A System Theory Approach for Designing Cryptosystems Based on Hyperchaos

Giuseppe Grassi and Saverio Mascolo

***Abstract*—In this paper a general methodology for designing chaotic and hyperchaotic cryptosystems is developed. The basic idea is to make the decrypter a nonlinear observer for the state of the encrypter. Referring to this concept, some propositions are given which enable the plaintext to be retrieved if proper structural properties of the chaotic system hold. The proposed tool proves to be powerful and flexible, since a wide class of cryptosystems can be designed by exploiting different chaotic and hyperchaotic circuits. The advantages of the suggested approach are illustrated in detail. In particular, the utilization of hyperchaos-based cryptosystems, as well as the increased complexity of the transmitted signal, make a contribution to the development of communication systems with higher security.**

***Index Terms*— Cryptosystems design, observers, synchronization of hyperchaotic systems.**

I. Introduction

Recently, synchronization of chaotic systems and its application to secure communications have received considerable attention [1]–[4]. Different methods have been developed in order to hide the contents of a message using chaotic signals. However, the attacks proposed in [5]–[8] have shown that most of these methods are not secure or have a low security.

These considerations have led the authors of [9] and [10] to propose a new chaos-based secure communication scheme. In particular, they have combined both conventional cryptographic method and synchronization of chaotic systems, so that the level of security is enhanced. However, these approaches are based on the synchronization properties of Chua's circuit [9] and Chua's oscillator [10], respectively. This feature represents a limitation, since the cryptosystem design may fail if different chaotic circuits are utilized.

The aim of this paper is to develop a more general approach to cryptography based on chaotic systems. This objective is achieved by designing the decrypter as a nonlinear observer [11], [12] for the state of the encrypter. In particular, some propositions are given which enable the plaintext to be retrieved if proper structural properties of the chaotic system hold. The proposed technique proves to be flexible, since different cryptosystems can be designed by making use of several chaotic [13]–[15] and hyperchaotic circuits [16]–[21]. Furthermore, the effectiveness of the communication scheme is enhanced, since both the adoption of hyperchaotic systems and the increased complexity of the transmitted signal enable us to weaken the low-security objections to low-dimensional chaos-based schemes [10].

II. Design of Chaotic and Hyperchaotic Cryptosystems

The proposed design framework consists of four parts.

Part 1: The chaotic (or hyperchaotic) system is described by the following state equations:

$$\dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}f(\boldsymbol{x}) + \boldsymbol{c} \tag{1}$$

where $\boldsymbol{x} \in \Re^{n\times 1}$, $\boldsymbol{A} \in \Re^{n\times n}$, $\boldsymbol{b} \in \Re^{n\times 1}$, $\boldsymbol{c} \in \Re^{n\times 1}$, and f: $\Re^n \to \Re$.

Part 2: Given a plaintext signal $p(t)$, the ciphertext is

$$e_{en}(t) = e_{en}(p(t), K(t)) \tag{2}$$

where $e_{en}(\cdot)$ is a generic encryption function that makes use of a key signal $K(t)$ [22]. By adopting symmetric algorithms (i.e., by using the same key for encryption and decryption), the plaintext is obtained from the ciphertext $e_{en}(t)$ as follows:

$$p(t) = d(e_{en}(t), K(t)) \tag{3}$$

where $d(\cdot)$ is the decryption function [22]. Since in chaotic cryptosystems the idea is to exploit (1) for generating the key signal $K(t)$, it is assumed that

$$K(t) = K(\boldsymbol{x}(t)), \qquad \text{where } K\colon \Re^n \to \Re. \tag{4}$$

Part 3: Given the chaotic system (1), the key (4), and the ciphertext (2), the encrypter is a dynamic system described by the equations

$$\dot{\boldsymbol{x}} = \boldsymbol{A}\boldsymbol{x} + \boldsymbol{b}f(\boldsymbol{x}) + \boldsymbol{c} + \boldsymbol{b}e_{en}(t). \tag{5}$$

In order to retrieve the plaintext, it is necessary to generate the key at the receiver, that is, synchronization between the encrypter and decrypter must be guaranteed [9]. Herein, this objective is achieved by designing the decrypter as a nonlinear observer for the state of the encrypter. It should be pointed out that an observer is a dynamic system designed to be driven by the output of another dynamic system (plant) and having the property that the state of the observer converges to the state of the plant [11], [12]. Therefore, the fourth part of the design framework is the following.

