Computers and Electrical Engineering 000 (2017) 1–17

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A novel parallel image encryption with chaotic windows based on logistic map☆

Mohamad Javad Rostami*, Abbas Shahba*, Saeid Saryazdi, Hossein Nezamabadi-pour

Department of Electrical Engineering, Shahid Bahonar University of Kerman, P.O. Box 76169-133, Iran

ARTICLE INFO

Article history:
Received 26 May 2015
Revised 5 April 2017
Accepted 6 April 2017
Available online xxx

Keywords:
Encryption
Chaotic map
Chaotic window
Gray scale image

ABSTRACT

Over the course of the last two decades, secure communication has become a very important issue due to the rapid growth of information technology and the development of public communication networks in which digital images are widely transmitted. In this paper, logistic map was employed for the encryption of gray-scale images. The proposed algorithm, demonstrating a proper performance according to the experimental results, divides the image into blocks and encrypts them with XOR operation and chaotic windows. Moreover, it has a large key space and the resulted encrypted images have homogeneous histograms. The large-enough NPCR and UACI of this algorithm indicate its resistance to differential attacks, not to mention the fact that it is suitable for noisy communication networks and could be made use of in parallel processing.

1. Introduction

Image encryption is one of the most effective ways of guaranteeing the transmission security of digital images that are being widely transmitted in the public communication networks [1].Chaotic system is a deterministic nonlinear system possessing various characteristics, such as high sensitivity to initial conditions, and determinacy [2] and has recently attracted many researchers into using it for image encryption. There exist a large number of image encryption methods owing to the variety of chaotic maps.

A novel algorithm was proposed in [3] for image encryption based on the mixture of chaotic maps. Some researchers employ hyper chaotic systems [4–10]. Hermassi et al. [4] proposed a symmetric image encryption scheme with PWLCM for creating permutation matrices in the confusion stage and Chen's chaotic system in the diffusion stage. Two image encryption algorithms were designed based on DNA sequence and hyper-chaotic system in [5] and [6]. Norouzi et al. [7] proposed an image encryption algorithm based on hyper-chaotic system with only one round of diffusion process. Parallel sub-image encryption with hyper chaos and time-delaying image encryption scheme based on hyper chaotic map were proposed in [8] and [9], respectively. Moreover, Huang et al. [10] proposed an image encryption algorithm based on Chua chaotic system with pixel and bit shuffling. Certain researchers have designed image encryption algorithms based on piecewise nonlinear chaotic maps (PWNLCM) [11–13]: Akhshani et al. [12] proposed a novel scheme for image encryption based on 2D piecewise nonlinear chaotic map with two similar stages for diffusion. Liu et al. [14] designed a method for image encryption with

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

* Corresponding authors.
E-mail addresses: rostami@uk.ac.ir (M.J. Rostami), a.shahba313@chmail.ir (A. Shahba).

http://dx.doi.org/10.1016/j.compeleceng.2017.04.004
0045-7906/

PWLCM and Chebyshev map in the confusion and diffusion stages, respectively. [15] proposed a fast chaotic block cipher for image encryption based on sorting the solutions of Linear Diophantine Equation (LDE), whose coefficients are integers dynamically generated from all types of chaotic systems. In some image encryption schemes, coupled map lattices (CML) were employed as the model of spatiotemporal chaotic systems [16,17–19]. [18] proposed a method for encrypting images using a new nonlinear chaotic algorithm (NCA) based on the logistic map in CML. An image encryption based on DNA addition and complement operation combined with 1D and 2D logistic maps was proposed in [2]. Zhang and Xiao [20] proposed an image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Furthermore, two image encryption methods were proposed in [21] and [22] based on 2D generalized Arnold map and 3D Arnold cat map, respectively. Zhang et al. [23] proposed a novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations.

1.1. Challenges and motivations

The above mentioned methods achieved satisfying results in image encryption yet have certain security drawbacks. This is despite the fact that an efficient image encryption must be able to resist any types of attacks. Differential attack is commonly used in cryptanalysis, which compares the corresponding encrypted outputs of two similar plaintexts with small changes in one of them (even only one bit). In some encryption methods, [2,6,7,10], however, hackers can change two pixels of the plaintext, increasing one pixel while decreasing the other, and subsequently comparing the two corresponding encrypted outputs. Moreover, the algorithm designed in[7] responded badly to the differential criteria for certain pixels. If a hacker changes one bit in plaintext P, the corresponding ciphertext C changes in many bits [24]. In line with this property, also called diffusion property, many researchers use encrypted pixels to encrypt next pixels in their image encryption algorithms [3,4,6–9,11–13,16–23].

Nonetheless, such diffusion structure has three major drawbacks: 1) It does not operate properly against some differential attacks. 2) It is not able to resist noise and data loss and as a result can injure the plain image: An efficient image encryption algorithm must be suitable for actual communication that inevitably involves undesirable effects such as noise and data loss. Such structure also diffuses noise over decrypted images in the receiver. 3) It is not able to include parallel processing: The effect of an encrypted pixel on another pixel leads to the sequential pixel-by-pixel encryption and prohibits parallel processing.

1.2. Our work

To overcome the above drawbacks, we propose a novel plaintext-dependent image encryption algorithm. We take a random number that depends on plaintext sensitively; then we use it to update initial values of chaotic maps. Moreover, use of two 16×16 chaotic blocks makes our algorithm suitable for parallel processing. Logistic chaotic map is used in this algorithm. This one-dimensional chaotic system has the advantages of high-level efficiency and simplicity [3,11,13,15,18], but there are fundamental drawbacks in this chaotic system, such as small key space [4,9,11,13,15–18]. To overcome this drawback, we use logistic map in image encryption several times and make initial values and parameters dependent on a value we take from the mean initial values. In some methods of image encryption, there is no permutation stage [3,7,11–13,17]. This stage enables the image encryption method to have a good behavior against the data loss attack with better security in encryption. We include this stage in our method.

The paper's contributions are:

- Satisfying the theoretical criteria including entropy, NPCR, UACI and CC while still being fast
- Parallel processing capability
- Generating a high sensitive and image dependent number that updates the initial values of chaotic map
- Simplicity and low complexity of encryption process
- High efficiency against noise and data loss attack

1.3. Paper organization

Section 1 of this paper includes the introduction and review of the literature. Section 2 presents the preliminaries of the proposed algorithm. In Section 3, the encryption process is discussed. Section 4 presents the results and security analysis of the proposed algorithm, and finally, Section 5 concludes the paper.

2. Preliminaries

In this section, the logistic map will be described along with its application in the proposed algorithm. We will then explain how to generate a random number that highly depends on the plaintext.

Please cite this article as: M.J. Rostami et al., A novel parallel image encryption with chaotic windows based on logistic map, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.004