Optics and Lasers in Engineering 68 (2015) 126–134

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Novel image encryption algorithm based on cycle shift and chaotic system

Xing-Yuan Wang [a,*], Sheng-Xian Gu [a], Ying-Qian Zhang [a,b]

[a] Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, China
[b] City Institute, Dalian University of Technology, Dalian 116600, China

ARTICLE INFO

Article history:
Received 12 March 2014
Received in revised form
23 December 2014
Accepted 23 December 2014
Available online 15 January 2015

Keywords:
Image encryption
Cycle shift
Chaotic system

ABSTRACT

In this paper, a novel image encryption algorithm is proposed. The cycle shift in bits of pixels and the chaotic system are employed for the encryption of the proposed scheme. For cycle shift operations, random integers with the same size of the original image are produced to scramble the plaintext image. Moreover, the scrambled image effects the initial values of the chaotic system for the further encryption process, which increases the sensitivity of plaintext images of the scheme. The scrambled image is encrypted into the ciphered image by the keys which are produced by the chaotic system. The simulation experiments and theoretical analyses indicate that the proposed scheme is superior and able to resist exhaustive attack and statistical attack.

1. Introduction

Nowadays the number of image files [1–3] transmitted over Internet keeps increasing. Therefore, the secure transmission of confidential digital images over public channels has become a common interest. Coordinate's conversion [4–8] and chaotic sequence have been widely applied in image encryptions [9–12]. The cycle shift is a suitable technology for scrambling images because this technology contains many features such as simplicity, efficiency, size flexibility of images, randomness. Therefore, the cycle shift can increase the security of the encryption scheme and resist common attacks [13–17].

Cycle shift can also change the values of image pixels [18–22]. For example, one image pixel value is 01100101 in binary. When its 3 bit is cycle shifted, the value of 00101011 is obtained. Obviously, the two binary sequences are different. It needs another 5 bit of cycle shift operations for the recovery the original value. The theoretical analyses and experimental results in the rest of the paper indicate the security of proposed image encryption scheme.

2. The novel image encryption algorithm

2.1. Related work

Chaotic system has been widely used in encryption algorithms for its good characteristics. Generally, chaotic systems are applied in both the key generations and data scramble for cryptography design based on its randomness characteristic [23–25]. Therefore, the chaotic system is applied to produce the key in the proposed scheme.

Cycle shift can efficiently change the values of pixels. Furthermore, this operation is reversible and asymmetric for a decryption process. Therefore, cycle shift is used in the proposed scheme in both changing the values of pixels in bit-level and scrambling the data of images.

2.2. Encryption process

The process of the proposed encryption scheme is as follows:

(1) Generate random numbers $R1, R2$ with size $M \times N$ by using Eqs. (1–4).

$$X1_{i+1} = \mu_1 X1_i(1 - X1_i), \quad i = 1, 2, 3\ldots \tag{1}$$

$$R1 = \{R1 | R1_i = \bmod(100,000 X1_i, 65, 536)\}, \quad i = 1, 2, 3, \ldots \tag{2}$$

$$X2_{i+1} = \mu_2 X2_i(1 - X2_i), \quad i = 1, 2, 3\ldots \tag{3}$$

$$R2 = \{R2 | R2_i = \bmod(10,000 X2_i, 8)\}, \quad i = 1, 2, 3, \ldots \tag{4}$$

here M and N are the height and the width of the original image, respectively. The initial values $X1_1$ and $X2_1$ are defined as Eq. (5) and Eq. (6), respectively:

$$X1_1 = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} A(i,j)}{M \times N}, \tag{5}$$

$$X2_1 = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} B(i,j)}{M \times N}. \tag{6}$$

* Corresponding author.
E-mail address: wangxy@dlut.edu.cn (X.-Y. Wang).

