Information Sciences 355–356 (2016) 314–327

Contents lists available at ScienceDirect

Information Sciences

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

Circular inter–intra pixels bit-level permutation and chaos-based image encryption

Adrian-Viorel Diaconu[a,b,*]

[a] Lumina – The University of South-East Europe, IT&C Department, Bucharest, 021187, Romania
[b] University Politehnica of Bucharest, ETTI Faculty, Bucharest, 061071, Romania

ARTICLE INFO

Article history:
Received 12 March 2015
Revised 27 September 2015
Accepted 9 October 2015
Available online 22 October 2015

Keywords:
Chaos-based cryptography
Image encryption
Security analysis
Inter–intra pixels bit-level permutation

ABSTRACT

The new image encryption architecture presented in this paper employs a novel circular inter–intra pixels bit-level permutation strategy. This strategy aims to reduce redundancies implied by the Fridrich's structure. The newly proposed scheme was subject to extensive security analyses, including statistical and differential analysis, and information entropy calculation. These highlight a desirable security level provided by the insurance of the coveted confusion and diffusion factors.

1. Introduction

Originating in the late 1960s, the chaos theory was already well established by the 1970s and has continued to provide valuable research material into many technological application fields. It has proved significant with regards to combined efforts into many different research areas, *e.g.*, mathematics [22,30], physics [29,15] and engineering [25]. Since the late 1990s and the newly proposed chaos-based ciphers (*e.g.* [1–3,12,18,58]) the most prolific influence of chaos theory has been found in the field of cryptography. There is a close connection between the two. Crucial cryptographic aspects including confusion and diffusion can be formalized with the help of fundamental chaotic properties, such as mixing and exactness, ergodicity and sensitive dependence to the initial conditions as revealed in [2,12] and [18].

Chaos-based cryptography has developed significantly during the 21st century, with a series of new ideas and proposals, as seen with [27,28,45]. However, after thorough cryptanalytic works, (*e.g.* [17,20,21]) some of these proposals were found to be unreliable.

Most chaos-based digital image encryption algorithms are built on the fundamental Fridrich's permutation – substitution model (*viz.*, one confusion round, resp., one diffusion round) [12], *e.g.*, [4,6,10,44,48,59].

In these cases, the confusion process consists of the pixels' permutation/relocation through the plain image, in order to hide the typical correlations within. It also considers the statistical link between the plain image, encrypted image and encryption key.

Through comprehensive studies, Zhang et al. [52], resp., Zhu et al. [60] have demonstrated the redundancy of Fridrich's structure-based image encryption schemes. The sequence of complex confusion and diffusion operations leads to only 3.3 percent bit value modifications; the remaining 96.7 percent is unchanged. This highlights three factors that need to be achieved

[*] Correspondence address: Lumina – The University of South-East Europe, IT&C Department, Bucharest 021187, Romania. Tel.: +40 722657621.
E-mail address: adrian.diaconu@lumina.org

http://dx.doi.org/10.1016/j.ins.2015.10.027
0020-0255/© 2015 Elsevier Inc. All rights reserved.

during the confusion phase: (i) the bit distribution of each bit-plane should be more uniform; (ii) the correlation between neighboring higher bit-planes should be reduced; (iii) both the positions and the pixel values are modified [60].

Based on these findings, scholars have developed new bit-level operation-based image cryptosystems over the past two years, *e.g.*, [5,13,23,36,38,39,43,48,51,53,55,57,60]. These aim to enhance the statistical properties of the confusion stage output images. For example, in [49], the appealed strategy enables the lower and higher bit-planes of pixels to mutually permute without any extra storage space; in [57], bit-planes of a source image are used as security key bit-plane to encrypt images; in [55], the confusion technique is based on the ordinary and reverse 2D chaotic map, but with the additional use of two permuting planes for exchange purposes; in [5] a nonlinear inter-pixel computing and swapping-based permutation approach for medical imagery is shown.

Bit-level operation approaches clearly present some shortcomings, such as repeated patterns in the permuted images [49], time-consuming operations [23,57] and the need for multiple mixing and/or ciphering rounds in order to approach desirable cryptographic performances [52,53,60].

