Chaotic Cryptosystem based on Inverse Duffing Circuit

Ch. K. VOLOS, I. M. KYPRIANIDIS, and I. N. STOUBOULOS
Physics Department
Aristotle University of Thessaloniki
Thessaloniki, 54124
GREECE

Abstract: - We have studied experimentally a chaotic cryptosystem, which is based on the inverse system approach. We applied this method to a second order nonlinear circuit (master circuit), which is described by a Duffing equation. We present the implementation of the slave circuit with the inverse system approach and we demonstrate the decryption when the information signal has several forms (sinusoidal and rectangular). By appropriate choice of the parameters of the nonlinear oscillator, and the signal oscillator, it is possible to have a cryptosystem capable of transmitting information securely and recovering it accurately.

Key-Words: - Chaos, Cryptosystem, Duffing equation, Synchronization, Inverse system approach, Master-Slave circuits.

1 Introduction

Since its ancient beginnings, cryptographical methods have been almost exclusively applied to discrete-value information. These methods range from the so-called Caesar Cipher over the well-known Vegenère Cipher up to modern encryption algorithms like Data Encryption Standard (DES) or the asymmetrical algorithm by Rivest, Shamir, and Adelman (RSA). With the work of Shannon [1, 2] the development of cryptographical methods became a modern science, which is the information theoretic basis for all encryption systems nowadays in use.

Despite the strong relevance of the discrete-value systems, there have been attempts to apply cryptographical methods to continuous-value information. At the beginning, autonomous chaotic systems were used as pseudo-random number generators in discrete-value implementations. Thereafter, the pioneering works on chaos synchronization, led to a new branch of applications. Now, nonautonomous chaotic systems with continuous-value signal were used to transmit information. Several schemes have been developed which allow to transform the information signal into a chaotic waveform on the encoder side and to extract the information signal from the transmitted waveform on the decoder side. The most important among them are:

- Chaos Shift Keying: The encoder consists of two or more autonomous chaotic systems with different parameters. According to the discrete information signal, one of them is selected and its output signal is transmitted over the channel. In the decoder the same number of chaotic systems tries to synchronize with their encoder counterparts. The parameters are adjusted in such a way that only one pair can synchronize at a time. Detecting this, synchronization decodes the discrete information.
- Chaotic Masking: The encoder consists of an autonomous chaotic system whose output signal is added to the information signal. This sum is transmitted over the channel. The decoder uses the transmission signal to synchronize an equivalent chaotic system with the encoder system. The reconstructed chaotic signal is then subtracted from the transmission signal, which finally reconstructs the information signal. In order to guarantee synchronization on the receiver side, the information signal has to be sufficiently small in respect to the chaotic signal.
- Chaotic Modulation or Inverse System: The encoder is a nonautonomous chaotic system whose state is influenced by the information signal. The decoder synchronizes with the encoder via reconstruction of its state using the transmission signal. The information signal is recovered by applying the inverse encoder operation to the reconstructed state and the transmission signal.

All of these schemes have been investigated analytically and experimentally in continuous-time as well as in discrete-time application [3-8]. From our viewpoint, the inverse system approach seems to be the most suitable scheme for continuous-value encryption because of its unrestricted signal structure.

2 The Structure of Cryptosystems

The basic structure of cryptosystems is shown in Fig.1. The information message to be transmitted is called the plaintext message or simply plaintext and is denoted by p. A plaintext p is encrypted to a ciphertext by an encryption function or encryption transformation E subject to a set of keys k from the key space K. Thus, the ciphertext, denoted by c, can formally be written as

$$c = E_k(p) \quad (1)$$

The ciphertext is transmitted to the receiver, which is the intended recipient of messages. The receiver decrypts the ciphertext by using a decryption function or decryption transformation D subject to the same set of keys k. The decryption of the plaintext p can be formally presented by

$$D_k(c) = D_k\left(E_k(p)\right) = p \quad (2)$$

That is, $D_k=E_k^{-1}$.

