Optics and Lasers in Engineering 80 (2016) 1–11

Contents lists available at ScienceDirect

Optics and Lasers in Engineering

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

Multiple-image encryption with bit-plane decomposition and chaotic maps

Zhenjun Tang [a,b,*], Juan Song [a,b], Xianquan Zhang [a,b], Ronghai Sun [a,b]

[a] Guangxi Key Lab of Multi-source Information Mining & Security, Guangxi Normal University, Guilin 541004, China
[b] Department of Computer Science, Guangxi Normal University, Guilin 541004, China

ARTICLE INFO

Article history:
Received 6 September 2015
Received in revised form
9 December 2015
Accepted 10 December 2015

Keywords:
Multiple-image encryption
Bit-plane decomposition
Encrypted image
PNG image
Chaotic map

ABSTRACT

Image encryption is an efficient technique of image content protection. In this work, we propose a useful image encryption algorithm for multiple grayscale images. The proposed algorithm decomposes input images into bit-planes, randomly swaps bit-blocks among different bit-planes, and conducts XOR operation between the scrambled images and secret matrix controlled by chaotic map. Finally, an encrypted PNG image is obtained by viewing four scrambled grayscale images as its red, green, blue and alpha components. Many simulations are done to illustrate efficiency of our algorithm.

1. Introduction

With the rapid development of multimedia technology, a growing number of images and videos are generated, transmitted and shared on the Internet. The increasing use of images and videos makes our lives wonderful, but also brings some problems. For example, more and more people would like to save their images in cyberspace, e.g., cloud storage. If these images are stored without technical protection, private and confidential information will be leaked. Therefore, image protection technology is in demand. In this study, we propose a new image encryption algorithm for protecting multiple grayscale images.

Image encryption is a useful technology for image protection [1]. It converts a meaningful image into a chaotic version. Since attackers cannot observe any original information from chaotic image, image protection is thus achieved. In the recent years, image encryption has attracted more attention from optical community [2–5], and many researchers have introduced various techniques to design image encryption algorithms. A widely used technique is Arnold transform [6]. For example, Zhu et al. [7] used Arnold transform and exclusive OR (XOR) operation to calculate chaotic images. Tang and Zhang [8] combined Arnold transform with random strategies and presented a secure encryption scheme without image size limitation. Besides Arnold transform, other techniques have been also reported. For example, Tang et al. [9] divided pixel bits into even and odd groups and computed chaotic image by randomly swapping even group and odd group. Martin et al. [10] selected partial wavelet coefficients to conduct image encryption. Lin et al. [11] applied blind source separation to multiple-image encryption. Liu and Wang [12] proposed to encrypt color images by one-time keys and chaotic maps. Wang et al. [13] designed an image encryption algorithm based on Lorenz chaotic system and perceptron model. Later, Wang et al. [14] exploited chaotic system to encrypt the red, green and blue components of color image at the same time, and made the three components affect each other. In another study, Zhang and Liu [15] used chaotic system to produce position mapping array for pixel shuffling. Liu and Wang [16] exploited piecewise linear chaotic map to conduct bit-level permutation and used Chen system to confuse and diffuse the red, green and blue components. Wang et al. [17] exploited linear blend operation and random phase encoding in fractional Fourier domain to convert two images into a single image. Recently, Wang et al. [18] proposed a multiple-image encryption scheme based on mixture retrieval algorithm and phase mask multiplexing in Fresnel domain. Ping et al. [19] presented a cellular automata (CA) based image encryption method. In another work, Wang et al. [20] exploited cycle shift operations and chaotic system to construct image encryption algorithm. Enayatifar et al. [21] jointly used Tinkerbell chaotic map, DNA and CA to design encryption scheme. Tang et al. [22] used chaotic

* Corresponding author at: Department of Computer Science, Guangxi Normal University, 15 Yucai Road, Guilin 541004, China.
E-mail addresses: tangzj230@163.com, zjtang@gxnu.edu.cn (Z. Tang).

http://dx.doi.org/10.1016/j.optlaseng.2015.12.004
0143-8166/

system and block shuffling to encrypt image. Wang et al. [23] proposed a hybrid encryption algorithm for color images by combining pixel permutation, XOR operation and data mixture among RGB channels.

