Signal Processing 93 (2013) 1328–1340

Contents lists available at SciVerse ScienceDirect

Signal Processing

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

Image encryption process based on chaotic synchronization phenomena

Ch.K. Volos [a,*], I.M. Kyprianidis [b], I.N. Stouboulos [b]

[a] Department of Mathematics and Engineering Studies, Hellenic Army Academy, Athens GR-16673, Greece
[b] Physics Department, Aristotle University of Thessaloniki GR-54124, Greece

ARTICLE INFO

Article history:
Received 27 January 2012
Received in revised form
15 September 2012
Accepted 12 November 2012
Available online 20 November 2012

Keywords:
True random bits generator
Chaos
Complete synchronization
Inverse π-lag synchronization
Nonlinear circuit
Encryption

ABSTRACT

This paper presents a novel image encryption scheme, which uses a chaotic True Random Bits Generator (TRBG). The chaotic TRBG is based on the coexistence of two different synchronization phenomena. The first one is the well-known complete chaotic synchronization while the second one is a recently new proposed synchronization phenomenon, the inverse π-lag synchronization. This coexistence is observed in the case of two mutually coupled identical nonlinear circuits. The nonlinear circuit, which is used, produces double-scroll chaotic attractors. The initial conditions of the coupled system and the values of the circuit's parameters serve as the private key of the proposed cryptographic scheme. In order to face the challenge of using this chaotic TRBG in such cryptographic schemes, the produced bits sequence is subjected to statistical tests which are the well-known Federal Information Processing Standards-140-2. This bits sequence has then been used to encrypt and decrypt gray-scale images. Also, the security analysis of the encrypted image demonstrates the high security of the proposed encryption scheme.

1. Introduction

In recent years, confidentiality of information is an essential feature of the digital era since the communications over open networks occur more and more frequently. The rapid development of Internet technology appointed communication using multimedia techniques one of the most prevailing approaches of communication. Also, digital image information has become very important because of the vitality and visualization. Nevertheless in many cases, image data transferred in the Internet must not be public. So, reliable, fast and secure communication systems must be implemented to transmit images or photographs in many applications, such as photographs from military satellites, drawings of military establishment, images of medical systems, online personal photographs, images of electronic publishing and fingerprint images of authentication systems.

As it is known, digital images have some very characteristic features such as, strong correlation among adjacent pixels, bulk data capacity, redundancy of data, being less sensitive compared to the text data and existence of patterns and backgrounds. Therefore, because of these features, traditional ciphers like DES, AES, IDEA and RSA, are not suitable for real time image encryption as these ciphers require a large computational time and high computing power. Also, most of the conventional image encryption algorithms are based on position permutation. This process has the advantage of fast encryption speed but the security depends on the security of the algorithm, which do not satisfy the requirement of a modern encryption system.

Nowadays, there are two major approaches that are used to protect digital images from attackers. The first one

* Corresponding author. Tel: +30 210 2833507.
E-mail address: chvolos@gmail.com (Ch.K. Volos).

0165-1684/$ - see front matter © 2012 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.sigpro.2012.11.008

is the information hiding, such as digital watermarking of an image [1–5]. The second one is the encryption, which includes conventional encryption techniques and others such as chaotic encryption [6–11].

The rapid development of nonlinear dynamics in the last two decades and especially of chaotic dynamics makes researchers realize that chaotic systems can be used in cryptosystems [12], because of their corresponding counterparts in cryptosystems, such as the sensitivity on initial conditions and system parameters, ergodicity and topological transitivity. Also, unlike the conventional cryptographic algorithms, which are mainly based on discrete mathematics, chaos-based cryptosystems rely on the complex dynamics of nonlinear systems which are deterministic.

The first, who proposed an encryption process based on chaos, was Matthews in 1989 [13]. After him, many other researchers have proposed schemes based on chaotic systems. In 2000, Yen and Guo [14] proposed a chaotic key-based algorithm for image encryption. A year later, in 2001 a fast encryption image encryption algorithm based on vector quantization was developed [15]. Also, in the last decade, image encryption schemes based on chaotic Cat maps and Baker maps were proposed [16–18].