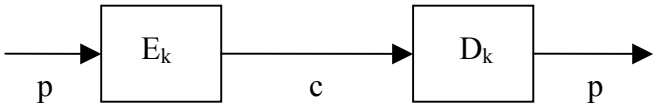


Fig.1. Basic structure of cryptosystems.

In the cryptosystems just described, the same keys are used for both encryption and decryption. This type of cryptosystem is called the symmetric or private or secret-key cryptosystem. In designing cryptosystems, in general, there are two important rules:

1. the encryption function should transform the plaintext p to a ciphertext c which would be infeasible to decrypt without the right keys,
2. the inverse of the encryption function, namely the decryption function, should exist and recover the plaintext accurately.

More cryptosystems are designed based on pure mathematical theories such as number theory, modular mathematics, algebra, and elliptic curves [9-14]. In this paper, a symmetric cryptosystem is designed based on a chaotic oscillator, namely a Duffing-type chaotic oscillator.

3 The Proposed Cryptosystem

The cryptosystem presented in this note is depicted in Fig.2. This system consists of the following components. S is the external sinusoidal voltage source, p is a signal which incorporates the transmitted plaintext and p′(t) is the recovered plaintext. The signals u and u′ are the input of the original circuit and the output of the inverse circuit respectively. If the two circuits are synchronized the signals u and u′ are identical. The transmitted signal (ciphertext) is c, which is chaotic. If we want to make the ciphertext c more complicated, we can add the signal from the output of the non-linear circuit with the signal from a second chaotic signal generator S_2, and then subtract this signal, S_2, from the ciphertext before the signal inserts to the non-linear invert circuit.

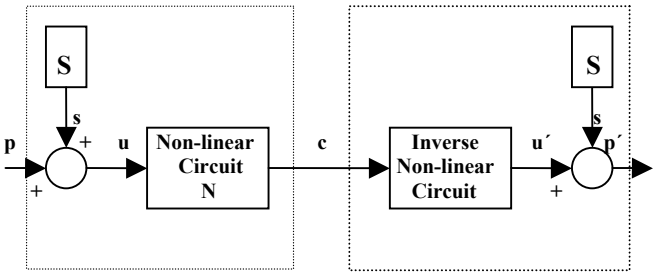


Fig.2. The proposed cryptosystem.

3.1 Encryption System

A major part of this encryption system is a non-linear time-varying system, which is a circuit obeying Duffing's equation. Duffing's equation,

$$\frac{d^2x_1}{dt^2} + \varepsilon \cdot \frac{dx_1}{dt} + a \cdot x_1 + b \cdot x_1^3 = u(t) \quad (3)$$

is one of the most famous and well studied nonlinear non-autonomous equations, exhibiting various dynamic behaviors, including chaos and bifurcations.

One of the simplest implementations of the Duffing equation has been presented by Leuciuc [15]. It is a second order nonlinear circuit, which is excited by a sinusoidal voltage source ($s(t)=V_0\cos(\omega t)$), and contains two op-amps (LF411) operating in the linear region (Fig.3).

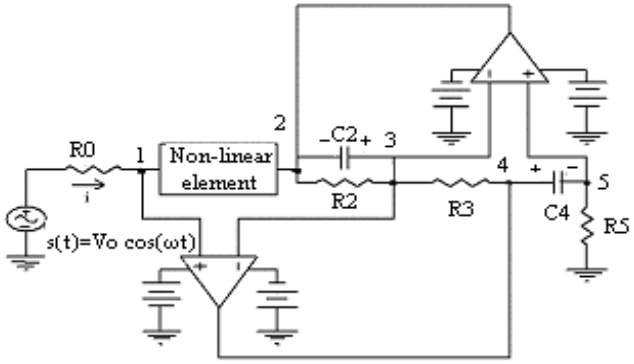


Fig.3. The electronic circuit obeying Duffing's equation.

