Applied Mathematics and Computation 218 (2012) 11799–11805

Contents lists available at SciVerse ScienceDirect

Applied Mathematics and Computation

journal homepage: www.elsevier.com/locate/amc

Design and implementation of the Sprott chaotic secure digital communication systems

Yi-You Hou [a], Hsin-Chieh Chen [b,*], Jen-Fuh Chang [c], Jun-Juh Yan [d], Teh-Lu Liao [c]

[a] Department of Electrical Engineering, Far East University, Tainan 74448, Taiwan
[b] Department of Biomedical Engineering, Hungkuang University, Taichung 43302, Taiwan
[c] Department of Engineering Science, National Cheng Kung University, Tainan 701, Taiwan
[d] Department of Computer and Communication, Shu-Te University, Kaohsiung 824, Taiwan

ARTICLE INFO

Keywords:
Synchronization
Sprott chaotic systems
Proportional-integral-derivative (PID)
Voltage controlled oscillator
Secure communication

ABSTRACT

In this paper, synchronization of Sprott chaotic systems and its application in secure communication are presented. We first utilize a proportional-integral-derivative (PID) control scheme to solve the synchronization problem of chaotic systems. Then for the purpose of application to secure communication, a state signal of the analog chaotic system is converted to a digital train with variable pulse width (square wave with random frequency) by voltage controlled oscillator (VCO). The original digital message is masked by the digital train generated from VCO in the chaotic transmitter via a logical exclusive-OR (XOR) operation and it can be successfully recovered by another VCO and XOR operation at the chaotic receiver due to the synchronization. To verify the system performance, basic electronic components containing operational amplifiers (OPAs), resistors and capacitors are used to implement the proposed PID-based chaotic secure communication system. Finally, the experimental results validate the proposed chaotic communication approach.

1. Introduction

A chaotic system is a very complex, dynamic nonlinear system and its response possesses intrinsic characteristics such as broadband noise-like waveform, prediction difficulty, sensitivity to initial condition variations, etc [1,2]. These properties offer some advantages in secure communication systems. Therefore, the synchronization of chaotic circuits for the secure communication has received much attention in the literature [3–6]. Based on the research reports in the literature, it reveals it is possible to setup a chaotic communication system to obtain a secure communication [7]. For achieving synchronization between two chaotic systems, the proportional-integral-derivative (PID) control is an effectively technique. However, the parameters for the PID controller must be applicable. There are some efficient selection mechanisms of parameters have been provided by genetic algorithm (GA), evolutionary programming (EP), particle swarm optimization (PSO), and also have been verified the success in tuning parameters of PID controller [8–12].

On the other hand, today, digital signals are extensively being used in commercial applications such as multimedia systems, mobile and wireless communications. Among all traditional analog-based secure communication scheme, chaotic switching (chaotic shift keying, CSK) is used to transmit digital signals. The binary CSK is widely studied where two different chaotic systems are present at the transmitter. Depending on the binary information bit (0-bit or 1-bit), one of these chaotic systems is selected to mask the digital message. Therefore, the employed chaotic system is switched from time to time. At

* Corresponding author.
E-mail address: hcchen@sunrise.hk.edu.tw (H.-C. Chen).

0096-3003/$ - see front matter
http://dx.doi.org/10.1016/j.amc.2012.04.076

the receiver, the digital message can be recovered according to which slave system can achieve synchronization with its corresponding master one. However, it has been shown that the transmission time of each bit should be long enough and transmission rate of CSK is generally slower than that of chaotic masking and modulation schemes [13].

Since EP algorithm has been proved as a useful technique for global optimization of complex functions [14–16], we first propose a proportional-integral-derivative (PID) control scheme based on EP algorithm to solve the synchronization problem of chaotic systems. The proposed PID controller is used to guarantee the synchronization between the transmitter and the receiver in communication systems. Thus, it can ensure that the digital message masked by digitized chaos state in the transmitter can be recovered in the receiver and high performance communication can be obtained by the proposed chaotic secure digital communication system.

To verify the system performance, a PID-based chaotic secure digital communication system is proposed in which two chaotic Sprott circuits (transmitter and receiver) and an EP-PID controller are implemented by using some electronic components containing OPAs, resistors and capacitors, etc. In addition, the encryption and decryption operations are realized by two voltage controlled oscillators (VCO), two XOR logic gates. Finally, the experimental results are given to verify the proposed EP-based PID scheme's success in the communication application.

2. Problem statement and preliminaries

The aim of this paper is to utilize the unpredictable characteristics of chaos signal, such as broadband noise-like waveform, prediction difficulty, sensitivity to initial condition variations, to construct a secure digital communication system. To achieve this goal involves two basic steps: (1) selecting an appropriate controller such that the master–slave chaotic systems can be synchronized; and (2) establishing a new method to digitize the chaotic state to mask the original digital information. Now we consider the following Sprott circuits, which are typical chaotic systems that have been thoroughly studied [17].

Master Sprott circuit:

$$\begin{aligned}
\dot{x}_{m1} &= x_{m2}\\
\dot{x}_{m2} &= x_{m3}\\
\dot{x}_{m3} &= -1.2x_{m1} - x_{m2} - 0.6x_{m3} + 2sign(x_{m1})\\
y_m &= x_{m1}
\end{aligned} \tag{1}$$

Slave Sprott circuit:

$$\begin{aligned}
\dot{x}_{s1} &= x_{s2}\\
\dot{x}_{s2} &= x_{s3} + u\\
\dot{x}_{s3} &= -1.2x_{s1} - x_{s2} - 0.6x_{s3} + 2sign(x_{s1})\\
y_s &= x_{s1}
\end{aligned} \tag{2}$$

where $\dot{x}_m$ and $\dot{x}_s$ denote the derivative of x_m and x_s with respect to time $t^{'}$, respectively. In order to speed up the dynamic response of Sprott chaotic circuit, we rescale the systems (1) and (2) by a new time variable $t = \frac{t'}{C}$, and then we have the following systems (3) and (4), respectively

$$\begin{aligned}
\dot{x}_{m1} &= C(x_{m2})\\
\dot{x}_{m2} &= C(x_{m3})\\
\dot{x}_{m3} &= C[-1.2x_{m1} - x_{m2} - 0.6x_{m3} + 2sign(x_{m1})]\\
y_m &= x_{m1}
\end{aligned} \tag{3}$$

$$\begin{aligned}
\dot{x}_{s1} &= C(x_{s2})\\
\dot{x}_{s2} &= C(x_{s3} + u)\\
\dot{x}_{s3} &= C[-1.2x_{s1} - x_{s2} - 0.6x_{s3} + 2sign(x_{s1})]\\
y_s &= x_{s1}
\end{aligned} \tag{4}$$

where $\dot{x}_m$ and $\dot{x}_s$ denote the derivative of x_m and x_s with respect to new time variable t, respectively. C is a weighting factor to speed up the response of the Sprott chaotic circuit , and $\infty > C \geqslant 1$.

Now let us define the state errors between the master and slave systems as

$$e_1 = x_{m1} - x_{s1}, \quad e_2 = x_{m2} - x_{s2}, \quad e_3 = x_{m3} - x_{s3} \tag{5}$$

Formerly, we have presented a simple but effective PID controller based on EP algorithm to achieve the synchronization of two identical chaotic systems [9]. The term u in (2) is a PID controller obtained via EP algorithm to guarantee the synchronization performance. The procedure to determine the PID controller u is to first define the output error signal $y_e = y_m - y_s$, then the continuous-form of a PID controller, with input $y_e(\cdot)$ and output $u(\cdot)$, is generally given as