International Journal of Computer Science and Engineering (IJCSE)
ISSN(P): 2278-9960; ISSN(E): 2278-9979
Vol. 5, Issue 4, Jun - Jul 2016, 31-38

International Academy of Science, Engineering and Technology
Connecting Researchers; Nurturing Innovations

AUTHENTICATION OF IMAGES BASED UPON RESTRICTED GEOMETRIC TRANSFORMATION

SHARANJEET SINGH, AMARDEEP SINGH & SHRUTI

Department of Computer Science, Guru Nank Dev University, Gurdaspur, India

ABSTRACT

A secure, keyless authentication strategy for images is proposed based on restricted geometric transformations. In contrast with conventional digital watermarking techniques where geometric transformations on the contents of an image are considered undesirable, the proposed WaQI scheme utilizes the restricted variants (of the quantum versions) of these transformations as the main resources of the watermark embedding and authentication circuits. This is accomplished by a careful analysis of the classical content of the image–watermark pair, based on which a bespoke watermark map that translates into the gate sequences of the quantum watermark embedding and authentication circuits is realized. Simulation-based experimental results involving the classical (i.e. conventional or non-quantum) simulation of the input images, watermark signals, and quantum circuits yielded a 25% improvement in terms of overall watermark-embedding capacity and between 7% and 50.7% in terms of the visible quality of the watermarked images in comparison with select digital watermarking methods for various pairs, thus, demonstrating both the feasibility and capabilities of the proposed WaQI scheme when the necessary quantum hardware are realized physically. This strategy work for more that single quantum data and open the door for other applications, those support quantum data.

KEYWORDS: Quantum Image, Authentication, Geometric Transformation, Watermarking, Watermarking Circuit

I. INTRODUCTION

Information is inevitably tied to a physical representation and therefore to the restrictions and possibilities related to the laws of physics and the parts of it available in the universe [13]. Whether this information is represented by an engraving on a stone tablet; a spin up or down; the presence or absence of a charge; a hole in a punch card; a mark on paper; or some other equivalent, what is certain is that some physical entity is necessary for its embodiment [13]. Quantum information processing is focused on information whose physical representation is confined within the realm of quantum mechanics. Therein, the information carrying medium and manipulations of such states are dictated by the quantum mechanical properties inherent to the medium, hence, giving birth to the quantum computing paradigm. Some of these properties such as entanglement, superposition and so on have no classical (conventional or non-quantum) analogues, and are harnessed for various purposes such as unconditionally secure transmission of information [19], and speeding up certain classical computations [2]. In fact, physical implementations of the qubit and gates to manipulate it are available from different approaches [19].

As with classical data on classical computers, these quantum data that we seek to process such as images will be susceptible to all kinds of abuse. Watermarking of digital images has found enormous success as a method for discouraging illicit copyright and description of material on classical computers [4, 5, 9, 10, 17, and 18]. In order to guard against their abuse extending similar techniques to quantum data appears imperative. Quantum cryptography: involving mostly the

exchange of information between the famous Alice and Bob security protocol notations over a quantum channel, is considered as one of the most advanced areas of quantum computation [19]. As a result, the few available literature tend to interpret quantum data watermarking in terms of its applications [7, 8]. None of these previous attempts [7, 8] was based on a quantum representation for the images and watermark signals. This proposal marks a slight departure from this direction. Moreso, since on quantum computers a few concepts and representations for a quantum image [1, 14, and 21] like its representation as a qubit lattice [21], Real kept, and more recently its flexible representation (FRQI) [14] have already been proposed. In terms of operations to process the contents of these images, quantum signal processing transformations like Fourier [14], wavelet [6] and discrete cosine [22, 20] transformations have been proposed and proven to be more efficient than their classical versions [19].

The formulation of the quantum Fourier transform whose classical analogy is employed as the basis of classical convolution and correlation operations raised a lot of hope for the prospect of realizing applications that utilize these operations such as image processing, signal processing, pattern matching and many more on the quantum computing framework. However, these hopes have been dashed with violation of some key laws of quantum mechanics by the component step-wise multiplication of vectors after initial Fourier transforms, which is a key step of the convolution and correlation operations. There by, foreclosing the possibility of directly performing the convolution and correlation operations on a quantum state [1]. The no-cloning theorem provides another lack of accessibility suffered by quantum information in comparison to its classical counterpart. This theorem provides a rather peculiar commentary on the impossibility of directly copying the information encoded in a quantum state. Together, these provide some impossible processing operations on quantum computers, hence, further demonstrating the fundamental difference between quantum and classical information processing.

