Signal Processing 111 (2015) 294–307

Contents lists available at ScienceDirect

Signal Processing

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

Reusing the permutation matrix dynamically for efficient image cryptographic algorithm

Jun-xin Chen [a], Zhi-liang Zhu [b,*], Chong Fu [a], Hai Yu [b], Yushu Zhang [c]

[a] School of Information Science and Engineering, Northeastern University, Shenyang 110004, China
[b] Software College, Northeastern University, Shenyang 110004, China
[c] School of Electronics and Information Engineering, Southwest University, Chongqing 400715, China

ARTICLE INFO

Article history:
Received 30 August 2014
Received in revised form
4 January 2015
Accepted 5 January 2015
Available online 12 January 2015

Keywords:
Image encryption
Dynamic key stream generation
Baker map
Permutation matrix

ABSTRACT

In traditional type of chaotic image ciphers with the architecture of permutation–diffusion, one-dimensional chaotic map is always employed for generating key stream in the diffusion procedure. However, the workloads derived from the iteration-then-quantization of the key stream generation operations severely downgrade the overall encryption efficiency of such cryptosystems. In this paper, we demonstrate how to obtain the diffusion key stream from the permutation matrix, which is produced and preserved in the permutation phase. No extra chaotic iteration and quantization is required in the diffusion procedure, the operation efficiency is thus improved. A complete cryptosystem is built using Bake map for image permutation. Simulations and security analyses have been carried out and the results illustrate the superior security and high efficiency of the proposed scheme.

1. Introduction

In recent years, secure transmission and storage of digital images over public networks have become attractive issues in both research and applications. Due to the properties of ergodic and high sensitivity to initial conditions and control parameters that can be employed in both permutation and diffusion processes with satisfied efficiency and security [1,2], chaotic systems have been extensively researched for digital image encryption. In 1998, Fridrich firstly proposed a general architecture for chaos-based image encryption, consisting of two stages, permutation and diffusion [3], as shown in Fig. 1. In the permutation procedure, pixels are shuffled by a two-dimensional area-preserving chaotic map, such as Arnold cat map, Chirikov standard map and Baker map. Then pixel values will be modified sequentially with a quantized one-dimensional chaotic map in the diffusion phase. This pioneering achievement has paved the way for amounts of chaos-based image encryption systems subsequently proposed [4–27]. In [4–6], novel pixel-level image permutation approaches were developed, whereas a number of permutation approaches in bit-level have also been investigated so as to simultaneously obtain image permutation and pixel modification effects [7–11]. As a basic and indispensable phase, numbers of improved image diffusion strategies have been reported in [12–16], while interesting approaches to obtain combined compression and encryption effects are proposed in [9,17–20]. Some other techniques, such as novel chaotic systems [21–23], cellular automaton [24,25], chaotic synchronization phenomena [26] and various bitplane decomposition methods [27] have also been employed to build secure image encryption schemes.

Security and efficiency are two most important issues for image ciphers. However, recent cryptanalysis achievements have demonstrated that some chaos-based image cryptosystems are vulnerable against various attacks [28–30]. The most serious flaw in these insecure algorithms is that the key stream completely depends on the secret key. That is, identical key stream will be generated to encrypt different plain images if the key remains the same. This drawback favors an attacker

* Corresponding author. Tel.: +86 24 8658 1232.
E-mail address: zhuzhiliang.sc@gmail.com (Z.-l. Zhu).

http://dx.doi.org/10.1016/j.sigpro.2015.01.003
0165-1684/

to launch known-plaintext or chosen-plaintext attack so as to retrieve the equivalent key stream elements and further break the whole cryptosystem. Therefore, the key stream elements extracted from identical secret key should better be distinct and related to the plain image [14]. With regard to the operation efficiency, the time consumption mainly derives from the floating point arithmetic in the chaotic iteration and quantization operations that are required for key stream generation in the diffusion procedure [6,12]. Accordingly, when satisfying the security requirements, how to reduce the number of chaotic map iteration and quantization plays critical role for promoting the encryption efficiency.

