Signal Processing: *Image Communication* 41 (2016) 144–157

Contents lists available at ScienceDirect

Signal Processing: *Image Communication*

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

A new chaos-based image encryption system

Safwan El Assad*, Mousa Farajallah

Ecole polytech – University of Nantes-Rue Christian Pauc-44306, Nantes cedex 3, France

ARTICLE INFO

Article history:
Received 6 July 2015
Received in revised form
18 September 2015
Accepted 20 October 2015
Available online 3 November 2015

Keywords:
Chaos-based cryptosystem
New formulation of the 2D-cat map
Binary diffusion matrix
Security analysis

ABSTRACT

During the last decade, a variety of chaos-based cryptosystems has been introduced to protect the content of the transmitted images. In this paper, we propose a new fast, simple, and robust chaos-based cryptosystem structure and we analyze its performances. The cryptosystem uses a diffusion layer followed by a bit-permutation layer, instead of byte-permutation, to shuffle the positions of the image pixels. Moreover, the permutation layer is achieved by a new proposed formulation of the 2D cat map that allows an efficient implementation, measured by the time complexity, in terms of arithmetic and logic operations, and also, in terms of clock cycles, of the key-dependent permutation process in comparison with the standard one. Hence, it provides a very fast diffusion process to spread the influence of a single bit over the others. The new cryptosystem includes a robust and uniform chaotic pseudo-random generator (a very simplified version of a generator published in our patent) to change the control parameters in each round of the encryption/decryption processes. The generator is highly nonlinear and produces robust sequences of discrete values having very long orbits. The proposed cryptosystem is defined on finite numbers, and its speed is faster than many chaos-based cryptosystems, while having a very high security level. The security analysis and the obtained simulation results show that the proposed cryptosystem is resistant to various types of attacks and it is efficient for hardware and software implementation.

1. Introduction

In any public communication network, such as satellite, mobile-phone, and the Internet, it is almost impossible to prevent unauthorized people from eavesdropping. To make use of the already existed public communication networks and to maintain the secrecy, cryptographic techniques are applied [1]. The security of image and video data has become increasingly important for many applications, including video conferencing, medical imaging, industrial, and military imaging systems. An increasing number of applications demand both real-time performance and security: private multimedia messages exchanged by portable devices over the wireless networks and sensitive data exchanged in wireless sensor networks. With a fixed block size, the advanced encryption standard (AES) [2–4] is not suitable for the above applications and for video encryption [5,6]. For example, in selective encryption we need to wait to have 128 bits before the starting of encryption process. This is an inconvenient for the latency of the system. Chaos-based cryptosystems are more flexible, whatever the block size.

The two important properties of confusion and diffusion for any good standard encryption algorithm [7] are also existed in chaotic systems, which are ergodic and extremely sensitive to the secret key, composed by the initial conditions and the system parameters. According to the classification of chaotic systems, the chaotic encryption schemes, which have been proposed, can be divided into analog chaotic cryptosystems utilizing continuous dynamical

* Corresponding author.

http://dx.doi.org/10.1016/j.image.2015.10.004
0923-5965/© 2015 Elsevier B.V. All rights reserved.

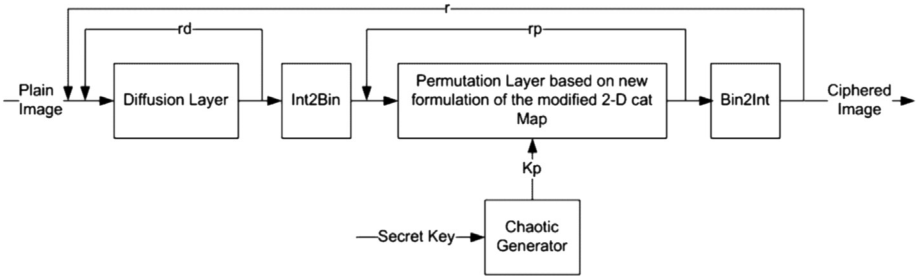

Fig. 1. Description of the encryption process.

systems [8] and digital chaotic cryptosystems utilizing discrete dynamical systems [9,10]. In addition, chaos based encryption algorithms are usually characterized by a low complexity of their structures. Therefore, in recent years, a number of chaos-based cryptosystems have been proposed [7,11–16]. Most of them are blocks ciphers and based on the substitution–permutation network (SPN). In a chaos-based encryption algorithm, the substitution and the permutation operations are done in accordance with chaotic sequences [17,18].

