Information Sciences 345 (2016) 257–270

Contents lists available at ScienceDirect

Information Sciences

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

Novel quantum image encryption using one-dimensional quantum cellular automata

Yu-Guang Yang[a,b,c,d,*], Ju Tian[a], He Lei[a], Yi-Hua Zhou[a], Wei-Min Shi[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
[c] Beijing Key Laboratory of Trusted Computing, Beijing 100124, China
[d] National Engineering Laboratory for Critical Technologies of Information Security Classified Protection, Beijing 100124, China

ARTICLE INFO

Article history:
Received 14 May 2014
Revised 23 January 2016
Accepted 29 January 2016
Available online 5 February 2016

PACS:
03.67.Dd
03.65.Ud

Keywords:
Image processing
Image encryption
Quantum cellular automata
One-dimensional
Gray-scale image
Quantum Fourier transform

ABSTRACT

We investigate the application of quantum cellular automata in image encryption and propose a novel quantum gray-scale image encryption algorithm based on one-dimensional quantum cellular automata. The quantum image encryption algorithm can be realized by subtly constructing the evolution rules of one-dimensional quantum cellular automata. Because all quantum operations are invertible, the quantum image decryption algorithm is the inverse of the encryption algorithm. The proposed quantum image encryption algorithm has an algorithm complexity of $\Theta(n)$, lower than the algorithm complexity, $\Theta(n^2)$ of existing quantum image encryption schemes based on quantum Fourier transform. Supported by detailed numerical simulation and theoretical analysis, our proposal has outperformed its classical counterpart and other image encryption schemes in terms of the security, computational complexity, and robustness. And it also provides a clue of introducing quantum cellular automata into image encryption.

1. Introduction

1.1. Background

The combination of quantum mechanics and information theory stimulates the development of quantum communication and quantum computation. Quantum communication involves the secure exchange of information between distant parties over quantum channels. The typical applications include quantum key distribution [3], quantum teleportation [4] and remote state preparation [29], etc. By contrast, quantum computation can store and process quantum information using the peculiar properties of quantum mechanics such as quantum superposition and entanglement. Quantum algorithms like Shor's polynomial speed-up for the integer factoring algorithm [34] and Grover's quadratic speed-up for database search algorithm [13] have been developed to demonstrate their proven efficiency over the classical versions.

With the advancement of quantum computation, an emerging branch, i.e., quantum image processing (QIP) [2,7] is attracting more and more attention. It combines quantum computation and digital image processing and has been proven

* Corresponding author at: College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China . Tel.: +86 01067396818.
E-mail address: 17431644@qq.com, yangyang7357@bjut.edu.cn (Y.-G. Yang).

http://dx.doi.org/10.1016/j.ins.2016.01.078
0020-0255/

Table 1
Complexity comparisons between classical and quantum algorithms. C denotes classical algorithm complexity, and Q for quantum algorithm complexity.

	Fourier transform	Discrete cosine transform	Wavelet transform	Fractional Walsh transform	Discrete Hartley transform	Search algorithm	Prime factorization
C	$\Theta(n2^n)$	$\Theta(n2^n)$	$\Theta(n2^n)$	$\Theta(n2^n)$	$\Theta(n2^n)$	$\Theta(n)$	$\exp(\Theta(n^{1/3}\log^{2/3}n))$
Q	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n)$	$\Theta(n^2)$	$\Theta(\sqrt{n})$	$\Theta(n^2 \log n \log\log n)$

to be very fruitful to deal with the performance that challenges current image processing applications. At present, QIP has four main directions: (1) quantum representation, storage, retrieval and compression of images; (2) expansion of classical transformations into quantum counterparts; (3) quantum watermarking; and (4) quantum image encryption(QIE).

