Contents lists available at ScienceDirect

Information Sciences

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

Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding

Yu-Guang Yang [a,b,*], Xin Jia [a], Si-Jia Sun [a], Qing-Xiang Pan [a]

[a] College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China
[b] State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China

ARTICLE INFO

Article history:
Received 20 May 2013
Received in revised form 10 February 2014
Accepted 18 February 2014
Available online xxxx

Keywords:
Image processing
Double random-phase encoding
Encryption
Decryption
Quantum Fourier transform

ABSTRACT

A novel encryption/decryption method for color images is proposed, in which quantum Fourier transform (QFT) and double random-phase encoding (DRPE) techniques have been used. The encryption process can be realized by performing two secret random-phase encoding operations respectively in the input and the QFT planes. Because all quantum operations are invertible, the decryption process is the inverse of the encryption process. Supported by detailed numerical simulation and theoretical analysis, the method has clarified its robustness, security and computational complexity over its classical counterpart. And it opens the door for introducing color image encryption into quantum scenarios.

1. Introduction

With the rapid development of multimedia networking and communication, the information security issue has attracted greater attention. Image, one of the most important information representation models, has been widely used in modern society. To realize the secure image transmission in public environment, image encryption technique has been introduced and studied [1,4–7,9,11,18,19,21–25,27,34,35,38,39,44].

Most traditional encryption algorithms, such as advanced encryption standard (AES) algorithm, initially designed for textual data, are too complex to encrypt images due to the unique characteristics of high data rate, loss tolerance and correlation among pixels. The Arnold cat map is often used to diffuse the pixel positions to disturb the high correlation among pixels [5,38]. However, this map has two drawbacks. One is the limited iteration times, usually less than 1000 times, and the other is that the width and height of the original image are required to be equal. Otherwise, the image cannot be completely permuted.

Due to some interesting features such as the ergodicity, mixing and exactness property and the sensitivity to initial conditions, chaotic systems for image encryption have been studied extensively [1,19,21,35,44]. In the cryptographic system, it is very important to choose a good chaotic generator with desirable dynamical statistical properties. It is well known that some smooth chaotic systems, such as the Logistic map, have a dense set of periodic windows for any range of parameter values [9], thus imposing restrictions for the practical applications. Recently, some researchers have investigated image encryption based on hyperchaos. Unfortunately, the hyperchaos-based image encryption strategies are also far from satisfactory [21,35].

* Corresponding author at: College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China. Tel.: +86 01067396818.
E-mail address: yangyang7357@bjut.edu.cn (Y.-G. Yang).

http://dx.doi.org/10.1016/j.ins.2014.02.124
0020-0255/© 2014 Elsevier Inc. All rights reserved.

Optical systems have been deeply developed due to their distinct advantages of processing 2-D complex data with parallelism and high speed. Various optical image encryption algorithms have been proposed during the past two decades [18,24,25,27,34,39]. Although optical systems may be useful for security applications owing to their operation with parallelism and high speed, most optical encryption systems are far from satisfactory. This is because (1) optical elements via free space transmission have big size, weak operating flexibility and stability such as the skew alignment drawbacks and the difficulty of storing and transmitting the encryption results in the form of the complex amplitude distributions for the DRPE method [24]; and (2) most optical encryption systems have vulnerabilities against various attacks. For example, the DRPE method is vulnerable to various attacks including known-plaintext attack [11,22], chosen-ciphertext attack [4] and chosen-plaintext attack [23], etc. Therefore, optical encryption systems should be used cautiously in practice.

With the development of quantum computation, classical image processing is naturally extended to quantum scenarios. As a novel computing model, quantum computation can store, process and transmit information using the peculiar properties of quantum mechanics [20] such as quantum superposition and entanglement. Quantum algorithms like Shor's integer factoring algorithm [26] and Grover's quantum search algorithm [13] have been developed to demonstrate their proven efficiency over the classical versions.

Quantum image processing is focused on images whose physical representation is confined within the realm of quantum mechanics. Research on quantum image processing started with proposals on quantum image representation [16,17,32,33,41,42]. Quantum algorithms have been developed to speed up classical image processing problems because of their proven efficiency over the classical versions [2,3,8,10,12,14,15,28–31]. Although a physical quantum computer has not been realized yet, it seems necessary to perform different information processing tasks on a quantum computer once it can be realized physically.

As a combination of quantum computation and image encryption, quantum image encryption is gradually drawing attention. Zhou et al. [43] presented a quantum gray-level image encryption algorithm based on quantum image geometric transformations. However, it was found that the design of the quantum image encryption/decryption algorithm violates the principles of quantum physics. That is, Zhou et al.'s scheme is invalid. To solve the problem of image encryption on a quantum computer, and to take the merits of optical encryption systems and quantum computation into account, we propose a novel color image encryption method by following the idea of the DRPE raised by Refregier and Javidi [24]. Thanks to the characteristics of quantum computation, the proposed method will greatly improve the efficiency and security of image encryption and decryption.

The rest of this paper is organized as follows. In next section, we discuss the related works. In Section 3, we describe our quantum encryption strategy in detail. Section 4 is devoted to classical simulation and performance comparison. And Section 5 is the conclusion.

2. Related works

Recently, the combination of quantum computation and digital image processing has been proven to be a very fruitful approach to deal with the performance that challenges current image-processing applications. To date, only one quantum gray-level image encryption/decryption algorithm is presented by Zhou et al. [43]. They used quantum image geometric transformations including quantum image translation, image sub-block swapping, image mirror transforms, and image addition and subtraction. However, we find that the design of Zhou et al.'s algorithm violates the principles of quantum mechanics.

It is convenient for us to use the same notations as those in Ref. [43]. Next we will analyze Zhou et al.'s algorithm [43] in detail. Assume the plaintext image is a gray-scale image stored in quantum states, and the corresponding ciphertext will also be quantum gray-scale image in the symmetric cryptosystem circumstance. The quantum image encryption process in Ref. [43] can be described in Fig. 1.

In Fig. 1, the original image I is prepared in quantum states for m times, i.e., m copies as m-layer images which are same as the original one in the state:

$$S = \{|Q\rangle, i\},\ |Q\rangle = \frac{1}{2^n}\sum_{j=0}^{2^{2n}-1}|M\rangle\otimes|j\rangle \qquad i = 1, 2, \ldots m, \tag{1}$$

where S represents the set of the storage, i is the layer number and $|Q\rangle$ is the quantum representation of the gray-level image I.

Then the m-layer images are put into the full-binary-tree array and classified into the layers by means of the left sub-tree, the right sub-tree and the root as shown in Fig. 2.

The connection between the full-binary-tree array and the transformations is established, and the geometric transformations are implemented independently in each layer. Assume that the quantum geometric transform G_i corresponds to the i-th layer of the m-layer images. After the transformations, images in each layer will be expressed as $|Q_i\rangle = G_i|Q\rangle$.

Then the so-called mutual transformations between layers are performed as follows.

Please cite this article in press as: Y.-G. Yang et al., Quantum cryptographic algorithm for color images using quantum Fourier transform and double random-phase encoding, Inform. Sci. (2014), http://dx.doi.org/10.1016/j.ins.2014.02.124