Efficient Signal Encryption using Chaos-based System

V. Sengodan¹ and A. Balamurugan²

¹Department of Electronics and VLSI, S.N.R. Sons College (Autonomous), Coimbatore-641006, India, E-mail: bala.snr@gmail.com
²Department of Electronics, S.N.R. Sons College (Autonomous), Coimbatore-641006, India.

Abstract: Signal encryption algorithm based on the Chaotic system has been increasingly used, but the drawbacks of small key space, less security in low dimensional chaotic crypto systems, simple chaotic and inconvenient for hardware implementation, are obvious. This paper presents a new signal encryption algorithm based on higher dimensional electronic chaos with the simple electronic system. The attacker cannot decrypt an encrypted signal without the correct key. The proposed system has high level security. The simulated result is checked with experimental one for authentication.

Keywords: Attack, Chaos, Encryption, Information Security, Nonlinear Electronic System.

1. INTRODUCTION

In recent years, due to massive amount of images/signals across the internet over the transmission media, it has become essential to secure them from their use environment. These requirements to meet the security needs of images/signals have led to the development of encryption techniques. A general encryption algorithm for image such as Data Encryption Standard (DES) has the weakness of low efficiency when the data/images is large [1–6].

2. CHAOTIC SYSTEM

These systems have some important properties such as the sensitive dependent on initial conditions and system parameters, pseudorandom property, non-periodicity, etc. Most properties met some requirements such as diffusion and mixing in the sense of cryptography [3]. Low dimensional chaotic system with the advantages of high—level efficiency and simplicity, such as logistic map or Lorenz map, have been widely used in the field of chaos cryptography now. But the weakness of system, such as small key space, weak security and easy to attack with chaotic model reconstruction, are also disturbing [4]. A three-dimensional chaotic system is used in image encryption [5]. But the chaotic system not complicated enough. And a high dimension chaotic system called cellular neural network (CNN) [6] was just proposed for image encryption, but its encryption is just pixel replacement only, and not change the histogram, so it is difficult to resist the attack based on statistical information. To overcome these disadvantages, a new chaotic system is proposed. The double scroll chaos is observed from Chua’s circuit which is made up of linear circuit element [7]. There are many chaotic systems, such as RLC circuit and Colpitts oscillators. But the circuit used in this paper includes a new circuit element p-n junction diode, and research in this field is becoming meaningful. Also this paper extends the basic function approach to proposed chaotic communication systems in order to provide a unified framework in which to compare and contrast conventional and chaotic communications techniques. The basic difference between conventional and chaotic system is that segment of chaotic wave forms, rather than sinusoids, are used as basic functions in chaotic communications. Because of the non-periodic property of the chaotic signals, there is a fundamental difference between conventional and chaotic systems.

3. PROPOSED ELECTRONIC CHAOS IN HIGHER DIMENSIONAL NONLINEAR SYSTEM

The third order chaos based encryption system is described by the set of equations:

\[ L_1 \frac{dl_1}{dt} + R i_1 (t) + L_2 \frac{dl_2}{dt} i_1 (t) - L_2 \frac{dl_2}{dt} i_1 (t) = A \sin \omega t \]

\[ L_2 \frac{dl_2}{dt} + 1/C - \alpha \int i_2 (t) - L_2 \frac{dl_2}{dt} i_2 (t) = 0 \]

\[ I_1 (S) [L_1 (S) + R + L_2 (S)] - I_2 (S) [L_2 \cdot S] = A \cdot (\omega s^2 + \omega^3) \]

\[ I_2 (S) + I_1 (S) [L_2 (S)]/L_2 (s) (s + 1/SC) \]

\[ I_1 (S) = [A \cdot \omega s^3 \cdot L_2 \cdot C + 1] / (s^2 + \omega^3) (s^3 \cdot L_1 \cdot L_2 \cdot C + s^2 \cdot L^2 \cdot R \cdot C + S \cdot (L_1 + L_2) + R) \]

\[ I_2 (S) = [A \cdot \omega \cdot s^3 \cdot L_2 \cdot C] / [(s^2 + \omega^3) (s^3 \cdot L_1 \cdot L_2 \cdot C + s^2 \cdot L^2 \cdot R \cdot C + S \cdot (L_1 + L_2) + R) \]