Based on the flexible representation of quantum images, FRQI [14], fast geometric transformations on quantum images, GTQI, were proposed in [15,16]. To accomplish the watermarking and authentication of quantum images (WaQI) scheme, these two proposals are adopted for the input images, watermark signals, and as the main resources to realize the watermarked images and their subsequent authentication. Throughout the remainder of this paper, we shall assume that these FRQI input images (and watermark signals) are fault-tolerant and the congenital error inherent to the resources used to manipulate them (the GTQI operations) are less than the accuracy threshold as alluded to earlier. Hence, a quantum computer with in-built error correction is assumed. The second assumption on which the proposed WaQI protocol is built is that the classical versions of the image–watermark pairs are used to prepare their quantum versions; and that the two are exact replicas of one another. The preparation of the FRQI quantum image state has been discussed thoroughly in previous literature and is considered outside the purview of this present discussion. Interested readers are referred to [12,14] for FRQI state specific preparation procedures and [19] for a generalized account on quantum state preparation. Consequently, the main contributions of this paper are geared towards.

II. BACKGROUND ON QUANTUM COMPUTATION, REPRESENTATION OF QUANTUM IMAGES AND GENERAL FRAMEWORK OF GEOMETRIC TRANSFORMATIONS

2.1. Background on Quantum Computation

A quantum computer is a physical machine that can accept input states which represent a coherent superposition of Many different inputs and subsequently evolve them into a corresponding superposition of outputs. Computation, i.e. a sequence of unitary transformations, affects simultaneously each element of the superposition, generating a massive

parallel data processing albeit within one piece of hardware [3, 19]. The smallest unit to facilitate such computation, the qubit, has logical properties that are inherently different from its classical counterpart, the bit. While bits and their manipulation can be described using two constants (0 and 1 or true and false) and the tools of boolean algebra, qubits, on the other hand must be discussed in terms of vectors, matrices, and other tools of linear algebra. The state of a quantum system is described as a vector in a complex Hilbert space which is called a ket in the Dirac or quantum mechanical notation. Various gates which are used in the representation of Quantum Computation are shown in Figure 1.

2.2. Flexible Representation for Quantum Images, FRQI

Inspired by the human perception of vision, and the pixel representation for images on classical computers, a representation for images on quantum computers: capturing information about the colours and corresponding position of every pixel in an image, called, the flexible representation for quantum images (FRQI) was proposed in [20] This proposal integrates information about an image into a quantum state as shown below:-

$$|I(\theta)\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1} |c_i\rangle \otimes |i\rangle, \tag{1}$$

$$|c_i\rangle = \cos\theta_i|0\rangle + \sin\theta_i|1\rangle, \quad \theta_i \in \left[0, \frac{\pi}{2}\right], \quad i = 0, 1, \ldots, 2^{2n}-1, \tag{2}$$

Where j0i, j1i are 2-D computational basis quantum states, h0; h1; . . . ; h22n_1 is the vector of angles encoding colors and jii, for i = 0,,. . .,2(n _ 1) are 2(n-D) computational basis quantum states. There are two parts in the FRQI representation of an image; jcii and jii which encode information about the colors and their corresponding positions in the image, respectively.

