based Lorenz system in communication security.

II. Lorenz system equations

There are three differential equations in Lorenz system firstly studied by Ed N, Lorenz. These three differential equations were derived from analyzing weather phenomena. Mathematically, the Lorenz attractor is simple, but the result shows chaotic behavior [7-10]. Each x, y and z component of Lorenz equations are as follows:

$$\dot{x}(t) = p(y(t) - x(t)) \qquad (1)$$
$$\dot{y}(t) = rx(t) - y(t) - x(t)z(t) \qquad (2)$$
$$\dot{z}(t) = x(t)y(t) - bz \qquad (3)$$

Above three set of differential equations, parameters x, y and z can be changed with respect to the time. To have the chaotic behavior of these set of differential equations, p, r and b are assigned to some specific constant values for the chaos based Lorenz attractor, those should be replaced with p = 10, r = 30.5 and b = 8/3.

III. Implementation of microcontroller based Lorenz system

For the microcontroller based chaotic oscillator, PIC18F family, based microcontroller has selected. The XC8 compiler has been selected for compilation the source code written in C language. In this circuit arrangement, three 3 D/A converters have implemented to convert digital signal into analog signal output. microcontroller will generate the Lorenz signal output x(t), y(t) and z(t) from its port B, port C, and port D respectively. (Fig. 1) Those three signal outputs are digital signal output from the microcontroller.

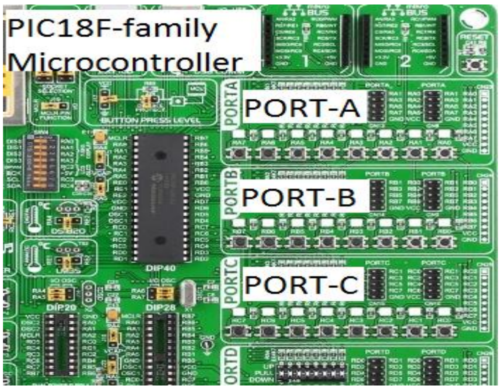

Fig. 1 PIC18F family based microcontroller experimental board

Fig. 1 shows PIC18F family based microcontroller experimental board, In this board, there are reserved ports for each microcontroller port output. in this experiment port, A to C have utilized, at each port output A/D converter has implemented for analog output of the chaotic signal.

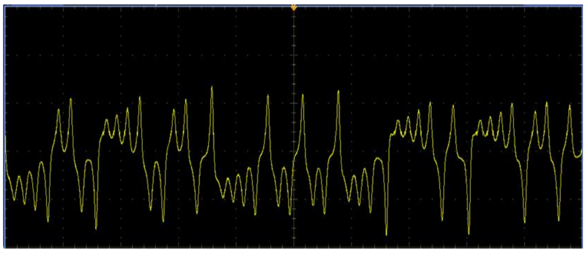

Fig. 2 Chaotic time waveform experimental output

for a example Fig. 2 represent analog time wave output of port A above Fig. 1

IV. Secure chaotic communication

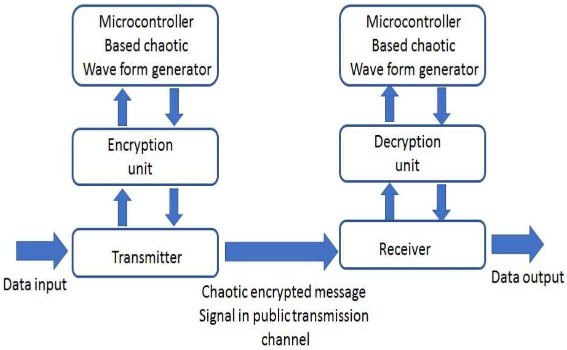
Microcontroller Based chaotic Wave form generator
Encryption unit
Transmitter
Data input
Microcontroller Based chaotic Wave form generator
Decryption unit
Receiver
Data output
Chaotic encrypted message Signal in public transmission channel

Fig. 3 Chaotic secure communication system block diagram

Fig. 3 shows the simplified diagram of chaotic secure communication system There is two main block of the system one is transmitter and the other one is the receiver. Receiver placed on some distance from the transmitter. At the transmitter end, original data signal is encrypted using microcontroller generated chaotic waveform. then this secured information signal can be transmitted to receiving end since chaotic waveform is very arbitrary waveform, this chaotic encrypted waveform well secured. At the receiving end original message will be decrypted by synchronized another chaotic oscillator at the receiving end. therefore, original data signal will be extracted. figure 4. shows the experimental results of chaotic communication system.

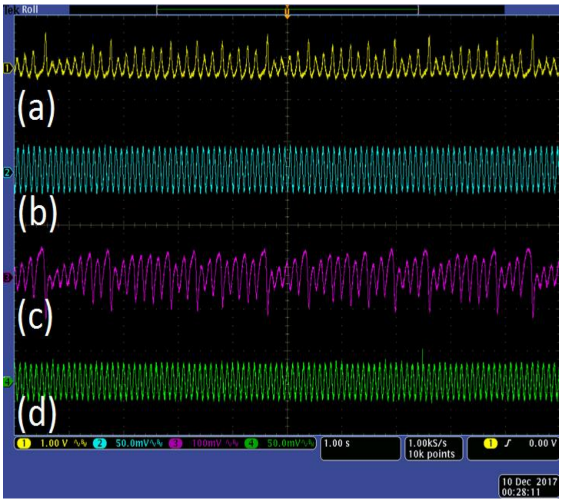

Fig. 4 Secure data transmission through a public channel. (a) Chaotic carrier signal. (b). Message signal (C) Modulated signal. (d) Recovered signal.

Ⅴ. Conclusion

This paper presents secure data communication using chaotic wave form encryption and description with message signal and synchronization both transmitter and receiver end using two microcontrollers engaging at Transmitting end and receiving end. The gained simulation results demonstrated that the Lorenz system can be implemented on the microcontroller and secure methods for information on the data communication is feasible.

References

[1] C. Han, S. Yu and G. Wang, "A Sinusoidally Driven Lorenz System and Circuit Implementation," *Mathematical Problems in Engineering,* Vol. 2015, No. 706902, pp. 1-11, 2015.

[2] Murali, Krishnamurthy, "Secure communication using a chaos based signal encryption scheme," *IEEE Transactions on Consumer Electronics*, Vol. 47, No. 4, pp. 709-714, 2001.

[3] R. Chiuab, M. M. Gonzaleza and D. L. Mancillaa, "Implementation of a Chaotic Oscillator into a Simple Microcontroller," *2013 International Conference on Electronic Engineering and Computer Science*, Vol. 4, pp. 247-252, 2013.

[4] G. Huang and Y. Zhou, "Circuit Simulation of the Modified Lorenz System," *Journal of Information & Computational Science,* pp. 4763-4772, 2013.

[5] A. G. Radwan, A. M. Soliman and A. E. Sedeek, "MOS realization of the modified Lorenz chaotic system," *Chaos, Solitons and Fractals*, Vol. 21, pp. 553-561, 2003.

[6] X. Huai-qing, P. Jian-kui, W. Zhen-qian, H. Ping and Z. Li, "A hyperchaotic Lorenz system circuit simulation and synchronization," *Journal of Lanzhou University (Natural Sciences)*, Vol. 47, No. 5, pp. 120-125, 2011.

[7] Q. H. Alsafasfehl and M. S. Al-Arni, "A New Chaotic Behavior from Lorenz and Rossler Systems and Its Electronic Circuit Implementation," *Circuits and Systems*, Vol. 2, pp. 101-105, 2011.