This circuit has also a very simple nonlinear element, implementing a cubic function of the form,

$$i(v) = p \cdot v + q \cdot v^3 \quad (4)$$

Denoting by x_1 and x_2 the voltages across capacitors C_2 and C_4 respectively, we have the following state equations.

$$\frac{dx_1}{dt} = -\frac{1}{C_2 \cdot R_2} \cdot x_1 + \frac{1}{C_2 \cdot R_3} \cdot x_2 \quad (5)$$

$$\frac{dx_2}{dt} = -\frac{R_0}{C_4 \cdot R_5} \cdot f(x_1) + \frac{V_0}{C_4 \cdot R_5} \cdot \cos(\omega \cdot t) \quad (6)$$

where, $f(x_1) = p \cdot x_1 + q \cdot x_1^3$, is a cubic function.

Finally, from equations (5) and (6), we take the Duffing equation (3), where,

$$\varepsilon = \frac{1}{C_2 \cdot R_2}, \qquad a = \frac{p \cdot R_0}{C_2 \cdot C_4 \cdot R_3 \cdot R_5}$$

$$b = \frac{r \cdot R_0}{C_2 \cdot C_4 \cdot R_3 \cdot R_5}, \quad B = \frac{V_0}{C_2 \cdot C_4 \cdot R_3 \cdot R_5} \quad (7)$$

Other significant part of the proposed cryptosystem is the signal generator S. The signal that signal generator produces is a sinusoidal signal, so ($s(t)=V_0 \cos(\omega t)$).

The private keys of the cryptosystem in Fig.2, are the system N (the non-linear circuit), its parameters, and the signal generator S. The values of circuit parameters are R_0=2.05kΩ, R_2=5.248kΩ, R_3=R_5=1kΩ, R_{11}=R_{12}=0.557kΩ, R_1=8.11kΩ, C_2=105.9nF, C_4=9.79nF, V_0=2V and f=1.273kHz, so the normalized parameters take the following values a=0.25, b=1, ε=0.18, ω= 0.8 and B=20. The plaintext to be transmitted is first converted to a appropriate information signal p(t). In this paper we choose two different forms of information signals (sinusoidal and rectangular). The information signal p(t) is added to s(t), so

$$u(t) = p(t) + s(t) \quad (8)$$

The function u(t) is then applied to the system N. The output of N is the transmitted signal c(t). By appropriate choice of the system N and the signal generator S, the output of N can be chaotic which would be difficult to be decrypted if it intercepted by an unintended party. The transmitted signal is transmitted to the intended party to use the decryption system to recover the information signal.

3.2 Decryption System

Although it is easy to choose an encryption system, it may be difficult to design a decryption system that would invert the encryption function. The inversion should be possible, implementable and accurate. The crucial part of the inversion of the encryption function in this paper is based on the inverse system approach. The inversed circuit (slave) are coupled with the Duffing's type circuit (master) via nodes-4, (Fig.4), so $c(t) = y_1(t)$. The slave circuit is described by the following set of equations.

$$\frac{dx_1'}{dt} = -\frac{1}{C_2 \cdot R_2} \cdot x_1' + \frac{1}{C_2 \cdot R_3} \cdot x_2'$$

$$\frac{dx_2'}{dt} = -\frac{1}{C_4 \cdot R_5} \cdot x_2' + \frac{1}{C_4 \cdot R_5} \cdot y_1 \quad (9)$$

$$u' = R_0 \cdot f(x_1') - x_2' + y_1$$

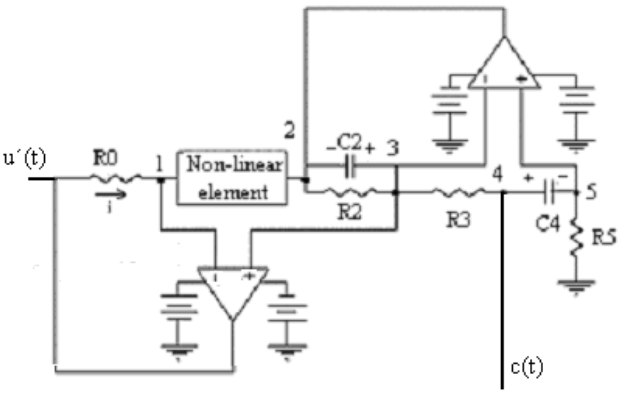


Fig.4. The decryption circuit.