Part 4: Given the encrypter (5), the decrypter is the dynamic system

$$\dot{\boldsymbol{y}} = \boldsymbol{A}\boldsymbol{y} + \boldsymbol{b}f(\boldsymbol{y}) + \boldsymbol{c} + \boldsymbol{g}(z - s(\boldsymbol{y})) \tag{6}$$

where $\boldsymbol{g}$: $\Re \to \Re^n$ is a suitably chosen nonlinear function, $z(t)$ is a scalar signal, which is transmitted through a public channel, whereas $s(\boldsymbol{y})$ is a scalar output of the chaotic system.

Taking into account the previous considerations, (6) has to be designed so that $\boldsymbol{y}$ converges to state $\boldsymbol{x}$ as $t \to \infty$, that is, $\boldsymbol{e}(t) = (\boldsymbol{y}(t) - \boldsymbol{x}(t)) \to \boldsymbol{0}$ as $t \to \infty$ where $\boldsymbol{e}$ represents the synchronization error [11]. If $\boldsymbol{e}(t) \to \mathrm{o}$ as $t \to \infty$ for any initial condition $\boldsymbol{y}(0)$, $\boldsymbol{x}(0)$, system (6) is said to be a global observer of (5) [12]. This means that the synchronization error system has a globally asymptotically stable equilibrium point for $\boldsymbol{e} = \boldsymbol{0}$.

A block diagram illustrating the proposed approach is reported in Fig. 1.

By exploiting system theory, a proposition is given which enables a cryptosystem to be designed if a structural property of system (1) holds.

Proposition 1: If the $n \times n$ matrix

$$\lfloor \boldsymbol{b} \quad \boldsymbol{A}\boldsymbol{b} \quad \boldsymbol{A}^2\boldsymbol{b} \quad \cdots \quad \boldsymbol{A}^{n-1}\boldsymbol{b} \rfloor \tag{7}$$

is full rank, then the decrypter (6) becomes a global observer of the encrypter (5) by taking

$$\boldsymbol{g}(z - s(\boldsymbol{y})) = \boldsymbol{b} \cdot (z - s(\boldsymbol{y})) \tag{8}$$

$$z = f(\boldsymbol{x}) + \boldsymbol{k}\boldsymbol{x} + e_{en}(t) \tag{9}$$

$$s(\boldsymbol{y}) = f(\boldsymbol{y}) + \boldsymbol{k}\boldsymbol{y} \tag{10}$$

where $\boldsymbol{k} = [k_1, k_2, \cdots, k_n] \in \Re^{1\times n}$ must be chosen so that the eigenvalues of $(\boldsymbol{A} - \boldsymbol{b}\boldsymbol{k})$ lie in the open left-half plane.

Manuscript received January 7, 1998; revised June 15, 1998. This paper was recommended by Associate Editor T. Roska.

G. Grassi is with the Dipartimento di Matematica, Università di Lecce, 73100 Lecce, Italy (e-mail: grassi@ingle01.unile.it).

S. Mascolo is with the Dipartimento di Elettrotecnica ed Elettronica, Politecnico di Bari, 70125 Bari, Italy (e-mail: mascolo@poliba.it).

Publisher Item Identifier S 1057-7122(99)07207-4.

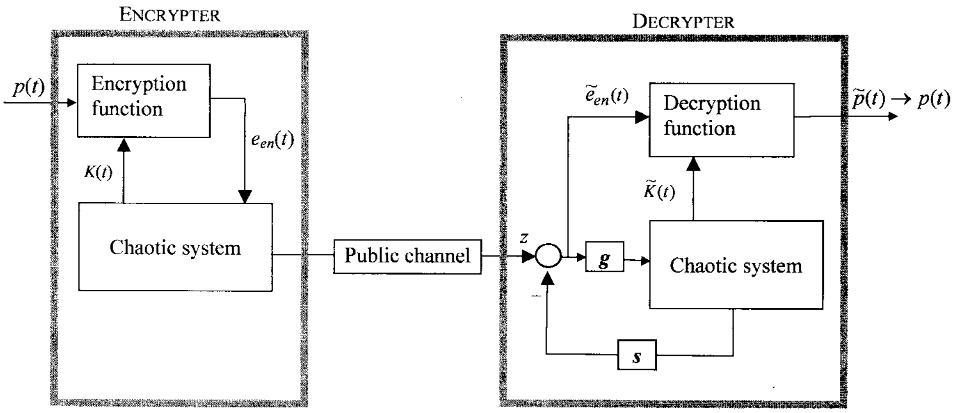

Fig. 1. A block diagram illustrating the proposed approach.