Considering the depth of previous research on the enhancement of the newly proposed image cryptosystems (through the promotion and use of bit-level operations), a new, straightforward and efficient bit-level permutation-based confusion strategy is presented within this paper.

While still based on the fundamental Fridrich's permutation – substitution model (*viz.* one confusion round, resp., one diffusion round), the confusion strategy employed considerably reduces the redundancies that such a model would impose. More precisely, each row of pixels within an image is converted into its binary equivalent and circular shifts are used to perform inter–intra pixels bit-level permutations. Intrinsic properties of the row's equivalent binary representation (*i.e.*, the number of bits with the logical value 1) are then used to compute the number and direction of the row's circular shifts. Using the circular shifting process, the bits corresponding to one pixel are then transferred to its neighbor, whilst the bits within pixels are changing between bit-planes. Thus, the scrambled image obtained at the output (of the one round confusion stage) demonstrates the following: (i) no repetitive pattern; (ii) a more uniform bits distribution within the image's bit-planes; (iii) a greatly reduced correlation between neighboring higher bit-planes.

The effectiveness of the proposed confusion round has been assessed using specific tools that comply with the criteria stipulated by Zhang et al. [52]. The use of the intrinsic properties of each row within the image to be scrambled ensures a much smaller key size and eventually facilitates its management.

Finally, the scrambled image is doubly ciphered using two uncorrelated chaos-based matrices through the one round diffusion stage [8]. Simulations and extensive security analysis demonstrate that the proposed image cryptosystem has a high level of security for practical, secure applications.

The following sections of this paper have been organized as follows: Section 2 presents a comprehensive design of the proposed image cryptosystem. Section 3 offers an assessment of the effectiveness of the proposed confusion phase (*i.e.*, as part of the two-stage cryptosystem of confusion and diffusion). Section 4 contains a report of the simulation results and performance analyses. Section 5 presents the concluding remarks.

2. The proposed cryptosystem

2.1. Ciphering matrices computation

The pseudorandom number generator PRNG (1) is used within the construction stages of the newly proposed image encryption algorithm, for the computation of the ciphering matrices used within the diffusion procedure. PRNG has been chosen for its cryptographic properties, which include high sensitivity to initial conditions, attractor's fractal structure, system's ergodicity and a large key space as proven in [9].

$$y_i = f_{r_1}\left(x_i^1\right) * f_{r_2}\left(x_i^2\right) = \frac{f_{r_1}\left(x_i^1\right) + f_{r_2}\left(x_i^2\right)}{1 - f_{r_1}\left(x_i^1\right) \cdot f_{r_2}\left(x_i^2\right)}. \tag{1}$$

where: x_0^1, x_0^2 are the initial seeding points, resp., r_1, r_2 are the control parameters of the two one-dimensional chaotic maps to be used; x_i^1, x_i^2 are the orbits obtained with recurrences $x_{i+1}^1 = f_{r_1}(x_i^1), x_{i+1}^2 = f_{r_2}(x_i^2), \ \forall\, i \in N$; and the one-dimensional chaotic discrete dynamical systems, *i.e.*, $f_{r_1}(x_i^1)$ and $f_{r_2}(x_i^2)$, are of the form:

$$f_{r_p} : [-1, 1] \to [-1, 1], \quad f_{r_p}\left(x_i^p\right) = \frac{2}{\pi} arctg\left(ctg\left(x_i^p \cdot r_p\right)\right). \tag{2}$$

In order to improve the shortcomings related to the orbit's high predictability (common with cryptosystems based on a single dynamical system) [9], the PRNG used within the proposed image encryption scheme (1) results as a binary composition (3) of two chaotic, discrete, dynamical systems of the same type (2). However, these do have different initial seeding points and control parameters.

$$a * b = \frac{a + b}{1 - a \cdot b}. \tag{3}$$

For performance testing, initial seeding points of the chaotic maps and the control parameters' values were chosen with the following values: $x_0^1 = 0.68775492511773$ and $r_1 = 5.938725025421$, resp., $x_0^2 = -0.0134623354671$ and $r_2 = 1.257490188615$.