http://dx.doi.org/10.1016/j.optlaseng.2014.12.025
0143-8166/

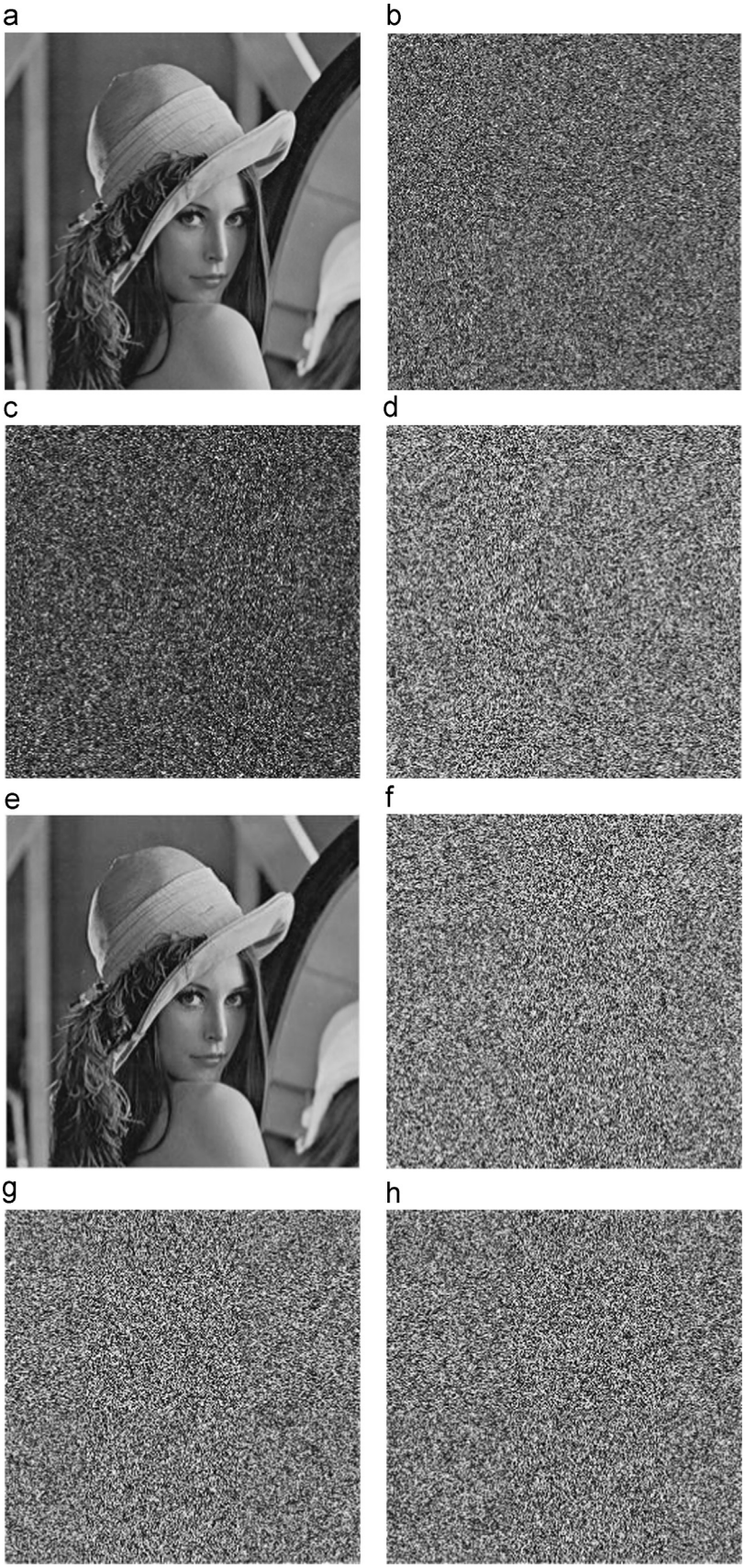

Fig. 1. The encryption and decryption of image Lena. (a) The original image. (b) The scrambled image. (c) The cycle shifted image. (d) The ciphered image. (e) The decrypted image with right keys. (f) The decrypted image with wrong key. (g) The decrypted image with wrong cycle shift. (h) The decrypted image with wrong scramble.