Digital Signal Processing 25 (2014) 266–274

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

# Efficient neural chaotic generator for image encryption

Ali Kassem, Hussein Al Haj Hassan, Youssef Harkouss *, Rima Assaf

*Lebanese University, Faculty of Engineering, Branch III, Al-Hadath, Beirut, Lebanon*

ARTICLE INFO

*Article history:*
Available online 18 November 2013

*Keywords:*
Chaotic generator
Neural network
Perturbation
Multilayer perceptron
Phase space
NIST tests

ABSTRACT

In this paper, we propose a new implementation of chaotic generator using artificial neural network. Neural network can act as an efficient source of perturbation in the chaotic generator which increases the cycle's length, and thus avoid the dynamical degradation due to the used finite dimensional space. On the other hand, the use of neural network enlarges the key space of the chaotic generator in an enormous way. The efficiency of the proposed neural chaotic generator is illustrated using some dynamical and NIST statistical tests. We also propose in this paper, a new image encryption method based on chaotic sequence, and the obtained results emphasize the efficiency of our technique.

## 1. Introduction

Drastic growth in multimedia communication resulted to numerous security issues in the data transmission over the Internet. To meet this challenge, a variety of encryption schemes have been proposed [1–6]. Among them, chaos-based algorithms emerged to be promising. They have shown some exceptionally good properties regarding complexity, speed, computing power and computational overhead, especially in domain of image encryption. Due to some intrinsic features of images, such as bulk data capacity and high correlation among pixels, traditional encryption algorithms such as DES, AES and RSA are not suitable for practical image encryption. The main obstacle in designing image encryption algorithms is that it is rather difficult to swiftly shuffle and diffuse data by traditional means of cryptology: traditional cryptographic algorithms shuffle and diffuse data by rounds of encryption, while chaotic maps spread the initial region over the entire phase space via iterations.

Chaos has been widely studied in secure communications [7–10], and the idea of using digital chaotic systems to construct cryptosystems has been extensively studied since 1989 [11], and attracts more and more attention in the last years [12,13]. In order to use chaotic systems in image encryption, chaotic sequences must seem absolutely random (practically very close to random) and have some properties such as: balance on {0, 1}, long cycle's length, high linear complexity, $\delta$-like auto-correlation, cross-correlation near to zero, and fully distributed phase space. Existing digital chaotic generators satisfy some of these properties, but most of them suffer from short cycle's length due to the dynamical degradation caused by $2^N$-dimensional finite space [14,15]. Usually some perturbation techniques are used to avoid such degradation [16–19]. Good dynamical and randomness properties allow chaotic generators to have a resistance against analysis and correlation attacks. However, enhancing dynamical properties do not prevent brute-force attack if the generator has few parameters.

In this paper, we firstly propose a new perturbation technique based on neural network: a neural network is trained to learn a certain chaotic function, then the neural network is called every a certain period to take the place of the chaotic generator during the generation of the chaotic sequence. As chaotic generators are very sensitive to any small variation in the current iteration, the error between the neural network response and the exact response of the chaotic generator leads to a deviation from the chaotic orbit, and thus acting as a good source of perturbation that enlarges the cycle length of the chaotic sequence. Moreover, the neural network parameters (network structure, activation functions, weights and biases) enlarge key space, and thus result in a robust chaotic generator in term of security. Our techniques can be implemented in any chaotic generator. Second, we propose a neural chaotic generator based on the neural perturbation technique. Third, we propose a new image encryption algorithm based on three-dimensional (3D) chaotic map. The new algorithm, first shuffles the positions of pixels (pixels permutation) in order to fast de-correlate relations among them. Then, to confuse the relationship between cipher image and plain image, a diffusion process among pixels is performed (permutation at bits level).

Many perturbation techniques are proposed [16–19], most of them based on maximal length LFSR. These perturbation techniques allow to elongate the cycle length and to obtain better dynamical properties of the chaotic sequences [17,18]. But it has been found many guess and correlation attacks on LFSR [19–23].

* Corresponding author.
*E-mail address:* harkouss@ul.edu.lb (Y. Harkouss).

1051-2004/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.dsp.2013.11.004

Moreover, they do not solve an important problem of chaotic generators that is fewness of parameters.

Our work follows the spirit of [24] where they model the dynamics of Chua's circuit using artificial neural network aiming to enlarge the key space. They show that the neural network can deliver a similar response as the numerical solution of Chua's circuit with a small error. Note that modeling a certain chaotic generator by a neural network does not solve the dynamical degradation. However, to the best of our knowledge, no body use neural network as a source of perturbation in order to avoid the dynamical degradation caused by the digital chaotic systems. We take the advantage of neural network error to use it as a source of perturbation in order to solve the dynamical degradation problem, at the same time enlarging the key space of the chaotic generator.

In Section 2, we present some known chaotic generators. In Section 3, we present the general implementation of neural network in any chaotic generator. Then in Section 4, a new chaotic generator is proposed. In Section 5, some experimental results and comparisons are made to illustrate the efficiency of the proposed neural chaotic generator. Finally before concluding, we propose a new image encryption method in Section 6.

