Optik 125 (2014) 6117–6122

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Encrypting the compressed image by chaotic map and arithmetic coding

Bin Wang*, Xuedong Zheng, Shihua Zhou, Changjun Zhou, Xiaopeng Wei, Qiang Zhang, Chao Che

Key Laboratory of Advanced Design and Intelligent Computing, Dalian University, Ministry of Education, Dalian 116622, China

ARTICLE INFO

Article history:
Received 31 October 2013
Accepted 3 June 2014

Keywords:
Chaotic map
Image encryption
Image compression

ABSTRACT

Due to the efficient and secure requirements of image transmission, a number of research works have been done to encrypt the compressed image. Inspired by the arithmetic coding and chaotic map which are used to compress and encrypt image, respectively. In this paper, a scheme is proposed to encrypt the compressed image by chaotic map and arithmetic coding. This scheme compresses the image row by row which is firstly permuted by two logistic maps before arithmetic coding. It not only enhances the security of arithmetic coding, but also improves the compression ratio. To further improve the security of binary data which has been compressed, we use the chaotic maps to encrypt the data, and set different parameters and initial value for chaotic maps. In order to possess high sensitivities of key and plain-image, the keys that are employed to determine the parameter and initial value of chaotic maps are related to the plain-image. The experimental results validate the effect of the proposed scheme and demonstrate that the compressed and encrypted image is secure and convenient for transmission.

1. Introduction

Recently, digital image is widely used in the domain of communication, computer science and others. Since digital image possesses some inherent features, such as bulk data capacity and high correlation among adjacent pixels, it is usually compressed before being applied and transmitted. At the same time, the security of information transmission has heightened the need for both research and applications, especially the security of digital image transmission. So a natural idea that joins image compression and encryption is proposed. Some works have been done about image compression and encryption based on chaotic maps [1–11].

There were many reports which used chaotic maps or maps of encrypt digital image [1–4,12–23]. A general permutation–diffusion cryptographic chaos-based architecture that was proposed in Ref. [12] was shown in Fig. 1. It included two iterative stages, namely permutation stage and diffusion stage. The former permuted the plain-image but did not change the value of pixel. The latter changed the value of pixel but did not change the position of pixel. In order to improve the effect of algorithms, the whole permutation–diffusion round would be repeated.

Because the permutation–diffusion architecture was inspired by the classic Shannon's paper on cryptography [24], it was widely used in image encryption based on chaotic maps. In Ref. [1], the authors generalized 2D Cat map to 3D for designing a secure symmetric encryption scheme, which used 3D cat map to permute the position of image pixels in the permutation stage and employed logistic chaotic system to diffuse the permuted image in the diffusion stage. In Ref. [2], the authors firstly analyzed the parameter sensitivity of standard map, and compared the secret key space of standard map with that of cat map and baker map. Then an improved standard map was used to realize position permutation, while the diffusion function consisted of logistic map that was used to realize the diffusion of image. In Ref. [3], the authors proposed a chaos-based image encryption algorithm with variable control parameters. The control parameters used in the permutation stage and the keystream employed in the diffusion stage were generated from two chaotic maps related to the plain-image. A fast image encryption algorithm combined with permutation and diffusion was proposed in Ref. [4]. First, the image was partitioned into blocks of pixels. Then, spatiotemporal chaos was employed to shuffle the blocks, and at the same time, to change the pixel values. Meanwhile, an efficient method for generating pseudorandom numbers from spatiotemporal chaos was suggested, which further increased the encryption speed. In Ref. [13], it was a typical map – the baker map – that was further extended to be 3D and then used to speed up image

* Corresponding author.
E-mail address: wangbinpaper@gmail.com (B. Wang).

http://dx.doi.org/10.1016/j.ijleo.2014.06.107
0030-4026/

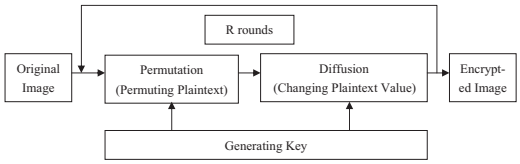

Fig. 1. Flowchart of permutation–diffusion architecture of chaos-based image cryptosystems.

encryption while permuting the position of plain-image. The logistic map was also used to diffuse the permuted image. In Ref. [14], the authors introduced a certain diffusion effect in the permutation stage by simple sequential add-and-shift operations. Although that led to a longer processing time in a single round, the overall encryption time was reduced as fewer rounds were required.

In Ref. [9], the authors developed an efficient prototype for lossy image compression with the property of chaotic maps. In recent years, some approaches had utilized chaotic systems for image compression [10,25,26]. A novel image compression pipeline was proposed in Ref. [10]. In the proposed compression pipeline, a linear feedback control strategy had been used to stabilize chaotic dynamic used to track the 1D signal generated by the input image. In Ref. [25], the authors proposed a copyright protection scheme based on self-similarity of discrete wavelet transform (DCT). Instead of modifying the original image to embed a watermark, the proposed scheme utilized the self-similar property and DWT to generate a watermark certificate from a protected image. A partial encryption technique based on SPIHT encoder was proposed in Ref. [26]. The proposed technique preserved the scalability property of the encoder and provided high data security without adversely affecting the compression efficiency.