Denoting by x_1', x_2', are the voltages across the capacitors C_2 and C_4 respectively of the slave circuit.

The decryption system consists of the inversed circuit and the signal generator S. The output of the inversed circuit is u´(t), which is equal to u(t) = p(t) + s(t). Subtracting s(t) from u´(t) yields p´(t), which is a good, approximation of p(t). Note that the keys, namely, the parameters of the inverse circuit and the signal generator S, are the same with the encryption system.

4 Experimental Results

We have studied this cryptosystem when,

- We don't have plaintext (p(t)=0), so the information signal is the $s(t)=V_0 \cos(\omega t)$.
- The information is another sinusoidal signal.
- And the information is a rectangular signal.

The two coupled circuits have exactly the same values of elements, so the two coupled circuits have the same parameters, a=0.25, b=1, ε=0.18, ω= 0.8 and B=20. For these values of the parameters, we observed chaotic behavior.

4.1 p(t)=0

In the first case, we don't have plaintext (p(t) = 0), so the information signal is $u(t)=s(t)=V_0 \cos(\omega t)$ [16,

17]. The cryptosystem work perfect as we observe from the plot of u´(t) vs. u(t), (Fig.5).

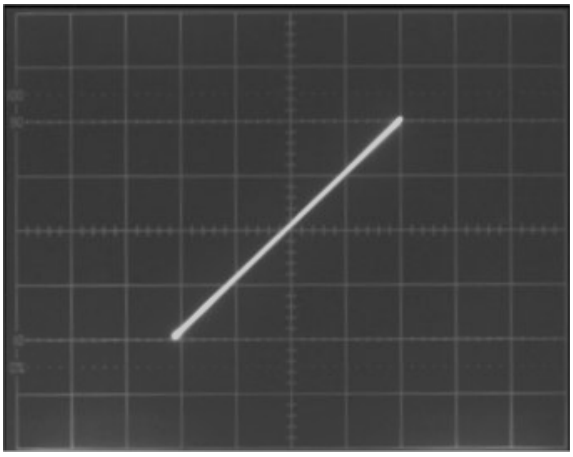


Fig.5. Plot of u´(t) vs. u(t) (Horiz.: 1V/div., Vert.: 1V/div.). Synchronization is observed.

4.2 $p(t) = V_0´\cos(\omega´t)$

In this case, the information signal has a sinusoidal form, $p(t)=V_0´\cos(\omega´t)$, with $V_0´=0.7V$ and $f´=0.1kHz$, so $u(t) = V_0´\cos(\omega´t) + V_0 \cos(\omega t)$. We must point out that in any practical application one should therefore use a chaotic system that oscillates with frequencies that are much higher than the characteristic frequencies of the information signal.

In Fig.6, the transmitted signal y_1 is shown. It is obvious a chaotic signal. The cryptosystem work good enough as we observe from the comparison of the waveforms of the transmitted information signal p(t), and recovered information signal p´(t) by the decryption system, (Fig.7).