## 2. Presentation of known chaotic generators

In this section, we present some of the well-known chaotic generators.

### 2.1. PWLC map

A piecewise linear chaotic map (PWLCM) [17] is a map composed of multiple linear segments. It is defined by the following equation:

$$x(n) = F\big(x(n-1)\big) = \begin{cases} \frac{x(n-1)}{p} & \text{if } x(n-1) \in [0, p[ \\ \frac{x(n-1)-p}{0.5-p} & \text{if } x(n-1) \in [p, 0.5[ \\ F(1-x(n-1)) & \text{if } x(n-1) \in [0.5, 1] \end{cases} \tag{1}$$

where $p \in [0, 0.5[$ and $x(n) \in [0, 1]$. $x(0)$ and $p$ are used as secret keys.

### 2.2. Frey map

An approach to generate chaos for secure communications has been demonstrated by Frey. Frey proposed a generator with $N$ finite precision bits, which consists of a nonlinear function $F(x)$ with delayed feedback. Fig. 1 shows the structure of the chaotic generator proposed by Frey [7]. It is defined by the following equation:

$$e(n) = U(n) + \big\{e(n-1) + F\big(e(n-2)\big)\big\} \tag{2}$$

where $F$ is the left circulate function, i.e., multiplication by 2 plus the carry bit. $U(n)$, $e(n-1)$ and $e(n-2)$ are usually used as secret keys.

It's clear that PWLCM and Frey map, as most chaotic generators, suffer from small key space. For instance PWLCM has only two parameters $p$ and the initial condition, and Frey map has $U(n)$ and two initial conditions. Furthermore, since digital chaotic iterations are constrained in a discrete space with $2^N$ elements, digital chaotic generators suffer from dynamical degradation [14,15]. So that every digital chaotic orbit will eventually be periodic and will finally go to a cycle with limited length not greater than $2^N$. Fig. 2 shows a typical digital chaotic orbit, where this orbit consists of two parts: transition part $(X_0, \dots, X_L)$ and the cycle or recurrent part $(X_{L,}, \dots, X_{L+n})$. As the cycle's length increases, the generated sequence would have more possibilities and thus the probability of occurrence of a number decreases.

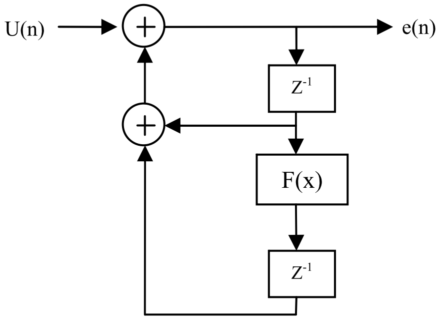

**Fig. 1.** Basic Frey generator structure.

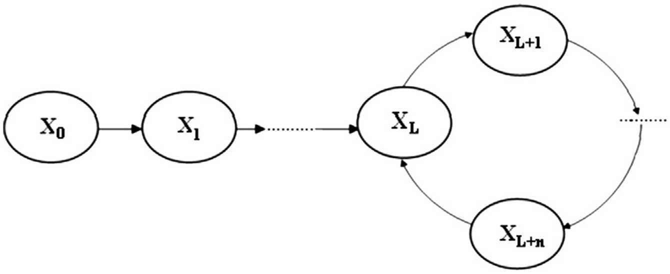

**Fig. 2.** A typical digital chaotic orbit.

These generators were already analyzed by applying NIST tests [17]. However, results showed that they do not pass successfully the considered tests. In [18], the authors show that perturbed PWLCM and Frey map have better dynamical and statistical properties than unperturbed ones, after subjecting them to NIST tests and other correlation and dynamical tests. The perturbation technique used in [18] is the one proposed in [16], it is based on LFSR. These results and many others emphasize the importance of perturbation techniques in obtaining better dynamical and statistical properties of generated chaotic sequences, as they help to obtain sequences much closer to randomness and with longer cycle.

## 3. General implementation of neural network in any chaotic generator

### 3.1. Artificial neural network: a brief overview

An artificial Neural Network (ANN) [25] is a highly parallel distributed network of connected processing units called neurons. It is motivated by the human brain which is a highly complex, nonlinear and parallel computer. The network has a series of external inputs and outputs which take or supply information to the surrounding environment. Weights and biases of the network are used to store knowledge acquired from the environment. Learning is achieved by adjusting these parameters in accordance with a learning algorithm. In general, the neural network derives its computing power from, first, the massively parallel distributed structure, and second, its ability to learn and generalize. Generalization is producing reasonable outputs (with a certain error) for the inputs not encountered during training. These two information capabilities make it possible for the neural network to solve complex problems.

One of the most used kinds of neural networks is the multilayer perceptron (MLP). Multilayer perceptrons have been applied successfully to solve some difficult diverse problems, especially in