Proof: By making use of (8)–(10), the synchronization error system between (6) and (5) can be written as

$$\begin{aligned}\dot{e} &= \boldsymbol{Ay} + \boldsymbol{b}f(\boldsymbol{y}) + \boldsymbol{c} + \boldsymbol{g}(z - s(\boldsymbol{y}))\\ &\quad - (\boldsymbol{Ax} + \boldsymbol{b}f(\boldsymbol{x}) + \boldsymbol{c} + \boldsymbol{b}e_{en}(t))\\ &= \boldsymbol{Ae} + \boldsymbol{b}f(\boldsymbol{y}) + \boldsymbol{b}(f(\boldsymbol{x}) + \boldsymbol{kx} + e_{en}(t) - (f(\boldsymbol{y}) + \boldsymbol{ky}))\\ &\quad - \boldsymbol{b}f(\boldsymbol{x}) - \boldsymbol{b}e_{en}(t)\end{aligned}$$

that is

$$\dot{e} = \boldsymbol{Ae} - \boldsymbol{bke} = \boldsymbol{Ae} + \boldsymbol{b}u. \tag{11}$$

Equation (11) represents a linear time-invariant single-input dynamic system where $\boldsymbol{u} = -\boldsymbol{ke}$ plays the role of a state feedback. Since (7) is the controllability matrix of (11), if (7) is full rank, all the eigenvalues of (11) are controllable, i.e., they can be placed anywhere by proper feedback gain vector $\boldsymbol{k}$ [23]. It can be concluded that (6) becomes a global observer of (5), provided that the eigenvalues of $(\boldsymbol{A} - \boldsymbol{bk})$ lie in the open left-half plane. ○

If the matrix (7) is not full rank, it is well known that (11) can be transformed to the Kalman controllable canonical form [24]

$$\dot{\bar{\boldsymbol{e}}} = \begin{bmatrix} \overline{\boldsymbol{A}}_{11} & \overline{\boldsymbol{A}}_{12} \\ 0 & \overline{\boldsymbol{A}}_{22} \end{bmatrix} \bar{\boldsymbol{e}} + \begin{bmatrix} \bar{\boldsymbol{b}}_1 \\ \boldsymbol{0} \end{bmatrix} \boldsymbol{u} \tag{12}$$

where $\{\overline{\boldsymbol{A}}_{11}, \bar{\boldsymbol{b}}_1\}$ is controllable. From (12) it follows that $\{\boldsymbol{A}, \boldsymbol{b}\}$ is stabilizable if all the eigenvalues of $\overline{\boldsymbol{A}}_{22}$ have negative real parts [24].

Now it is proved that the plaintext is retrieved from the ciphertext using the key $\tilde{K}(t) = K(\boldsymbol{y}(t))$, generated by the decrypter (6).

Proposition 2: Let

$$\tilde{e}_{en}(t) = z - s(\boldsymbol{y}) \tag{13}$$

be the ciphertext recovered by the decrypter, and let

$$\tilde{p}(t) = d(\tilde{e}_{en}(t), \tilde{K}(t)) \tag{14}$$

be the plaintext retrieved using $\tilde{e}_{en}(t)$ and $\tilde{K}(t)$. If (6) is a global observer of (5), it results

$$\tilde{p}(t) \to p(t). \tag{15}$$

Proof: If (6) is a global observer of (5), $\boldsymbol{y} \to \boldsymbol{x}$ as $t \to \infty$ for any initial condition. As a consequence, $K(\boldsymbol{y}(t)) \to K(\boldsymbol{x}(t))$, that is, $\tilde{K}(t) \to K(t)$. Moreover, from (9), (10), and (13) it follows that $\tilde{e}_{en}(t) \to e_{en}(t)$. Finally, the comparison between (3) and (14) clearly shows that (15) holds. ○

