Design of a New Chaos Circuit and Its Encryption to Digital Information

WANG Hong¹,  PENG Jian-hua²,  ZHOU Zheng-ou¹

(¹. School of Electronic Engineer, UESTC Chengdu 610054 China; ². College of Science, Shenzhen University Guangdong Shenzhen 518060 China)

Abstract  A new hyperchaos circuit system with simple structure is designed in this paper. It can be implemented with changeable dimensions 3, 5, 7, 9, etc, therefore it can afford different security grades for applications. The dynamic characters of the 7th order circuit have been analyzed as an example. Using the hyperchaos time sequence produced by this circuit as key sequence, the encryption and decryption to digital signals of text and image files have been realized, and the real-time ability has been increased with encrypting digital signals per byte.

Key words  hyperchaos; dynamic character; key sequence; encryption

With the development of Internet and multimedia technology, multimedia communication has become the most important method to transmit information. Meanwhile, the problem of information security is more important than ever [1, 2]. In recent years, applying chaos dynamic systems to information encryption has caused great interesting to many authors. The study in this field has developed a new aspect, chaotic cryptography. It has advantages of simple algorithms, key sequence generated easily, sensitivity to initial variable values, and white noise statistics characters, in contrast with traditional cryptography. Some chaotic encryption systems have been proposed presently. But most systems are designed simply as low dimensional chaos systems without theory analysis to security, not satisfying the need for higher security. From view of practice, it is significant and necessary to design a system with powerful security but not too complex structure. In theory, the higher the order of a system is, the more powerful the security is [3]. But the system’s complexity is increased accordingly.

In this paper, a new hyperchaos circuit system is reported. It has a simple structure and changeable dimensions and can, therefore, satisfy the need for different security grades.

Fig.1  A changeable dimensions chaos circuit

Fig.2  Negative resistor circuit

Fig.3  Piecewise linear circuit

Received 2004-04-05
1 Model of a Changeable Dimensions Chaos Circuit

The circuit of a changeable dimensions chaos system is shown in Fig.1. It consists of three parts: a negative resistor circuit, LC resonance parts, and a piecewise linear circuit. The outstanding work of this design is that the circuit’s dimensions can be changed easily to satisfy different security grades. The detail circuit of the negative resistor is shown in Fig.2, the function of which is to supply energy to the circuit in Fig.1 can be described as follows, the main components are 5 operational amplifiers and a diode. The piecewise linear character of this circuit is realized by the diode, as shown in Fig.4.

![V-I curve of the piecewise linear circuit](image)

According to Kirchoff law, the state equations of the circuit in Fig.1 can be described as follows,

\[
\begin{align*}
\frac{dV_{C1}}{dt} &= \frac{1}{C_1}\left(V_{C1} - i_{L2}\right) \\
& \vdots \\
\frac{dV_{C2m-1}}{dt} &= \frac{1}{C_{2m-1}}(i_{L2m-2} - i_{L2m-1}) \\
\frac{dV_{C2m}}{dt} &= \frac{1}{L_{2m-2}}(V_{C2m-1} - V_{C2m} - R_{L2m-2}i_{L2m-2}) \\
& \vdots \\
\frac{dV_{CN}}{dt} &= \frac{1}{C_N}\left[8(i_{L2N-1} - 3)H(i_{L2N-1} - 3) - V_{CN} \right]
\end{align*}
\]

where \(m=2, 3, \ldots, (N-1)/2\) is the Heaviside step function, \(H(x) = 1\) if \(x>0\) and \(H(x) = 0\) for \(x \leq 0\), \(R_L\) is the serial resistor of an inductance, and \(N\) is the circuit’s order. \(N\) is an odd number and \(N \geq 3\) in our consideration. To simplify Eq.(1), we employ the following normalization

\[
C_1 = C_{2m-1} = C_N = C \\
L_{2m-2} = L_{N-1} = L \\
R_{L2m-2} = R_{L2m-1} = R_L \\
x_1 = V_{C1} \\
x_{2m-2} = \rho_{L2m-2} \\
x_{2m-1} = V_{C2m-1} \\
x_N = V_{CN} \\
\tau = t/\sqrt{LC} \\
a = \rho/R \\
c = \rho/R_N \\
b = R_L/\rho \\
d = 2\rho
\]

Hence the normalized form of Eq.(1) is

\[
\frac{dx_1}{dt} = ax_1 - x_2 \\
\vdots \\
\frac{dx_{2m-2}}{dt} = x_{2m-3} - x_{2m-1} - bx_{2m-2} \\
\frac{dx_{2m-1}}{dt} = x_{2m-2} - x_{2m} \\
\vdots \\
\frac{dx_{N-1}}{dt} = x_{N-2} - x_N - bx_{N-1} \\
\frac{dx_N}{dt} = 8(x_{N-1} - d)H(x_{N-1} - d) - cx_N
\]

where \(a, b, c, d\) are system parameters. To be convenient to numerical analysis and computer simulation, the values of all capacitances and all inductances are equal, 33 nF and 33 mH, respectively. The absolute value of the negative resistor \(R\) is 3.3 kΩ, which can be calculated from Fig.2. The values of all resistors serialized with inductances are same, symbolized with \(R_L\). The dynamic characters of the circuit are analyzed by adjusting the value of \(R_L\). To Eq.(2), it means that parameters \(a, c, d\) are the constants and parameter \(b\) is changeable. The values of \(a, c, d\) are 0.3, 1.0, 3.0, respectively.