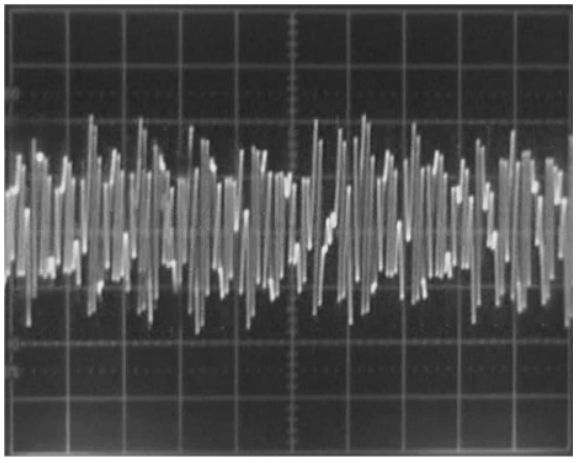
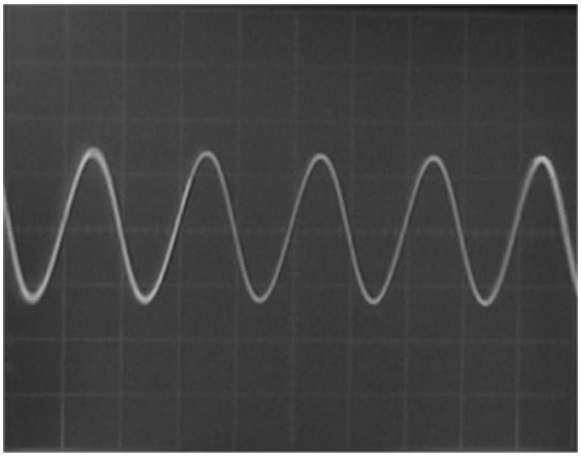
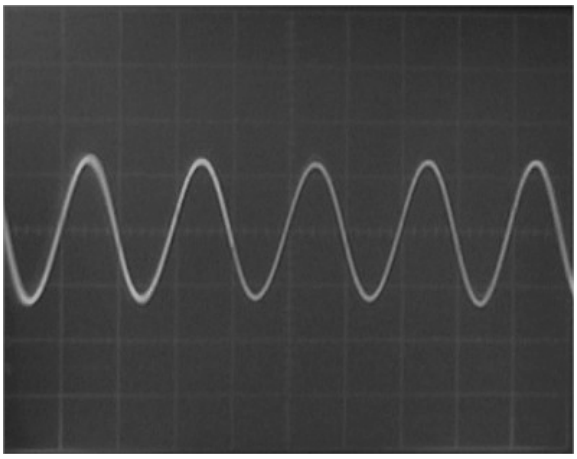


Fig.6. Transmitted signal c(t) (chaotic signal), (Horiz.: 0.5msec/div., Vert.: 5V/div.)



(a)



(b)

Fig.7. Waveforms of (a) information signal p(t) and (b) recovered information signal p´(t) (Horiz.: 5msec/div., Vert.: 0.5V/div.)

4.3 The information p(t) is a rectangular signal

In this case, the information signal is a train of pulses of amplitude zero or 0.7Volt and frequency f=0.1kHz. As we can see in Fig.8, the transmitted signal y_1 is a chaotic signal. Also we can see in Fig.9 that the recovered information signal by the decryption system is a good but noisy approximation of p(t).

If we run the simulation of the circuit behavior in PSpice, we can take a diagram of the difference $x = |p(t) - p´(t)|$ between the transmitted and recovered information signal (Fig.10). From this diagram we compute that the average value of this difference is $\bar{x} = 0.00984\,V$. This means that the noise of the signal is very low, 1.4%. If we want to decrease the noise further, we can use a low-pass filter. It is remarked that the filter should be designed

carefully in order to be able to recover the information fully and accurately.

