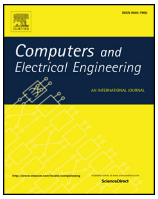
Computers and Electrical Engineering 71 (2018) 77–92

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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



Duffing oscillators for secure communication☆

Ashraf A. Zaher

Electrical and Computer Engineering Department, College of Arts and Sciences, American University of Kuwait, P. O. Box 3323, Safat 13034, Kuwait

ARTICLE INFO

Keywords:
Duffing oscillators
Chaos
Secure communication
Lyapunov-based control

ABSTRACT

This paper introduces a new technique for using chaotic Duffing oscillators in secure communication. The secret message is encrypted using the parameters of the Duffing oscillator that indirectly affect the generated chaotic orbits. The mathematical model of the chaotic transmitter uses three parameters that can be altered between two levels, depending on the binary sequence of the digital secret message and the corresponding cipher. Consequently, a total of eight chaotic attractors are used to scramble the binary-based signal. Two different structures, for the synchronization and encryption mechanisms, between the transmitter and the receiver, are introduced. The first one uses the time series of the two chaotic signals generated by the Duffing transmitter, while implementing a cipher-less encryption mechanism. The second one uses a single time series of the Duffing transmitter, while allowing one of its parameters to act as a digital cipher. Better utilization of the communication channel is proved for the second method, while using a new adaptive Lyapunov-based technique to implement both the state synchronization and the parameters estimation at the receiver side. Both simulation and experimental case studies are presented to illustrate the proposed techniques and their applicability to securely transmit various multimedia digital signals.

1. Introduction

Promoting security for communication systems has been an important application for chaos over the past few years. The rapid advances in this field of research were mainly due to introducing several synchronization techniques for chaotic systems that have a similar structure to the transmitter/receiver couple of a typical communication system [1]. The systems that have been used to design and implement chaos-based secure communication systems (CBSCs) can be classified into many different categories [2]. Using either continuous or discrete systems is a fundamental choice that affects the desired implementation method and the required bandwidth of the transmitted signals. In addition, adopting either an electronic or optical implementation may dictate the nature of the system to be used as well as its operating speed and channel bandwidth. Another category that is used in classifying CBSCs is whether the system is autonomous or nonautonomous. The Lorenz system [3] and the Chua circuit [4] are examples of the former, as they are free-running systems that do not require an external driving force, while the Duffing oscillator [5] is an example of the latter that needs to have a persistent exciting input. Moreover, the structure of an existing chaotic system can be made hyperchaotic via inserting additional states into the system to increase its order and the number of positive Lyapunov exponents [6]. This has the effect of enriching the chaotic behavior of the system, which makes it more appealing to hiding secret signals and making them appear like almost white noise for an intruder trying to break into the public communication channel [7].

Unlike conventional communication systems, where the transmitted signal is used directly to modulate the amplitude, frequency,

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. E. Cabal-Yepez.

E-mail address: azaher@auk.edu.kw.

https://doi.org/10.1016/j.compeleceng.2018.07.005
Received 28 December 2017; Received in revised form 8 June 2018; Accepted 11 July 2018

or phase of a carrier signal, CBSCs use a variety of other techniques that replace the *periodical* carrier with a *chaotic* signal. Direct modulation was used in [8] and additive masking was used in [9], where the chaotic signal was modulated directly by the transmitted signal, or simply added to it, respectively. However, these two methods were very sensitive to noise, which is inherent in public communication channels. In addition, they provided poor security measures [1]. For transmitting digital signals, two more techniques, known as chaotic shift keying and chaotic switching could be used, for which the two binary levels of the data correspond to two different chaotic trajectories. Single or two different chaotic systems can be used to generate these two trajectories via manipulating some of their parameters. Examples for these two methods can be found in [10]. The success of these two methods strongly depends on accomplishing very fast synchronization, while having short bit duration, which is an obvious conflict [11]. Return map techniques were successfully implemented to break their weak security [2].

New generations of CBSCs employed cryptography to achieve robustness and improved security. These new techniques combine chaotic nonlinear dynamics with soft computing and data security algorithms to provide better protection for the transmitted data [12,13]. They were successful in replacing traditional methods that rely on number theory and traditional algebraic ciphers, such as DES, AES, IDEA, and RSA, especially when dealing with multimedia processing [14,15].