III. Example

In order to illustrate the proposed approach, a hyperchaotic cryptosystem is now designed. It is based on the Matsumoto–Chua–Kobayashi circuit [17], which has been the first example of experimental observation of hyperchaos from a real physical system. The circuit dynamics are described by the following equations in dimensionless form [20]:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0.7 & 0 & 0 \\ 0 & 0 & 0 & -10 \\ 0 & 0 & 1.5 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} -1 \\ 0 \\ 10 \\ 0 \end{bmatrix} g(x_1, x_3) \tag{16}$$

where $g(\cdot)$ is the piecewise-linear function given by

$$g(x_1, x_3) = \begin{cases} -0.2 + 3(x_1 - x_3 + 1), & x_1 - x_3 < -1, \\ -0.2(x_1 - x_3), & -1 \le x_1 - x_3 \le 1, \\ -0.2 + 3(x_1 - x_3 - 1), & x_1 - x_3 > 1. \end{cases}$$

Since the matrix (7) is full rank, the proposed method will surely succeed in designing the desired cryptosystem. In order to encrypt the plaintext, an n-shift cipher is chosen [9]

$$e_{en}(t) = f_1(\cdots f_1(f_1(p(t), K(t)), K(t)), \cdots, K(t)) \tag{17}$$

where

$$f_1(x, K) = \begin{cases} (x + K) + 2h & -2h \le (x + K) \le -h, \\ (x + K) & -h < (x + K) < h, \\ (x + K) - 2h & h \le (x + K) \le 2h. \end{cases} \tag{18}$$

$p(t) = \sin t$, $h = 3$, and $n = 30$. For the sake of simplicity, the key $K(t) = x_4(t)$ has been chosen, although any generic function $K(\boldsymbol{x})$ could be used. Equations (5) and (6) can be written as

$$\begin{aligned}\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} &= \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0.7 & 0 & 0 \\ 0 & 0 & 0 & -10 \\ 0 & 0 & 1.5 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}\\ &\quad + \begin{bmatrix} -1 \\ 0 \\ 10 \\ 0 \end{bmatrix} g(x_1, x_3) + \begin{bmatrix} -1 \\ 0 \\ 10 \\ 0 \end{bmatrix} e_{en}(t)\end{aligned} \tag{19}$$

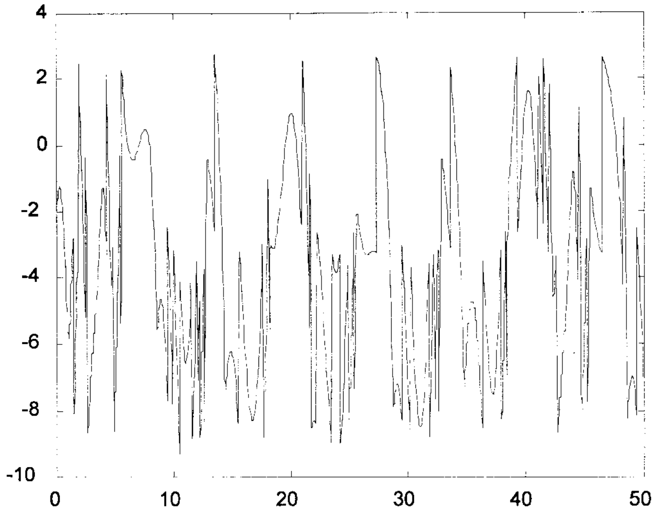

Fig. 2. Time waveform of the transmitted signal (21).

$$\begin{bmatrix}\dot y_1\\ \dot y_2\\ \dot y_3\\ \dot y_4\end{bmatrix} = \begin{bmatrix}0 & -1 & 0 & 0\\ 1 & 0.7 & 0 & 0\\ 0 & 0 & 0 & -10\\ 0 & 0 & 1.5 & 0\end{bmatrix}\begin{bmatrix}y_1\\ y_2\\ y_3\\ y_4\end{bmatrix} + \begin{bmatrix}-1\\ 0\\ 10\\ 0\end{bmatrix} g(y_1, y_3) + \begin{bmatrix}-1\\ 0\\ 10\\ 0\end{bmatrix} \cdot \left(z - g(y_1, y_3) - \sum_{i=1}^{4} k_i y_i\right) \tag{20}$$

