Commun Nonlinear Sci Numer Simulat 19 (2014) 74–82

Contents lists available at SciVerse ScienceDirect

Commun Nonlinear Sci Numer Simulat

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

An image encryption scheme based on rotation matrix bit-level permutation and block diffusion

Yushu Zhang, Di Xiao *

College of Computer Science, Chongqing University, Chongqing 400044, China

ARTICLE INFO

Article history:
Received 6 June 2012
Received in revised form 11 December 2012
Accepted 24 June 2013
Available online 4 July 2013

Keywords:
Rotation matrix
Bit-level permutation
Block diffusion
Parallel mode
Noise robustness

ABSTRACT

This paper proposes a novel image encryption scheme based on rotation matrix bit-level permutation and block diffusion. Firstly, divide plain image into non-overlapping 8 × 8 pixels blocks with a random matrix, then transform each block into an 8 × 8 × 8 three-dimensional (3-D) binary matrix, which has six directions just as a cube. Permutation is performed by multiplying the 3-D matrix by the rotation matrix that relies on plain image according to different direction. Secondly, use block diffusion to further change the statistical characteristics of the image after confusion. Experiment results and analysis show that the scheme can not only achieve a satisfactory security performance, but also have the suitability for a parallel mode and the robustness against noise in communication system.

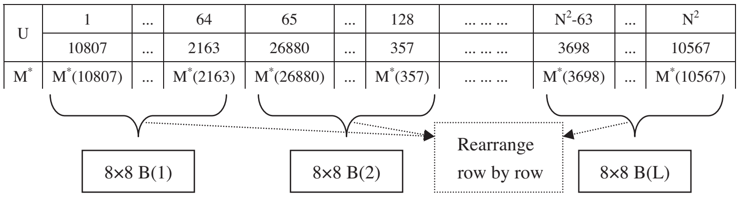
1. Introduction

In recent years, the transmission of digital images over communication media has developed greatly. The security of multimedia data is receiving more and more attention due to the widespread transmission over various communication networks. It has been noticed that image encryption is different from traditional text encryption due to some inherent features of the image, such as bulk data capacity, high redundancy, and strong correlation among adjacent pixels. To meet a great demand for secure image transmission over networks, a variety of encryption schemes have been proposed [1–9].

Chaotic cryptosystems have been studied extensively due to its ergodicity, pseudo-randomness and sensitivity to initial conditions and control parameters, which are close to confusion and diffusion in cryptography. These properties make chaotic systems a potential choice for constructing cryptosystems [3–10]. According to the difference of the basic permutation unit, the existing chaotic image cryptosystems can be classified into two groups. In the first group, which most the existing cryptosystems belong to, the basic permutation unit is each pixel. While in the second group, a pixel is further divided into 8 bits, and each bit is chosen as the basic permutation unit. Since each pixel bit contains percentage of the pixel information, the confusion performance at the bit-level is quite different. In [11], Chen et al. designed a new typical bit-level system called Two-Dimensional Circulation Encryption Algorithm (TDCEA). Authors define two bit-circulation functions for one-dimensional binary array transformation and exploit a chaotic system to control them. Then, each eight 8-bit data element is regarded as a set and fed into an 8 × 8 binary matrix being transformed on each row and each column of the matrix by these two bit-circulation functions. Unfortunately, TDCEA was cryptanalyzed in [12,13] due to its permutation-only operation which is unsafe under a known/chosen-plaintext attack [14,15]. Because of this vulnerability, Zhu et al proposed

* Corresponding author. Tel.: +86 23 8633 3521; fax: +86 23 6510 3199.
E-mail address: xiaodi_cqu@hotmail.com (D. Xiao).

1007-5704/$ - see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.cnsns.2013.06.031



U	1	...	64	65	...	128	... ...	N^2-63	...	N^2
	10807	...	2163	26880	...	357	... ...	3698	...	10567
M^*	M^*(10807)	...	M^*(2163)	M^*(26880)	...	M^*(357)	... ...	M^*(3698)	...	M^*(10567)

Fig. 1. An example of PM.

an image cryptosystem with the architecture of confusion and diffusion employing the Arnold cat map for bit-level permutation and the logistic map for diffusion (BLP) in [16]. In [17], lightweight bit-level confusion and cascade cross circular diffusion were used to encrypt image. However, in our opinion, to ensure the transmission of digital images, besides the security of a cryptosystem, the robustness of cipher image against noise or other external disturbances is also important.

Based on the above analysis, a novel image encryption scheme with confusion-diffusion is proposed in this paper, where rotation matrix is used in its confusion phase. Meanwhile, block diffusion is adopted for secure communication on noisy channels.

The rest of the paper is organized as follows: In the next section, the concept of the rotation matrix is introduced simply. Then, the proposed image cryptosystem is described in Section 3. Performance and security analysis are reported in Section 4. Finally, main conclusions are given in Section 5.

2. Rotation matrix

In linear algebra, a rotation matrix is a matrix that is used to perform a rotation in Euclidean space [18]. For example, the matrix

$$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

rotates points in the *xy*-Cartesian plane counterclockwise through an angle θ about the origin of the Cartesian coordinate system. Rotation matrices are square matrices, with real entries. More specifically, they can be characterized as orthogonal matrices with determinant ±1:

$$R^T = R^{-1}, \quad \det(R) = \pm 1.$$

The set of all such matrices of size n forms a group, known as the special orthogonal group $SO(n)$. Let us consider a special Rotation Matrix (RM) of $SO(8)$. In *RM*, every row or column has exactly one “1” and the rest of the values are all “0”. Fig 1 shows an example of 8×8 permutation matrix (PM). In the proposed scheme, RM will be used as a permutation matrix (PM).

3. The proposed cryptosystem

As we know in cryptography, confusion and diffusion are two desired properties of a secure cipher which were identified by Shannon [19], so the general image encryption algorithm is composed of confusion-diffusion.

3.1. Confusion phase

A common design principle is to use nonlinear functions for confusion operation and nonlinear components are essential to every strong cryptosystem. For instance, in Advanced Encryption Standard (AES), nonlinear functions are generally implemented as S-box which is a table-driven nonlinear substitution operation [20]. Chaotic maps can also be proper alternatives to S-box thanks to their interesting properties such as sensitive dependence on initial conditions and topological transitivity, ergodicity and random-like behaviors. In particular, many chaotic encryption schemes produce a pseudorandom permutation from chaotic maps and permute plaintext images with the pseudorandom permutation. However, these traditional permutation operations usually swap two pixels only. In the proposed cryptosystem, we introduce novel bit-level confusion instead, which can not only change the locations of the image pixels, but also modify their values. The Rotation Matrix (RM) is utilized to realize confusion here.

3.1.1. Construction of permutation matrices

Any chaotic map that produces a series of permutation matrices (PMs) can be used in the proposed scheme. For a reference implementation, we design construction of 8×8 PMs based on a Logistic map and summarize the generation process as Algorithm 1.