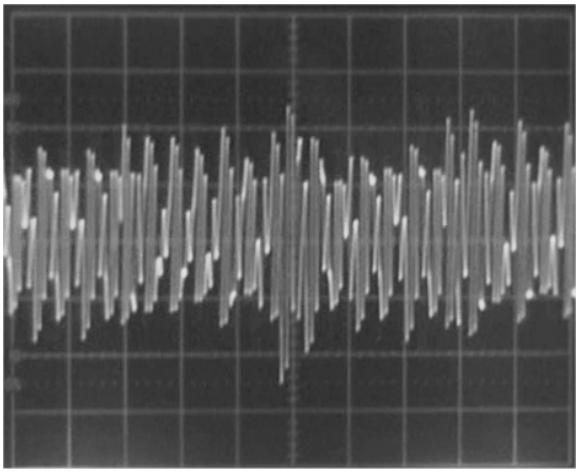
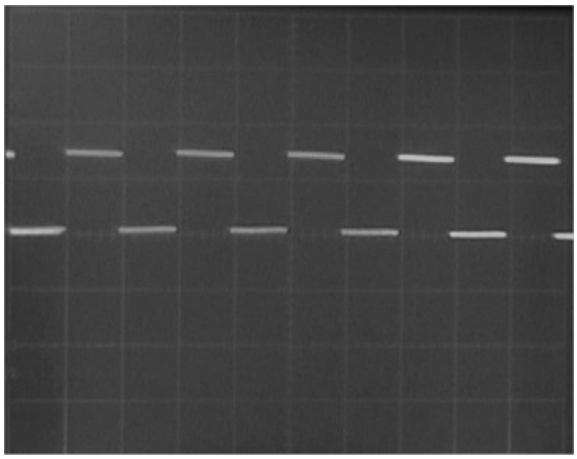
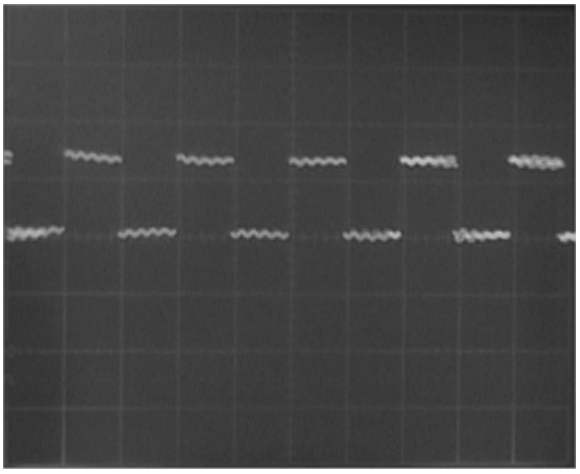


Fig.8. Transmitted signal c(t) (chaotic signal), (Horiz.: 0.5msec/div., Vert.: 5V/div.)



(a)



(b)

Fig.9. Waveforms of (a) information signal p(t) and (b) recovered information signal p´(t) (Horiz.: 5msec/div., Vert.: 0.5V/div.)

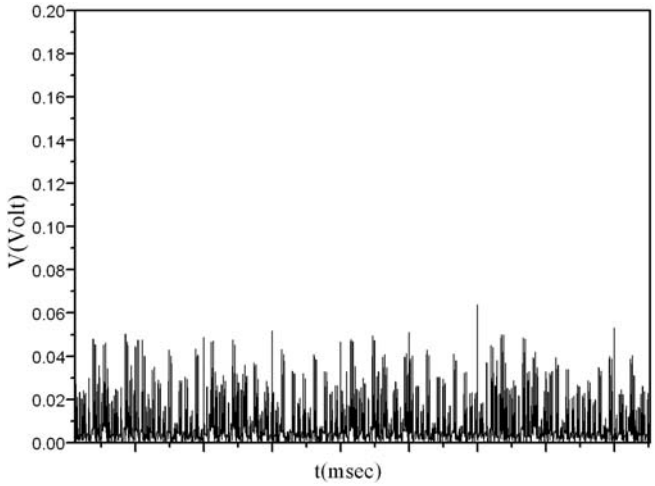


Fig.10. Difference $|p(t)-p'(t)|$ between the transmitted and recovered information.

5 Conclusions

In this paper a chaotic cryptosystem is proposed. This type of cryptosystem is based on inverse system approach. The encryption system consists of a nonlinear chaotic oscillator (Duffing-type circuit) and a signal generator. The nonlinear oscillator, its parameters, and the signal generator are the private keys of the cryptosystem. The encryption function consists of the dynamics (evolution) of the nonlinear oscillator. The decryption system uses the same keys as those of the encryption system and consists of the inverse Duffing-type circuit. By appropriate choice of the nonlinear oscillator, and the signal generator, it is possible to have a cryptosystem capable of transmitting information securely and recovering it accurately. Three examples of information signals illustrated the good performance of the proposed cryptosystem. The recovered information signal is a good but noisy approximation of the transmitted information, especially when the information is a rectangular signal. Finally, if the decryption system has a low-pass filter the information signal recovered fully and accurately.