where the observed quantity z is the scalar transmitted signal

$$z(t) = g(x_1, x_3) + \sum_{i=1}^{4} k_i x_i + e_{en}(t). \tag{21}$$

By placing the eigenvalues of system (11) in -1, it results $k_1 = -0.3764$, $k_2 = 0.2384$, $k_3 = 0.4324$, $k_4 = -0.4314$ and the decrypter (20) becomes a global observer of the encrypter (19). From (13) the ciphertext recovered by the decrypter is

$$\tilde e_{en}(t) = z - g(y_1, y_3) - \sum_{i=1}^{4} k_i y_i \tag{22}$$

whereas from (14), the following plaintext is obtained:

$$\tilde p(t) = f_1(\cdots f_1(f_1(\tilde e_{en}(t), -\tilde K(t)), -\tilde K(t)), \cdots, -\tilde K(t)) \tag{23}$$

where the decryption rule is the same as the encryption one [9], with $\tilde K(t) = y_4(t)$. From Proposition 2, it follows that $\tilde p(t) \rightarrow p(t)$. The validity of the proposed theoretic approach is confirmed by simulation results. In particular, the transmitted signal (21) is shown in Fig. 2, whereas the recovered plaintext (23) is shown in Fig. 3.

IV. Discussion

Now, the advantages of the proposed approach are illustrated.

1) The methods proposed in [9] and [10] are closely related to Chua's circuit and Chua's oscillator, respectively. In particular, the configuration in [9] guarantees synchronization since the error system $\dot e = \boldsymbol{A}e$ is characterized by eigenvalues of $\boldsymbol{A}$ in the open left-half plane [2]. Unfortunately, this hypothesis on $\boldsymbol{A}$ is not satisfied for several chaotic systems [12]. Unlike [9] and [10], in this paper any chaotic system in the form (1) can be used, provided that the error system $\dot{\boldsymbol{e}} = \boldsymbol{Ae} + \boldsymbol{b}u$ is stabilizable via state feedback $u = -\boldsymbol{ke}$.

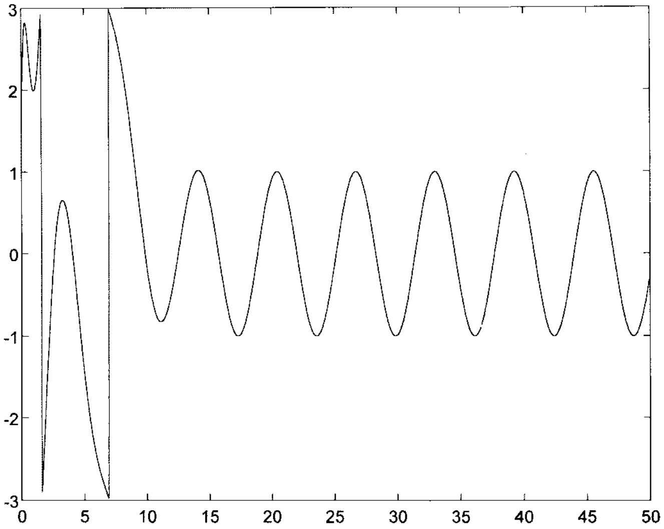

Fig. 3. Time waveform of the recovered plaintext (23).

