The Journal of Systems and Software 98 (2014) 140–154

Contents lists available at ScienceDirect

The Journal of Systems and Software

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

A new chaotic map based image encryption schemes for several image formats

Miao Zhang, Xiaojun Tong*

School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209, China

ARTICLE INFO

Article history:
Received 17 July 2013
Received in revised form 12 August 2014
Accepted 27 August 2014
Available online 6 September 2014

Keywords:
Image encryption
Cross chaotic map
Sequence generator

ABSTRACT

This paper proposes several image encryption schemes for popular image formats as Joint Photographic Experts Group (JPEG), Graphics Interchange Format (GIF), Portable Network Graphics (PNG), and Tagged Image File Format (TIFF). A cross chaotic map proposed based on Devaney's theory and dynamic block dividing of the 3D baker using the cross chaotic map are used for diffusion and permutation in encryption. Moreover, in order to verify user's identity, authentication is carried out using information hiding based on the cross chaotic function. In our methods, image files syntax and structure are not destructed, and the original image can be recovered lossless. For GIF, it keeps the property of animation successfully. The security test results indicate the proposed methods have high security, and the speed of our algorithm is faster than classical solutions. JPEG, GIF, TIFF and PNG image formats are popular contemporarily. Therefore this paper shows that the prospect of chaotic image encryption is promising.

1. Introduction

In recent years, various images have increasingly become available in different formats. The rapid growth in the demand of image transmission or storage in different formats has made the image security based on image formats become very important. Image encryption is an efficient method for ensuring image security.

Conventional cryptographic techniques, such as the IDEA or AES, are not suitable for image encryption due to the bulky data capacity and high correlation among pixels in image files. To solve this problem, chaos-based image encryption methods have also been recently proposed (Liu et al., 2009; Liao et al., 2010; Wang et al., 2008, 2011, 2012; Sahar and Amir, 2009; Tong and Cui, 2009; Tong, 2012) and have developed considerably. Because of its characteristics of ergodicity, sensitive dependence on initial conditions, random-like behavior and mixing effect, chaos has shown superior performance in the field of image encryption. It is invalid for chaotic cryptography to execute attacks dependent of tracing the pattern of the output cipher, such as differential attacks.

In some of these schemes, permutation and diffusion based on chaotic maps are employed. In the permutation process, image pixels are reallocated with the help of a chaotic map. In the diffusion process, the value of pixels is changed by applying a chaos sequence to it. In Wang et al. (2008), a cross chaotic map is proposed to improve security and reduce calculation complexity. A new dynamic block dividing of the 3D baker scheme using the compound chaotic map in Tong and Cui (2009), Tong (2012) is an excellent scheme. However, they all focus on the bitmap images and do not consider other image formats. And there are limited papers about encryption for specified image formats now, such as Portable Network Graphics (PNG), Graphics Interchange Format (GIF), Joint Photographic Experts Group (JPEG), Tagged Image File Format (TIFF), etc. Several encryption schemes for JPEG images are introduced (Lian et al., 2004; Niu et al., 2008; Vancea et al., 2005), but none of them owns a satisfied result, due to problems of security, recover lossless, and etc. Fortunately, it is practicable to apply the chaotic image encryption to JPEG, GIF, PNG and TIFF. So we propose several image encryption schemes based on cross-chaos for several popular image formats which are PNG, GIF, JPEG, and TIFF. The 3D baker scheme is used in permutation in which dynamic block dividing using cross chaotic map. In our methods, image files syntax and structure are not destructed, and the original image can be recovered lossless. Moreover, in order to verify user's identity, authentication is carried out using information hiding based on the cross chaotic map. Our method has the characteristic of high speed, high security and recovering losslessly.

The rest of this paper is organized as follows. A review of several popular mage formats (PNG, GIF, JPEG, and TIF) is given in Section 2. The design of new cross chaotic map by Devaney's definition of chaos is given in Section 3. In Section 4 the proposed approaches are

* Corresponding author.
E-mail address: tong_xiaojun@163.com (X. Tong).

http://dx.doi.org/10.1016/j.jss.2014.08.066
0164-1212/

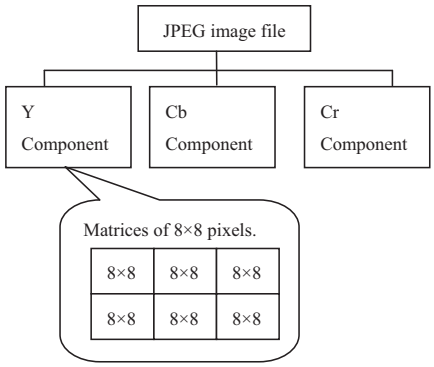

Fig. 1. JPEG image file structure.

described. The security test results and analysis of our new schemes are given in Section 5. Finally, the conclusions are drawn in Section 6.

2. Image formats analysis

2.1. Joint Photographic Experts Group (JPEG) file format

JPEG is a successful image format standard and is suitable for transmission on the network. In JPEG, discrete cosine transformation (DCT) and quantization are introduced to process the original image data (InterNational Telecommunication Union, 1992).