Although many encryption algorithms have been proposed, there are still some practical problems. For instance, efficient techniques are needed for encrypting multiple images. Some reported techniques [11,17] can encrypt multiple images, but their decrypted images are not completely the same with the original images. This means that they are lossy algorithms and thus are not suitable for those applications requiring images with good visual quality, such as medical images. Aiming at this problem, we propose an efficient multiple-image encryption algorithm based on bit-plane decomposition and chaotic maps, which is novel to optical community. The proposed algorithm reaches good performances in security, robustness, and computational time. It can losslessly retrieve original images from the encrypted images. Many simulations are conducted to validate efficiency of the proposed algorithm. The rest of this paper is organized as follows. Section 2 introduces the proposed algorithm. Section 3 analyzes our key space. Simulation results and conclusions are presented in Sections 4 and 5, respectively.

2. Proposed algorithm

Fig. 1 shows block diagram of our image encryption. In the first step, four input grayscale images are decomposed into bit-planes. In the second step, these bit-planes are randomly divided into bit-blocks controlled by Henon map and thus bit-blocks among different bit-planes are randomly swapped. Finally, XOR operations between four shuffled images and a secret matrix controlled by Logistic map are conducted to generate four chaotic images, which are viewed as the red, green, blue, and alpha components of a PNG (Portable Network Graphics) image, respectively. In the following sections, we firstly introduce the key techniques, including PNG image, bit-plane decomposition, random bit-block partition and chaotic maps, and thus describe details of the proposed algorithm.

2.1. PNG image

Portable network graphics (PNG) is a popular image format widely used on the Internet. It is published as an ISO/IEC standard in 2004 and supports lossless data compression. Compared with traditional BMP image, PNG image has below advantages. (1) It has a small file size due to the use of lossless data compression. (2) As an alpha component is added, it supports transparency. In the alpha component, every image pixel has a corresponding value ranging from 0 to 255 for illustrating transparency. In this work, we achieve multiple-image encryption by viewing four processed grayscale images as the red, green, blue and alpha components of a PNG image.

2.2. Bit-plane decomposition

A non-negative decimal number d can be converted to a binary representation with n bits as follows.

$$d = \sum_{i=1}^{n} b_i 2^{i-1} = b_1 2^0 + b_2 2^1 + \ldots + b_i 2^{i-1} + \ldots + b_n 2^{n-1} \quad (1)$$

For a grayscale image, pixel value ranges from 0 to 255 and thus each pixel can be represented by an 8-bit binary sequence. Consequently, we can decompose a grayscale image into 8 bit-planes, where the i-th bit-plane is formed by the i-th bit of all pixels ($i=1$, 2, …, 8). Note that a higher bit-plane contains more significant visual information of the original image. Fig. 2 is a standard grayscale image Lena and its 8 bit-planes are presented in Fig. 3.

2.3. Random bit-block pattern

Random partition is an efficient method for image encryption. Motivated by random image block partition proposed in [22], we divide bit-planes into random overlapping bit-blocks and swap bit-blocks among different bit-planes to achieve encryption. The random bit-block pattern can be determined as follows. Suppose that the size of bit-plane is $M \times N$ (i.e., input image is $M \times N$), the selected bit-block size is $S \times S$, and the overlapping sizes between adjacent blocks along the x-axis and the y-axis are both t, where $t \in (1, S)$. Thus, the bit-block numbers along the x-axis and the y-axis are n_x and n_y, which can be calculated by the following equations.

$$n_x = \begin{cases} \frac{N-t}{S-t}, \text{if } \mathrm{mod}(N-t, S-t) = 0 \\ \left\lfloor \frac{N-t}{S-t} \right\rfloor + 1, \text{otherwise} \end{cases} \quad (2)$$

Fig. 2. Lena.

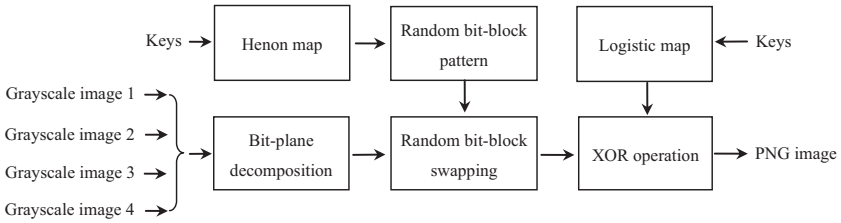

Fig. 1. Block diagram of our image encryption.