2) By computing the rank of (7) or the eigenvalues of $\overline{\boldsymbol{A}}_{22}$, it can be easily shown that the encrypter (5) and the decrypter (6) can include several chaotic systems, such as Chua's circuit, Chua's oscillator, higher dimensional Chua's circuits [13], and the chaotic circuits proposed in [14] and [15].
3) Regarding hyperchaos, the proposed cryptosystem can include Rössler's system [16], the Matsumoto–Chua–Kobayashi circuit [17] and its modified version [20], the oscillators in [18] and [19], and the circuit with hysteretic nonlinearity in [21]. This is because they are all examples of hyperchaotic systems for which (7) is full rank.
4) In relation to the concept illustrated in [25], one could design a communications system with one encrypter and multiple decrypters. Let $\{\boldsymbol{A}, \boldsymbol{b}\}$ be stabilizable and let $\boldsymbol{k}_1, \boldsymbol{k}_2, \cdots, \boldsymbol{k}_m$ be m different gain vectors. In this case, the communications scheme is constituted by one encrypter and m decrypters. The encrypter's $\boldsymbol{k}$ can be tuned to switch from one specific decrypter to another. In this way, the components of $\boldsymbol{k}_1$, $\boldsymbol{k}_2$, $\cdots$, $\boldsymbol{k}_m$ at the decrypters constitute a synchronization address, in the sense that the only receiver that will synchronize to the transmitter is the one with the same $\boldsymbol{k}$.
5) The tool developed herein is flexible and powerful, since a wide class of cryptosystems can be designed by making use of different circuits as well as multiple decrypters.
6) The suggested approach enables synchronization to be achieved via a scalar transmitted signal. This is a remarkable feature, since a single channel is usually available for communication applications [25].
7) If (7) is full rank, all the modes of system (11) can be arbitrarily assigned. As a consequence, it is possible to generate cryptosystems characterized by short synchronization times, in order to avoid having part of the message lost during the transient behavior. Nevertheless, if $\{\boldsymbol{A}, \boldsymbol{b}\}$ is stabilizable, synchronization is practically achieved after the time 4τ, where τ is the largest time constant deriving from the uncontrollable part of system (12).
8) The proposed class of cryptosystems does not require initial conditions of (5) and (6) belonging to the same basin of attraction. This represents another remarkable feature of the method developed herein [25].
9) Low-dimensional chaotic systems exhibit very regular geometric structures when viewed in some suitable phase space

[5]. For these systems, it is possible to reveal the hidden information by creating the geometric structure with a forecasting approach [6]. However, when the chaotic dynamics are more complex, the forecasting approach may fail, since it becomes difficult to recreate the underlying geometric structure in the phase space [8]. Thus, a way to improve the level of security is surely the adoption of hyperchaotic systems [8], [25].

10) The security of a communications scheme can be enhanced by making the transmitted signal more complex [5], [10]. In particular, in [5] it is suggested that two chaotic signals can be added together to create a carrier signal of sufficient complexity. In this way, it is not possible to predict the carrier dynamics based on a reconstruction of the geometric structure in the phase space [5]. The present paper makes a further contribution in this direction, since a transmitted signal of high complexity is used. Namely, in (9) the first addend is related to the nonlinear element of the chaotic circuit, the second one is a linear combination of all the chaotic state variables, whereas the third one is the ciphertext.

11) The forecasting approach developed in [5] and [6] enables the behavior of the chaotic carrier to be predicted in low-dimensional systems. Although this is hard to do for hyperchaotic systems, consider the transmitted signal (21) and suppose that the carrier $z'(t) = g(x_1, x_3) + \sum_{i=1}^{4} k_i x_i$ is reconstructed in some way by an intruder. By considering the results available in the literature, it seems that it is not possible for an intruder to reconstruct the key $x_4(t)$ starting from a completely different signal $z'(t)$. This conjecture leads to the conclusion that, even if the ciphertext $e_{en}(t) = z(t) - z'(t)$ is reconstructed, it is not possible for an intruder to obtain the plaintext $p(t)$.

12) Although the suggested approach presents several advantages, two issues need to be further investigated. The first one regards the truthfulness of the above mentioned conjecture, whereas the second one is related to the practical implementation of the proposed method.

V. Conclusion

In this paper a general framework for hyperchaos-based cryptography has been developed. By applying the proposed technique, it is possible to design cryptosystems based on different chaotic and hyperchaotic circuits. This objective has been achieved by making the decrypter a nonlinear observer for the state of the encrypter. Finally, the advantages of the suggested approach have been discussed in detail. Taking into account the considerations reported in [25], it can be concluded that the proposed approach has most of the features that are desirable in private and secure communications systems. In particular, the utilization of hyperchaotic cryptosystems, as well as the increased complexity of the transmitted signal, seem to make a further contribution to the development of communication systems with higher security.

Acknowledgment

The authors are grateful to the reviewers for their valuable comments and suggestions.

References

[1] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, “Synchronization of Lorenz-based chaotic circuits with applications to communications,” *IEEE Trans. Circuits Syst.,* vol. 40, pp. 626–633, Oct. 1993.

[2] C. W. Wu and L. O. Chua, “A simple way to synchronize chaotic systems with applications to secure communication systems,” *Int. J. Bifurcation Chaos,* vol. 3, no. 6, pp. 1619–1627, 1993.

[3] T. Kapitaniak, *Controlling Chaos.* San Diego, CA: Academic, 1996.

