Computers and Electrical Engineering 000 (2017) 1–13

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Multiple-image encryption algorithm based on mixed image element and chaos☆

Xiaoqiang Zhang*, Xuesong Wang

School of Information and Electrical Engineering, China University of Mining and Technology, Xuzhou 221116, China

ARTICLE INFO

Article history:
Received 5 March 2016
Revised 25 December 2016
Accepted 26 December 2016
Available online xxx

Keywords:
Multiple-image encryption (MIE)
Single-image encryption (SIE)
Chaotic system
Big image
Encryption efficiency

ABSTRACT

To improve the encryption efficiency and facilitate the secure transmission of multiple images, this paper presents a new multiple-image encryption (MIE) algorithm based on the mixed image element and piecewise linear chaotic maps (PWLCM). Firstly, Alice (the sender) combines original images into a big image, and divides it into many pure image elements; secondly, she scrambles these pure image elements with the chaotic sequence generated by the PWLCM system to get mixed image elements; thirdly, she combines these mixed image elements into a big-scrambled image, and segments it into small images with the equal size of original images; finally, these small images, i.e., encrypted images, are named with the filenames generated by another PWLCM system. Meanwhile, the comparison analysis with a similar existing algorithm is made. Experimental results and algorithm analyses show that the new algorithm is very efficient and secure.

1. Introduction

A large quantity of images are generated in many fields, such as military detection, natural disaster monitoring, traffic monitoring, weather forecasting, electronic government, and personal affairs. Meanwhile, the appearance of all kinds of shooting devices accelerates the age of big data during the past decade. E.g., a common single lens reflex camera can shoot several images per second, and a traffic camera can shoot thousands of images per day at least. In the age of big data, digital images often carry many secrets or much privacy information. With the rapid development of computer and Internet, multimedia security, especially for image security becomes a challenge both for the academic research and industry.

To ensure the security of image transmission, people have proposed many single-image encryption (SIE) algorithms. The main SIE algorithms include the image encryption algorithm based on a modern cryptosystem [1], image encryption algorithm based on a matrix transform [2], image encryption algorithm based on the chaotic system [3], image encryption algorithm in the transform domain [4], and image encryption algorithm based on the DNA computing [5].

In the age of big data, although multiple images can be repeatedly encrypted by the SIE algorithm in theory, the encryption efficiency is always undesirable. As a new multimedia security technology, that possesses high efficiency of secret information transmission, multiple-image encryption (MIE) has received increasing attention. Researchers have proposed several MIE algorithms based on the optical information processing system. E.g., Zhu et al. proposed a MIE algorithm based on the wavelet transform [6]. Li et al. proposed a MIE algorithm based on the cascaded fractional Fourier transform [7].

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Area Editor Dr. E. Cabal-Yepez.

* Corresponding author.
E-mail address: grayqiang@163.com (X. Zhang).

http://dx.doi.org/10.1016/j.compeleceng.2016.12.025
0045-7906/

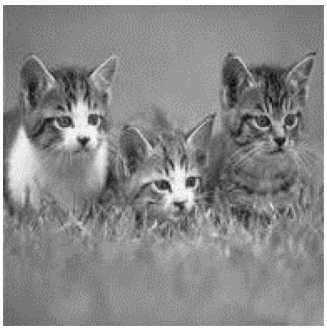

Fig. 1. Cats.

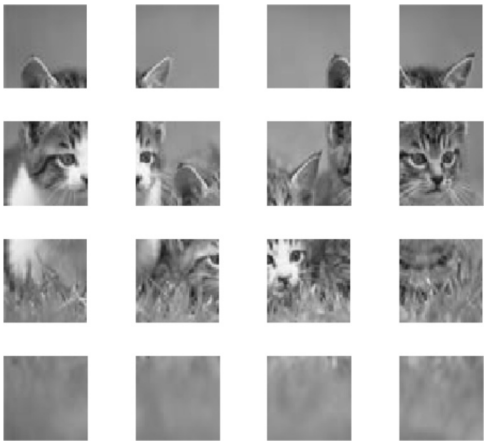

Fig. 2. Pure image elements of cats.

Nevertheless, most of these algorithms encrypt images in the transform domain and usually combine with the image compression technology, so the decryption images are always with some obvious distortion. Meanwhile, these algorithms require the data conversion between the spatial domain and the transform domain. Therefore, their encryption efficiency is always undesirable [8]. In terms of the digital information processing means, Tang et al. proposed a MIE algorithm based on the bit-plane decomposition and the chaotic maps [9]. For the complex computation, its encryption efficiency is undesirable.

To improve the encryption efficiency, this paper presents a new MIE algorithm based on the mixed image element and the piecewise linear chaotic map (PWLCM). Experimental results show its feasibility and high efficiency.

The rest of the paper is organized as follows. Section 2 defines the pure image element and the mixed image element. A new MIE algorithm is designed in Section 3. Experimental results and algorithm analyses are given in Section 4. Section 5 makes a comparison with a similar algorithm. Conclusions are drawn in Section 6.

2. Pure image element and mixed image element

With the knowledge of matrix theory, a big matrix can be easily divided into several small matrixes. Conversely, some small matrixes can constitute a big matrix. In the field of image processing, an 8-bit gray image can be viewed as a matrix in nature, whose pixel values are from the set {0, 1,..., 255}. Therefore, it is easy to segment an image into an orderly group of small images with the modern computer technology. Similarly, it is also much easier to restore the original image from these small images. E.g., Fig. 1 can be easily segmented into 16 small image blocks with the equal size, as shown in Fig. 2. Meanwhile, the original image can be easily restored from these 16 image blocks.

Suppose that k original images are $I^1_{m\times n}, I^2_{m\times n}, \ldots, I^k_{m\times n}$. $I^1_{m\times n}$ can be segmented into a set of small image blocks $\{B^1_i\}$, whose sizes may be different. Any element $B^1_i \in \{B^1_i\}$ is called as the pure image element. Similarly, k sets of pure image elements $\{B^1_i\}, \{B^2_i\}, \ldots, \{B^k_i\}$ can be obtained, which correspond to $I^1_{m\times n}, I^2_{m\times n}, \ldots, I^k_{m\times n}$, respectively. If all these pure image elements are mixed together, a large set $C = \{B^1_i\} \cup \{B^2_i\} \cup \cdots \cup \{B^k_i\}$ can be obtained. Any element $C_i \in C$ is defined as the mixed image element.

Inspired by the jigsaw puzzle, this paper designs a new MIE algorithm based on the mixed image element and chaos. Without the key, it is very difficult to recover original images from mixed image elements, especially for the small sizes of mixed image elements.

Please cite this article as: X. Zhang, X. Wang, Multiple-image encryption algorithm based on mixed image element and chaos, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2016.12.025