An original image is dealt with to form JPEG as follows:

(1) Preprocessing.
(2) Discrete cosine transformation.
(3) Quantization.
(4) Entropy encoding.

Preprocessing includes converting an image to YUV color space, sampling and organizing minimum coded unit (MCU). In YUV color space, JPEG image data is stored into three components: Y (luminance component, standing for brightness), Cb (blue-difference chromatic component), and Cr (red-difference chromatic component). Each component is split into several 8×8 pixels, as shown in Fig. 1. Then in the following step the data undergoes a discrete cosine transform, quantization and entropy encoding (InterNational Telecommunication Union, 1992; Yuen and Wong, 2011).

Because of the distribution of color-sensitive and brightness-sensitive receptors in the human eyes, downsampling is used to reduce the spatial resolution of the Cb and Cr components to compress images. The most used ratios for downsampling in JPEG images are 4:4:4 (no downsampling), 4:2:2 (reduction by a factor of 2 in the horizontal direction), or most commonly, 4:2:0 (reduction by a factor of 2 in both the horizontal and vertical directions).

Here we give the definition of sampling factor:

Definition 1. For each component, sampling factors H_i and V_i are defined to be related to component dimensions x_i and y_i, maximum dimensions X and Y, according to the following expressions:

$$x_i = \left\lceil X \times \frac{H_i}{H_{\max}} \right\rceil, \quad y_i = \left\lceil Y \times \frac{V_i}{V_{\max}} \right\rceil \tag{1}$$

where $H_{\max}$ and $V_{\max}$ are the maximum sampling factors for all components, and $\lceil\rceil$ is the ceiling function (Yuen and Wong, 2011).

The smallest unit of JPEG compression is MCU. A MCU is the sequence of the data units defined by the sample factors of the component in the scan. For interleaved order, each component is divided into small rectangular arrays of H_n horizontal data units by V_n vertical data units. Here H_n and V_n denote the horizontal and vertical sampling factors.

Fig. 2 indicates the most common situation (4:2:0) of interleaved data. Then the MCU can be written as follows.

$$\begin{aligned} \mathrm{MCU}_1 &= d^Y_{00} d^Y_{01} d^Y_{10} d^Y_{11} d^{Cb}_{00} d^{Cr}_{00} \\ \mathrm{MCU}_2 &= d^Y_{02} d^Y_{03} d^Y_{12} d^Y_{13} d^{Cb}_{01} d^{Cr}_{01} \\ \mathrm{MCU}_3 &= d^Y_{20} d^Y_{21} d^Y_{30} d^Y_{31} d^{Cb}_{10} d^{Cr}_{10} \\ \mathrm{MCU}_4 &= d^Y_{22} d^Y_{23} d^Y_{32} d^Y_{33} d^{Cb}_{11} d^{Cr}_{11} \end{aligned} \tag{2}$$

In formula (2), d^Y_{ij} stands for the matrix of 8×8 pixels in i-th row and j-th column of component.

Therefore, we have the formula to work out the height and width of the particular component in a JPEG image.

$$\begin{aligned} \mathrm{Width} &= H \times X \times 8 \\ \mathrm{Height} &= V \times Y \times 8 \end{aligned} \tag{3}$$

where H and V are horizontal and vertical sampling factors. Y stands for number of lines, and X stands for number of MCUs per line. Both of them are specified in the frame header.

2.2. Graphics Interchange Format (GIF) file format

A GIF image file includes a global palette, several frames and local palettes if exist, as shown in Fig. 3. A GIF image file may have many images, and each image is called a frame. If these image data stored in an image file are read frame by frame, an animation forms. In each frame, the image data is stored in the form of indices to the global (or local) palette and is compressed by Lempel–Ziv–Welch (LZW) algorithm (CompuServe Incorporated, 1990).

The indices of each frame is assigned by horizontal and vertical ordinates, just as the same as normal bitmaps. However, to reduce the file size totally, each frame only describes part of the logical

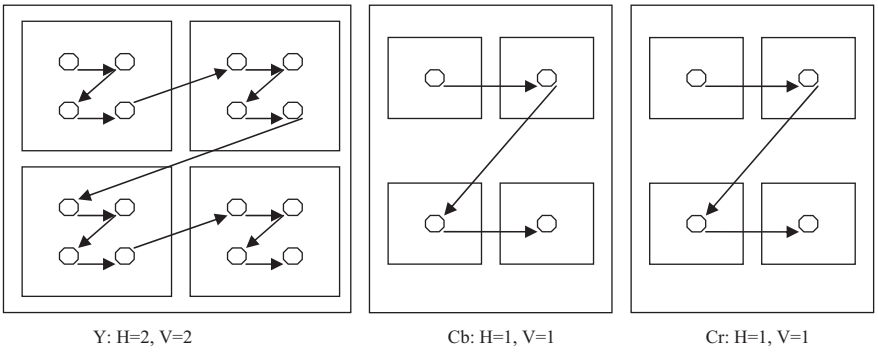

Fig. 2. Interleaved data order example.