[4] H. Leung and J. Lam, “Design of demodulator for the chaotic modulation communication system,” *IEEE Trans. Circuits Syst.,* vol. 44, pp. 262–267, Mar. 1997.

[5] K. M. Short, “Steps toward unmasking secure communications,” *Int. J. Bifurcation Chaos,* vol. 4, no. 4, pp. 959–977, 1994.

[6] ———, “Unmasking a modulated chaotic communications scheme,” *Int. J. Bifurcation Chaos,* vol. 6, no. 2, pp. 367–375, 1996.

[7] T. Yang, “Recovery of digital signals from chaotic switching,” *Int. J. Circuit Theory Appl.,* vol. 23, no. 6, pp. 611–615, 1995.

[8] C. Zhou and T. Chen, “Extracting information masked by chaos and contaminated with noise: Some considerations on the security of communication approaches using chaos,” *Phys. Lett. A,* vol. 234, pp. 429–435, 1997.

[9] T. Yang, C. W. Wu, and L. O. Chua, “Cryptography based on chaotic systems,” *IEEE Trans. Circuits Syst.,* vol. 44, pp. 469–472, May 1997.

[10] T. Yang and L. O. Chua, “Impulsive control and synchronization of nonlinear dynamical systems and application to secure communication,” *Int. J. Bifurcation Chaos,* vol. 7, no. 3, pp. 645–664, 1997.

[11] H. Nijmeijer and I. M. Y. Mareels, “An observer looks at synchronization,” *IEEE Trans. Circuits Syst. I (Special Issue on Chaos Synchronization, Control, and Applications),* vol. 44, pp. 882–890, Oct. 1997.

[12] G. Grassi and S. Mascolo, “Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal,” *IEEE Trans. Circuits Syst. I (Special Issue on Chaos Synchronization, Control and Applications),* vol. 44, pp. 1011–1014, Oct. 1997.

[13] M. Gotz, U. Feldmann, and W. Schwarz, “Synthesis of higher dimensional Chua circuits,” *IEEE Trans. Circuits Syst.,* vol. 40, pp. 854–860, Nov. 1993.

[14] A. Namajunas and A. Tamasevicius, “Simple RC chaotic oscillator,” *Electron. Lett.,* vol. 32, no. 11, pp. 945–946, 1996.

[15] A. Tamasevicius, “Reproducible analogue circuit for chaotic synchronization,” *Electron. Lett.,* vol. 33, no. 13, pp. 1105–1106, 1997.

[16] O. E. Rössler, “An equation for hyperchaos,” *Phys. Lett.,* vol. 71A, no. 2/3, pp. 155–157, 1979.

[17] T. Matsumoto, L. O. Chua, and K. Kobayashi, “Hyperchaos: Laboratory experiment and numerical confirmation,” *IEEE Trans. Circuits Syst.,* vol. 33, pp. 1143–1147, Nov. 1986.

[18] A. Tamasevicius, A. Namajunas, and A. Cenys, “Simple 4D chaotic oscillator,” *Electron. Lett.,* vol. 32, no. 11, pp. 957–958, 1996.

[19] A. Tamasevicius, A. Cenys, G. Mykolaitis, A. Namajunas, and E. Lindberg, “Hyperchaotic oscillators with gyrators,” *Electron. Lett.,* vol. 33, no. 7, pp. 542–544, 1997.

[20] A. Tamasevicius, “Hyperchaotic circuits: State of the art,” in *Proc. 5th Int. Workshop Nonlinear Dynamics Electronic Systems (NDES’97),* Moscow, Russia, 1997, pp. 97–102.

[21] T. Saito, “An approach toward higher dimensional hysteresis chaos generators,” *IEEE Trans. Circuits Syst.,* vol. 37, pp. 399–409, Mar. 1990.

[22] D. Stinson, *Cryptography: Theory and Practice.* Boca Raton, FL: CRC, 1995.

[23] W. L. Brogan, *Modern Control Theory.* Englewood Cliffs, NJ: Prentice-Hall, 1991.

[24] C. T. Chen, *Linear System Theory and Design.* Holt, Rinehart and Winston, 1984.

[25] L. M. Pecora, T. L. Carroll, G. Johnson, and D. Mar, “Volume-preserving and volume-expanding synchronized chaotic systems,” *Phys. Rev. E,* vol. 56, no. 5, pp. 5090–5100, 1997.