Acknowledgements

This work has been supported by the research program "EPEAEK II, PYTHAGORAS II", with code number 80831, of the Greek Ministry of Education and E.U.

References:

[1] A. Leuciuc, Information Transmission Using Chaotic Discrete-Time Filter, IEEE Trans. Circuits Syst. I, Vol.47, 2000, pp.82-88.

[2] Z. He, K. Li, L. Yang, and Y. Shi, A Robust Digital Secure Communication Scheme Based on Sporadic Coupling Chaos Synchronization", IEEE Trans, Circuits Syst. I, Vol.47, 2000, pp.397-403.
[3] D. R.Frey, Chaotic Digital Encoding: An Approach to Secure Communication, IEEE Trans. Circuits Syst. II, Vol.40, No.10, 1993, pp.660-666.
[4] S. Papadimitriou, G. Pavlides, A. Bezerianos and T. Bountis, Chaotic Systems of Difference Equations for Real-Time Encryption, in Proc. Workshop Nonlinear Signal and Image Processing (NSIP ´95), 1995, pp.145-149.
[5] K. Kelber, T. Falk, M. Gotz, W. Schwarz and T. Kilias, Discrete-Time Chaotic Coders for Information Encryption – Part 2: Continuous-and Discrete-Value Realization, in Proc. Workshop Nonlinear Dynamics of Electronic Systems (NDES ´96), 1996, pp.27-32.
[6] A. Leuciuc and V. Grigoras, Multi-Parameter Chaos Modulation of Discrete-Time Filters", in Proc. Workshop Nonlinear Dynamics of Electronic Systems (NDES ´97), 1997, pp.81-86.
[7] S. Papadimitriou, A. Bezerianos and T. Bountis, Secure Communication with Chaotic Systems of Difference Equations, IEEE Trans. Comput., Vol.46, 1997, pp. 27.
[8] H. Zhou and X. T. Ling, Problems with the Chaotic Inverse System Encryption Approach, IEEE Trans. Circuits Syst. I, Vol.44, 1997, pp.268-271.
[9] B. Schneier, Applied Cryptography: Protocols, Algorithms and Sourse Code in C, New York, NY: John Wiley; second edition, 1996.
[10] A. J. Menezes, P. C. Van Oorschot and S. A. Vansttone, Handbook of Applied Cryptography, Boca Raton, FL: CRC Press, 1997.
[11] J. C. A. Van Der Luubbe, Basic Methods of Cryptography, Cambridge, UK: Cambridge University Press, 1999.
[12] J. A. Buchmann, Introduction of Cryptography, New York, NY: Springer-Verlag, 2001.
[13] S. C. Coutinho, The Mathematics of Ciphers: Number Theory and RSA Cryptography, Natick MA: A. K. Peters Ltd, 1999.
[14] I. F. Blake, G. Seroussi and N. P. Smart, Elliptic Curves in Cryptography, Cambridge, UK: Cambridge University Press, 1999.
[15] A. Leuciuc, The Realization of Inverse System for Circuits Containing Nullors with Application in Chaos Synvhronization, Int. J. Circ. Theory Appl. Vol.26, 1998, pp.1-12.
[16] Ch. Volos, I. M. Kyprianidis and I. N. Stouboulos, Synchronization of Two Chaotic Duffing-type Electrical Oscillators, in Proc. 10th WSEAS Int. Conference on Circuits, Vouliagmeni, Athens, July 2006, pp.179-184.
[17] Ch. Volos, I. M. Kyprianidis and I. N. Stouboulos, Designing a Coupling Scheme between two Chaotic Duffing-type Electrical Oscillators, WSEAS Trans. Circuits Syst., Issue 7, Vol.5, 2006, pp.985-992.