Inspired by arithmetic coding, some researchers proposed many algorithms of data compression based on chaotic maps [5,6,8,11,27,28]. Arithmetic coding, in its essence, assigns to each possible character a range, the width of which reflects the frequency of occurrence of the symbol [7,29,30]. Arithmetic coding is a form of variable-length entropy encoding used in lossless data compression. In arithmetic coding, frequently used characters will be stored with fewer bits and not-so-frequently occurring characters will be stored with more bits. It results in fewer bits used in total when a string is converted to arithmetic encoding. Arithmetic coding differs from other forms of entropy encoding such as Huffman coding in that rather than separating the input into component symbols and replacing each with a code, arithmetic coding encodes the entire message into a single number, a fraction n where $0 \leq n < 1.0$.

In Ref. [6], a simultaneous compression and encryption scheme was proposed. This scheme based on the observation that iterating a skew tent map reversely was equivalent to arithmetic coding, where the chaotic map model for arithmetic coding was determined by a secret key and kept changing. Moreover, the compressed sequence was masked by a pseudorandom keystream generated by another chaotic map. In Ref. [8], the authors proposed a new compression method using a particular chaotic modulation type. The presented symbolic approach associated with every informational sequence a trajectory in state space of the chaotic generator. They also introduced a new type of chaotic generator adapted to the probability distribution of the informational sequence, and proved that the theoretical compression performances attained the optimal entropy compression by using described generator. In Ref. [11], the authors proposed an approach for improving the compression performance of an existing chaos-based joint compression and encryption scheme. In the proposed algorithm, the model of sampling without replacement was adopted. In Ref. [27], a novel chaotic encryption scheme was presented which combined arithmetic coding with logistic map. The plaintexts were encrypted and compressed by using an arithmetic coding whose mapping intervals were changed irregularly according to a keystream derived from chaotic map and plaintext. In Ref. [28], the authors generalized the Generalized Luroth Series (GLS) to piecewise non-linear maps (Skewed-nGLS), and motivated the use of Skewed-nGLS as a framework for joint source coding and encryption.

Some works have been done to date, but more studies need to consider the joint image compression and encryption to overcome different attacks for them. Inspired by the introductions above, in this paper, a scheme of image compression and encryption based on arithmetic coding and chaotic map is proposed. We permute the plain-image and encrypt the binary data by chaotic maps which have different parameter and initial values. It can enhance the security of image compression and improve the compression ratio based on arithmetic coding. To resist the cryptanalysis for image which has been compressed such as chosen-plain attack [31], and further heighten the security, the keys that are employed to determine the parameter and initial value of chaotic maps are related to the plain-image. The experimental results validate the effect of the proposed scheme and demonstrate that the encrypted and compressed image is secure for transmission.

The remaining of this paper is organized as follows. In Section 2, the chaotic map and arithmetic coding are briefly introduced. The stage of image compression and encryption is described in Section 3. Performance analysis and simulation results are reported in Section 4. In Section 5, an important reason will be discussed in detail. Finally, conclusions are drawn in Section 6.

2. The chaotic map and arithmetic coding

Due to their features of ergodicity, sensitivity to initial conditions and sensitivity to control parameters, etc., chaotic maps have a good potential for information encryption, especially image encryption. Most chaotic maps are more complex than the logistic map that makes the rise of runtime of chaos-based image encryption. So the logistic map is widely used to design fast architecture of image encryption. Some works related to the logistic map have been published, including parameter sensitivity, initial value sensitivity, statistical properties and degradation phenomenon [32,33]. It can be denoted as follows:

$$x_{i+1} = \mu x_i(1 - x_i) \tag{1}$$

Here μ is control parameter for chaotic map, x_i and x_{i+1} are the ith and the $i+1$th state of chaotic map, respectively. In this paper, the logistic map is used to generate a set of pseudorandom sequences which are employed to permute the plain-image and encrypt the binary data which has been compressed.

As a compression technique, arithmetic coding assumes an explicitly probabilistic model of the source and implements nearly optimal compression with the given probability estimates [7,34,35]. A small example of arithmetic coding algorithm is explained as follows. Consider an alphabet {A, B, C, D} with known probabilistic model {0.6, 0.2, 0.1, 0.1}. The conceptual space [0.1) is divided among A, B, C and D consecutively with A occupying [0, 0.6), B occupying [0.6, 0.8), C occupying [0.8, 0.9) and D occupying [0.9, 1). Consider the process for decoding a message encoded with the given four-symbol model. The message is encoded in the fraction 0.458 (using decimal for clarity, instead of binary; also assuming that there are only as many digits as needed to decode the message). The process starts with the same interval used by the encoder: [0,1), and using the same model, dividing it into the same four subintervals that the encoder must have. The fraction 0.458 falls into the sub-interval for A [0, 0.6); this indicates that the first symbol