We call an inductance serialized with a resistor and a capacitance connected before it an LC unit. If an LC unit is added to the circuit or removed from it, the circuit will be a changeable dimensional autonomic system. A series of hyperchaos systems with arbitrary positive Lyapunov exponents can be obtained from adding LC units to the circuit. This method of creating a hyperchaos system is much more easy than the way of coupling low dimensional chaos systems reported by Ref.[4], and it is beneficial to applications, too.
dimensional chaos system should be adopted to ensure higher security of the cryptography system. But that usually means the increased complexity of the system. In our design, the circuit’s dimensions can be increased easily by adding LC units, and a lot of hyperchaos sequences can be obtained more random while not at the cost of increasing the circuit’s complexity remarkably. Furthermore, higher security can be guaranteed.

2 Dynamics Analysis

Lyapunov exponents $\lambda_i$ are usually used to describe the stability of an observed orbit of a dynamical system. For the case of a one-dimensional orbit, if Lyapunov exponent $\lambda > 0$, then the orbit is unstable, else it is stable. For the case of a multiple dimensional orbit, if one or more of the $\lambda_i > 0$, then we have chaos or hyperchaos. According to numerical calculation results, when the circuit’s order $N=3$, only low dimensional chaos sequences can be generated by the circuit, it means that the system has only one positive Lyapunov exponent. When $N \geq 5$, the circuit can create a series of hyperchaos sequences with two or more positive Lyapunov exponents.

The 7th order circuit is selected as an example to create key sequences in this paper. When $N = 7$, the detail nondimensional equations can be obtained straight from Eq.(2).

\[
\begin{align*}
\frac{dx_1}{dt} &= 0.3x_1 - x_2 \\
\frac{dx_2}{dt} &= x_1 - x_3 - bx_2 \\
\frac{dx_3}{dt} &= x_4 - x_5 \\
\frac{dx_4}{dt} &= x_5 - x_6 \\
\frac{dx_5}{dt} &= x_6 - x_4 \\
\frac{dx_6}{dt} &= x_7 - x_6 \\
\frac{dx_7}{dt} &= 8(x_4 - 3.0)H(x_6 - 3.0) - x_5 
\end{align*}
\]

When $b=0.025$, Eq.(3) gives 4 positive Lyapunov exponents: $\lambda_1 = 0.066$, $\lambda_2 = 0.054$, $\lambda_3 = 0.044$, and $\lambda_4 = 0.014$. It means that the circuit is at the state of hyperchaos. The security is higher than a low dimensional chaos system that has only one positive Lyapunov exponent. Fig.5 shows a hyperchaos attractor of state variables $x_1$ and $x_2$ when $b=0.025$ and initial values of $x_1, x_2, \ldots, x_7$ are 2.6, 3.0, 2.8, 3.0, 4.0, 4.0, 3.0, respectively.

![Fig.5 Hyperchaos attractor](image)

Chaos encryption is a kind of sequence encrypting algorithm. Its principle shows in Fig.6. A plaintext $X$ is seen as a byte stream of $x_1x_2 \ldots x_i \ldots$, and a key sequence $K (k_1k_2 \ldots k_i \ldots)$ is generated from the 7th order hyperchaos circuit equations. An encrypted file sequence $Y (y_1y_2 \ldots y_i \ldots)$ is obtained by modulo-256 adding calculation of the plaintext sequence and the key sequence. That means $y_i = x_i \oplus k_i$ ($i = 1,2, \ldots$), where $x_i, k_i, y_i$ is a byte, respectively. The symbol “\(\oplus\)” means the modulo-256 adding calculation. Decryption is a reverse process of encryption with the same key sequence generated from the same chaos system. Encrypting files per byte can enhance the speed of encryption compared with encrypting files per bit[5]. It is suitable for the occasions of large amounts of data and high-speed real time.

![Fig.6 Hyperchaos encryption](image)

4 Encryption Results

The results of encryption and decryption to a text
file and an image are obtained according to the encryption algorithm. The key sequence is generated from Eq.(3). Fig. 7 shows the encryption results to a text file, with the initial values of variables $x_1, x_2, \cdots, x_5$ are 2.6, 3.0, 2.8, 3.0, 4.0, 4.0, 3.0 and parameter $b = 0.025$. Fig. 8 shows the encryption results to an image. The initial values of variables and parameter $b$ are same as those in Fig. 7. Fig. 8d shows the decrypted result to the image when the initial value of $x_1$ is 2.60001, which has a little difference with 2.6, while other values have no change. It means that chaos systems are very sensitive to initial values. This character increases the difficulty of decryption, in other words, enhances the security of systems.

“No pains, no gains.”

(a) Plaintext

(b) Encrypted text

(c) Decrypted text

Fig. 7 Text encryption

(a) Original image

(b) Encrypted image

(c) Decrypted image

(d) Decrypted image when initial value has little difference

Fig. 8 Image encryption

5 Conclusions

A new changeable dimensional chaos circuit with simple structure is represented in this paper. It can satisfy different security grades by changing the numbers of LC units. It is a good hyperchaos generator for security communication. The dynamics analysis results to the 7th order circuit are given in this paper. And the encryption simulation results to a text file and an image are presented in the end of the paper.

References


Brief Introduction to Author(s)

Wang Hong (王宏) was born in Daqing, Heilongjiang, China in 1975. Now She is a Ph.D. candidate of Communication and Information Engineering at UESTC. Her current research interests include in security communications, nonlinear circuits and system theory and digital signal processing. E-mail: wanghong@uestc.edu.cn

Peng Jian-hua (彭建华) now is a professor a in College of Science, Shenzhen University. His current research interests include in nonlinear theory and applications.

Zhou Zheng-ou (周正欧) now is a professor and doctoral advisor in UESTC. His current research interests include in radar signal processing and digital communications.