According to the dynamical equation shown above, chaotic attractors can be observed. The characteristic of the chaotic system is determined and provides the security
analysis by the following chaotic attractors. A good encryption algorithm/system should be sensitive to the initial condition. So the encryption algorithm based on the chaotic system has a good security property. The observations and experimental actions of the proposed system as follows [see Fig. 1]. For small values of $F$ ($\approx 50$ mV), quasiperiodicity occurs. This quasi periodicity is stable for $50 < F < 168$ mV. When the amplitude is increased to $F = 168$ mV, the quasiperiodicity becomes unstable and a period $1T$ orbit is born and is stable in the range of amplitude $168 < F < 280$ mV. As the parameter $F$ is further increased, period $2T$, $4T$,…. orbits are found to occur leading to onset of chaos. The amplitude of the external periodic signal $F$ is further increased the period $2T$ orbit at $F = 280$ mV and it is stable in the range $280 < F < 335$ mV. When the amplitude of the circuit is kept as further increased, period $4T$ orbit is born at the amplitude value $F = 335$ mV and is stable in the range of $335 < F < 344$ mV. The chaotic attractor is stable up to $397$ mV. And it is maintained the same in the range of $344 < F < 397$ mV. After that the system exhibits period 5 windows. When the amplitude of the periodic signal is kept at $397$ mV, period 5 windows occur and it is stable in the range $397 < F < 434$ mV. Finally, the system goes to the boundary crisis when the amplitude value exceeds $475$ mV.

Fig. 1: Experimental Results of Crypto System
4. STATISTICAL ANALYSIS
The comparison between the original information and the encrypted signal can be seen in the histogram. It is shown in the Fig. 2.

The histogram on the signal is similar to that of the random signal, so the performance of the encryption signal is good. Also we provided the simulated onset of chaos and Poincare surface of the complex attractor in Fig. 3.

![Fig. 2: Decrypted Signals: (a) Decrypted Chaos Signal, (b) Decrypted Information Signal](image1)

![Fig. 3: (a) Poincare Map of Chaotic Attractor (b) Simulated Result of Onset of Chaos for Fig. 1 (c).](image2)

5. CHAOS SYNCHRONIZATION
Driving a nonlinear system with a periodic signal is a common feature in nonlinear dynamics. However, the idea of using a Chaotic signal to drive a system in phase and amplitude and so far synchronization is rather new. Now focus on the use of synchronized chaotic signal as vehicles for effective transmission of signals in the context of Cryptography. This system is shown in Fig. 4. The point is that when a chaotic signal is transmitted, it can not be deciphered by a second person unless one has the full information about the transmitting system to couple with it appropriately for synchronization. The proposed system satisfy the synchronization and the characteristic of chaotic signal is obtained from the receiver and the \( m'(t) \) signal (transmitted signal at the receiver end) is also observed. Thus the synchronization receivers can be recognized as a form of matched filter for the chaotic transmitted signal.

![Fig. 4: Synchronization of the Proposed Electronic Cryptosystem](image3)

6. CONCLUSION
The non-autonomous chaotic system with a simple nonlinear element can generate chaos. Using this system, chaotic sequences can be obtained and used for encryption. The simulation result shows that the encryption meets the basic requirements. Analysis of security and numerical experiments explain the effectiveness of the system. The key in this system is exactly the initial conditions, and the security
of the system is totally depending on the principle of basic Kirchhoff’s theorems. It should be noted that the chaotic system used in this paper is the complex three dimensional one. And this system is highly useful in the secure communication at defence applications.

REFERENCES