In [19], Fridrich proposed a chaos-based encryption scheme in which a process of permutation on the pixels, followed by a nonlinear process are iterated. The permutation is done using three 2D chaotic maps, namely the Backer map, the Cat map, and the Standard map. The nonlinear process is achieved by a nonlinear feedback register.

Masuda et al, considered in [20] two classes of chaotic finite-state maps: key-dependent chaotic S-boxes and chaotic mixing transformation. They proposed two chaotic block ciphers, i.e., uniform and Feistel, and they exactly estimate bounds for the differential probability and the linear probability to make their ciphers resistant to differential and linear cryptanalysis.

In [21], a fast and robust image encryption algorithm called Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption (ECKBA) was proposed. The algorithm performs *r* rounds of an SP-network on each pixel. Two PWLCM maps are used, one in the substitution process (addition modulo 256 and bitwise operations) and the other one in the permutation process. The permutation is of degree 8, and its index in the full symmetric group S8 is sorted in lexicographical Cartesian of *i* order (see appendix of reference [21]). The weakness of this algorithm is the error propagation caused by the used perturbation technique.

Yang et al, derived in [22] a fast image encryption and authentication scheme. A key Hash function is introduced to generate 128 bits hash value from both of the plain image and the secret hash keys. The hash value plays the role of the key for encryption and decryption, while the secret hash keys are used to authenticate the decrypted image. The permutation and substitution are performed in a single scan of the plain-image pixels. The permutation process is achieved by the modified standard map and the substitution process (based on a logistic map) is done in a way that the change made to a particular pixel depends on the accumulated effect of all previous pixel values. Chen et al. analyzed the period distribution of the generalized discrete cat map over the Galois ring. Used as a generator, the produced sequences by this map are modeled as a 2-dimensional LFSR sequences [23].

Zhang et al. [15] proposed a chaotic image encryption based on circular substitution box and key stream buffer. The encryption process consists of a substitution and diffusion layers to encrypt each pixel of the image using an encryption key that depends on the plain image. In this way, one encryption round is sufficient to achieve the security against the known and plain text attacks. However, this scheme is not a practical one, because, it is obligatory to send a new encryption key for each new plain image.

In this paper, we propose an efficient chaos-based cryptosystem formed by two layers: a diffusion layer, operating on the pixels, followed by a key-dependent chaotic permutation process, operating on the bits. The linear diffusion transformation is done by a binary matrix that gives high diffusion effects without using any multiplications. So, it provides a simpler implementation of bitwise operations. The permutation process is achieved by using a new proposed expression of the modified 2D cat map which is implemented with an efficient manner, as compared to the basic calculation. This proposed structure achieves a higher security level. Also, it is faster than many known chaos-based encryption algorithms. The paper is organized as follows. In Section 2, the proposed chaos-based cryptosystem is described. In Section 2.1, we describe in detail the encryption process. The diffusion layer is given in Section 2.1.1 and in Section 2.1.2, we study in detail the formulation and the time complexity in terms of arithmetic and logic operations, and also, in terms of clock cycles, of the key-dependent permutation process. The implemented chaotic generator and its performances are given in Section 2.2. Section 2.3 presents in detail the decryption process. In Section 3, we illustrate the obtained performance in terms of time consuming and security analysis of our proposed cryptosystem. Finally, Section 4 contains our conclusion and perspectives.

2. Proposed chaos-based cryptosystem

The structure of the proposed chaos-based cryptosystem is shown in Fig. 1, for the encryption part, and in Fig. 4, for the decryption part. The cryptosystem is a block cipher implemented in CBC mode. This new structure has efficient encryption features, i.e., robustness against the cryptanalysis and a high calculation speed. Moreover, it is adequate for a software and hardware implementations (using FPGA card or an ASIC).