Furthermore, in the last decade, the security of many cryptographic systems was based on random number generators. Generators that produce random sequences can be classified into three types: True Random Number Generators (TRNGs), Pseudo-Random Number Generators (PRNGs) and Hybrid Random Number Generators (HRNGs) [19]. This classification is mainly based on the source of the randomness. The first type of these generators, TRNGs take advantage of nondeterministic sources, which come from an unpredictable natural process in a physical or hardware device that can output a sequence of statistically independent data, as opposed to PRNGs that produce numbers sequences by a computer program. As sources of random numbers may be considered the elapsed time during radioactive decay [20], the thermal and shot noise [21], the frequency instability of an oscillator [22], the variations in disk drive response times [23], the integrating dark current from a metal insulator semiconductor capacitor [24], the mouse movement [25] and the environmental noise [26].

A new approach is suggested in this paper for efficient and practical chaotic image encryption scheme. The basic idea of our method is to encrypt a gray-scale image via a chaotic True Random Bits Generator (TRBG), which is based on the interaction between two mutually coupled identical chaotic circuits [27,28]. The proposed coupled system shows the phenomenon of the coexistence of two different synchronization phenomena, the well-known complete chaotic synchronization and the recently new proposed synchronization phenomenon, the inverse π-lag synchronization [27,28]. According to a binary sequence generated from the chaotic generator, the pixels of the gray-scale image XOR-ed to the predetermined keys.

The rest of the paper is organized as follows: In Section 2 basic features of chaotic systems and the synchronization phenomena, which are the base of this work, are presented. Section 3 introduces the chaotic TRBG. In Section 4 the results of the use of a well known statistical tests suite (FIPS-140-2) are presented. Section 5 demonstrates how to encrypt and decrypt the "Lenna" images via the chaotic sequences obtained from the chaotic TRBG. In Section 6 security analysis on the proposed "Lenna" image encryption scheme, is presented. Finally, conclusion remarks are drawn in the last Section.

2. Chaotic systems and synchronization phenomena

As it known, a dynamical system in order to be considered as chaotic must fulfill the three following conditions [29]:

- It must be very sensitive on initial conditions,
- its periodic orbits must be dense and
- it must be topologically mixing.

In this work the use of coupled continuous-time chaotic systems for generating true random bits sequences in image encryption process is shown. The study of the interaction between coupled chaotic systems was a landmark in the evolution of the chaotic synchronization's theory [30]. The most well-known type of synchronization is the complete or full synchronization, in which the interaction between two identical coupled chaotic systems leads to a perfect coincidence of their chaotic trajectories, i.e.

$$x_1(t) = x_2(t) \ \text{ as } t \to \infty \tag{1}$$

where x_1 and x_2 are the signals of the coupled chaotic systems.

Although, since 2010 a new synchronization phenomenon, the inverse π-lag synchronization, between two mutually coupled identical nonlinear systems, has been observed [27,28]. This new type of synchronization is observed when the coupled system is in a phase locked (periodic) state, depending on the coupling factor and it can be characterized by eliminating the sum of two relevant periodic signals (x_1 and x_2) with a time lag τ, which is equal to $T/2$, where T is the period of the signals x_1 and x_2:

$$x_1(t) = -x_2(t+\tau), \ \ \tau = T/2 \tag{2}$$

Nevertheless, depending on the coupling factor and the chosen set of system's initial conditions, the inverse π-lag synchronization coexists with a complete synchronization [28]. So, the proposed TRBG, which is used for the image encryption, is based on the coexistence of these two types of synchronization, which are used as representing the states "0" and "1" in the seed generation, as it will be described in details in the next section.

3. The chaotic true random bits generator

The proposed chaotic TRBG, which is used, in this work, for the image encryption process, consists of three blocks (Fig. 1). The first of these blocks (S_1) includes the coupled nonlinear system, which is necessary in this TRBG. This system is based on a nonlinear Chua's like autonomous circuit which demonstrates the inverse π-lag synchronization [28,31].