(I) Quantum representation, storage, retrieval and compression of images.
Research in QIP started with proposals on quantum image representation, storage, retrieval and compression such as Qubit Lattice [39,40], Real Ket [23], Flexible Representation of Quantum Images (FRQI) [25], Novel Enhanced Quantum Representation of digital images (NEQR) [48], quantum representation for log polar images [49] and other novel methods for quantum representation, storage, retrieval and compression [14,26–28], etc. The quantum images are two-dimensional arrays of qubits in Refs. [39,40] and a quantum state in Ref. [23], respectively. The FRQI model [25] encodes information about the color and position of each pixel in an image into a normalized quantum superposition state. The NEQR representation [48] improves the FRQI model and uses the basis state of a qubit sequence to store the gray-scale value of each pixel in the image, instead of the probability amplitude of a qubit, as in FRQI model. Refs. [14,26–28] proposed various novel methods for multidimensional color image storage, retrieval and compression.

(II) Expansion of classical transformations into quantum counterparts.
The quantum counterparts of many classical transformations have been proposed, including quantum Fourier transform (QFT) [31], quantum Cosine transform (QCT) [16,36], quantum Wavelet transform (QWT) [9], quantum Walsh transform (QWT) [24], and quantum Hartley transform (QHT) [37,38]. These quantum transforms are more efficient than their classical counterparts [31]. Table 1 summarizes the complexity comparisons between some classical algorithms and their quantum counterparts.

(III) Quantum watermarking.
Watermarking is aimed to guard against data abuse by embedding invisible watermark signal into public data carriers while the watermarked carriers are still readable. The users of the public data cannot feel the existence of the watermark signal so that the safety of the watermark information embedded in the public data can be ensured. The embedded watermark information can be used to protect copyright or to communicate secretly. However, a watermarking scheme is limited by the tradeoff between robustness and payload. As the quantum counterpart of classical watermarking schemes, several quantum image watermarking schemes were proposed [15,43,44,50] based on quantum transformations such as QFT and geometric transformations of quantum images (GTQI).

(IV) Quantum image encryption.
In an encryption scheme, the sender encrypts and transmits the data in public environment, and only the designated receiver can decrypt the encrypted data with the decryption key. Different from watermarking, the attacker can detect the existence of the secret information but unfortunately he/she cannot illegally obtain it. As the quantum counterpart of classical encryption schemes, several QIE algorithms were proposed [45–47,52].

1.2. Motivation

In this paper, we focus on QIE. To date, very few results on QIE were presented [45–47,52]. For example, Zhou et al. [47] presented a quantum gray-scale image encryption algorithm based on GTQI. By taking the merits of optical encryption and quantum computation into account, we [45,46] proposed two novel QIE methods for gray-scale images and color images based on QFT and double random-phase encoding (DRPE) [33], respectively. However, the two schemes [45,46] have some drawbacks: (i) because of the use of the FRQI model, to extract the information about the decrypted quantum image state, many copies of quantum image states have to be prepared, and are measured to summarize some sort of histogram; and (ii) the computational complexity of these two schemes depends on that of QFT, i.e.,$\Theta(n^2)$ [31] and thus the QFT-based QIE algorithms have a computational complexity of $\Theta(n^2)$ gates. Because of the expensive quantum devices and the difficulty of quantum operations, a natural question exists. Can we design a QIE algorithm with a lower computational complexity?

Classical cellular automata (CA) first proposed by von Neumann serves as a model of self-replication systems [30]. Wolfram investigated one-dimensional CA with one bit per cell [41]. Since then, CA has successfully served as a kind of parallel-computation architecture to simulate physical systems and processes [17–19]. It was also developed to model quantum systems, referred to as quantum cellular automata (QCA) [10]. However, the “no-go” lemma shows that only trivial QCA with one qubit per cell may exist and it is impossible to perform unitary evolution of one-dimensional QCA given the “no-go” lemma [11]. Fortunately, QCA with two qubits per cell can bypass the “no-go” lemma [20] and it has linear unitary evolution and maybe serves the image encryption.