Taking both the issues into consideration, we propose an efficient image encryption scheme with dynamic reuse of the permutation matrix (DRPM) in this paper. The classical permutation–diffusion architecture is adopted, and the DRPM is an innovation that can generate dynamic diffusion key stream from the permutation matrix, which is produced and preserved in the permutation phase. In traditional chaos-based image cryptosystems, independent chaotic iterations have to be executed for the permutation and diffusion, respectively. Besides, quantization is further needed to convert the chaotic state variable to the required key stream element in the diffusion procedure. However, in our scheme, the permutation matrix [31] generated in the permutation stage will be preserved and further exploited in the diffusion phase, the key stream elements required for image diffusion is obtained by DRPM. As no extra chaotic iteration and quantization is needed in the diffusion phase and DRPM seems like table lookup which is more efficient than real number arithmetic operations, the proposed mechanism can lead to substantial promotion of the operation efficiency. Moreover, different key stream elements will be extracted for distinct plain images when using DRPM, even though the permutation matrix is the same one. The known-plaintext or chosen-plaintext attack is consequently infeasible. Chaotic Baker map is introduced as experimental permutation technique, and then a complete cryptosystem is built. Simulation results and security analyses have proved the efficiency and security of the cryptosystem.

The remainder of this paper is organized as follows. In next section, the proposed image encryption scheme is described in detail. Simulation results, the effectiveness and efficiency comparisons are reported in Section 3, while thorough security analyses of the cryptosystem are carried out in Section 4. Finally, conclusions will be drawn in the last section.

2. The proposed cryptosystem

In our scheme, the classical permutation–diffusion architecture is adopted. A two-dimensional area-preserving chaotic map is introduced for pixel shuffling in the permutation stage, whereas its permutation matrix will then be persevered. The key stream elements required in the diffusion stage are extracted from the permutation matrix, so-called the DRPM. In this paper, Baker map is employed as an example for illustrating the DRPM clearly. Yet, it is straightforward to apply some other similar chaotic maps as alternatives, such as cat map and standard map.

2.1. Image permutation using Baker map

The so-called chaotic Baker map is a well-known image permutation approach [3,5,14,15]. It is essentially a bijection of the lattice $N \times N$ onto itself, where N is number of pixels in one row (column). The discretized Baker map is most easily described in geometric terms, as depicted in Fig. 2. An image with size $N \times N$ is firstly divided into k vertical rectangles of height N and width n_i (i=0, 1, …,

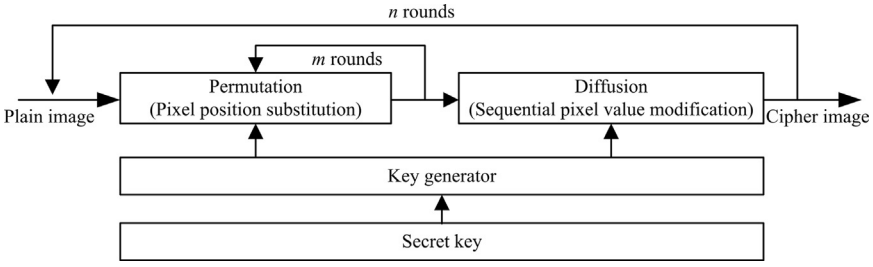

Fig. 1. Typical architecture for chaos-based image encryption.

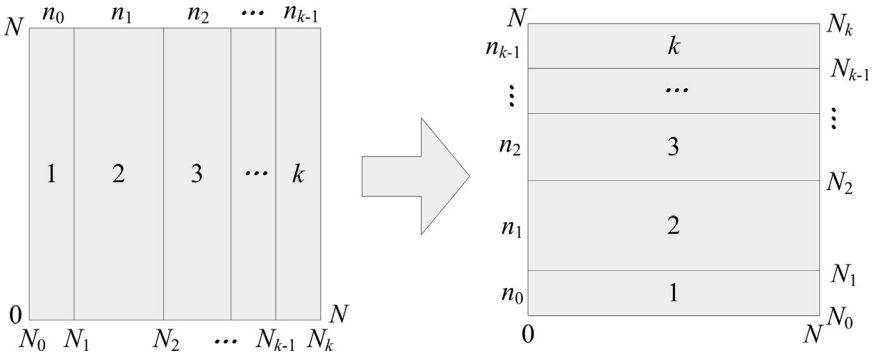

Fig. 2. Illustration of the discretized Baker map.