The work illustrated in this paper aims to provide a hybrid technique that applies cryptography to directly alter all the parameters of a Duffing oscillator, such that multiple chaotic attractors are employed in the modulation process. The proposed mathematical model of the chaotic Duffing oscillator has three parameters. Allowing these parameters to change within prescribed ranges, such that the chaotic behavior is retained, prevents intruders from breaking into the communication channel, using traditional attacks that are based on the return maps and the like. The information in the secret digital message, which could correspond to any form of multimedia data, such as text, audio, image, or video, is distributed among all the transmitter parameters to robustify the encryption process. An adaptive Lyapunov-based technique is employed to faithfully estimate these parameters at the receiver side in order to reconstruct the original message, using a decryption algorithm. Two methods are introduced; the first one allows one of the three transmitter parameters to change randomly, while splitting the digital information of the secret message between the remaining two parameters, according to an encryption function. Two signals need to be transmitted through the communication channel to generate the estimates of the three parameters of the Duffing oscillator at the receiver side. It is demonstrated that the receiver can settle down to the true, unbiased, estimates of the parameters within an adjustable time that is fast enough to sustain the required data rate, and yet long enough to effectively establish synchronization, prior to identifying the unknown parameters. A Lyapunov-based complete synchronization method is used to achieve such a goal. The second method adds a significant improvement via allowing a single time series of the Duffing transmitter to be used. In this case, one of the three parameters, at the transmitter side, is used as a cipher of a prescribed length, replacing the randomized parameter in the first method. A slightly different encryption function algorithm is used to split the secret message between the remaining two parameters. Proof of stability and convergence to the true values for the identified parameters, at the receiver side, is established, using a modified structure for the Lyapunov function that utilizes a reconstructed signal for the transmitter state that was not sent through the communication channel. This method is considered novel, as the methodology used for structuring the Lyapunov function is new.

Most of the CBSCs, which deal with transmitting digital signals, associate the two levels of the binary-based information to only two different chaotic orbits [8–15]. This is usually done using a one-to-one mapping, as illustrated in Fig. 1-a. Of course, this results in poor security, as the association could be easily discovered [2,5], resulting in the vulnerability of reconstructing the secret information, by intruders. Utilizing more chaotic orbits for scrambling the digital information should provide better security, as one-to-many mapping results in robust scrambling of the digital information. The main contribution of this paper is providing two different control schemes that allow using four and eight different chaotic orbits for implementing the CBSC system, via utilizing two and three parameters of the Duffing oscillator, as shown in Fig. 1-b and 1-c, respectively. This is achieved via using an encryption-based algorithm, while allowing each parameter to alternate between two levels. In addition, the paper provides a systematic approach to

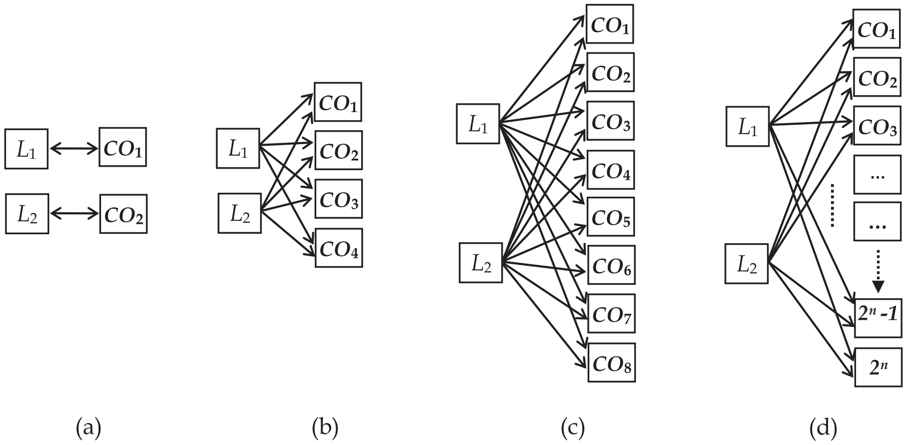


Fig. 1. Association of the binary levels of the digital signals to the chaotic orbits (COs). One-to-one mapping is shown in (a), while one-to-many mapping is shown in (b), (c), and (d).