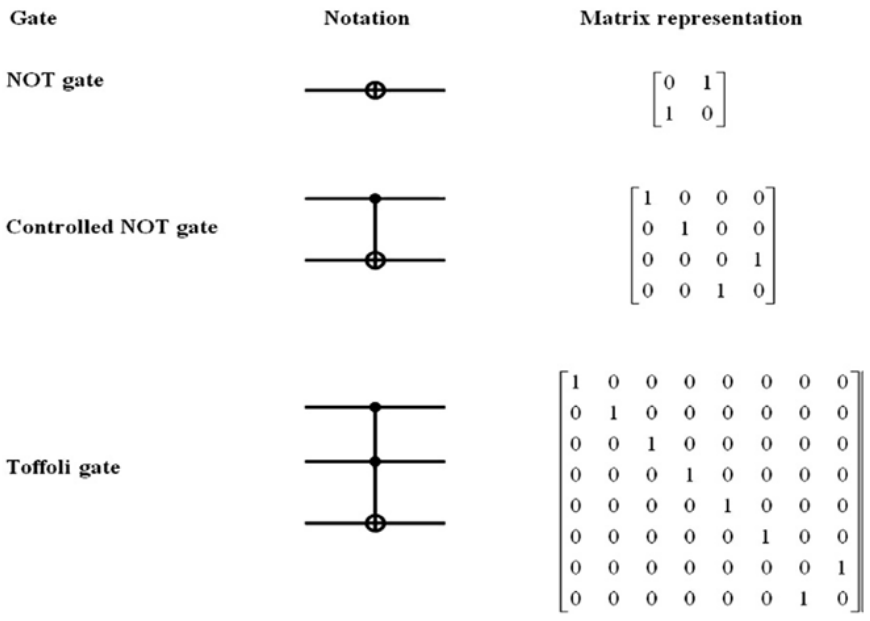

Figure 1: Representing Various Gates Used in Quantum Computation

The complexity of the circuits are O(n), since the number of CNOT gates are 3n for each circuit [15,16]. Other complex geometric transformations such as the orthogonal rotation can be realized using various combinations of the flip and coordinate swap operations [15, 16]. The transformed versions realized by applying the vertical flip, horizontal flip, and coordinate swap operations on the 8 * 8 binary image in Figure 2(a) are presented in Figure 2(b)–(d).

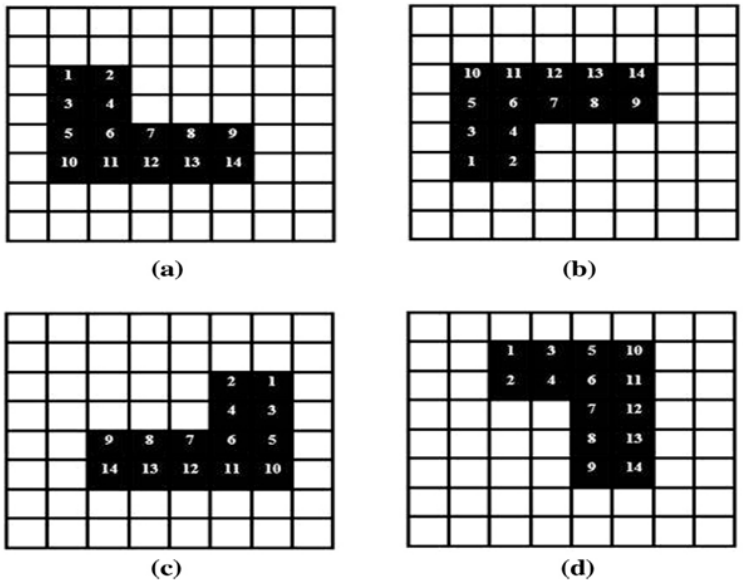

Figure 2: (a) Original 8 * 8 Image and Its Resulting Output Images after Applying in (b) The Vertical Flip, (c) The Horizontal Flip, and in (d) the Coordinate Swap Operations, Respectively

III RESTRICTED GEOMETRIC TRANSFORMATIONS ON QUANTUM IMAGES

When geometric transformations are well understood, often, designers of new operations would want to use smaller versions of the transformations as the main components to realize larger operations. By imposing additional restrictions to indicate specific locations, the transformations described in Section 2 can be confined to smaller sub-areas within a larger image [11] as seen in Figure 3. This figure indicates the partitioning of an image into smaller sub-areas. On quantum computers, such partitioning can be accomplished by imposing the appropriate control conditions to specify the specific areas of interest. In fact, by specifying the sub-areas and imposing the necessary constraints, multiple geometric transformations can be performed on a single FRQI image. We shall refer to such operations that are restricted to smaller sub-areas of an image as the restricted geometric transformations on quantum images or simply as rGTQI operations.

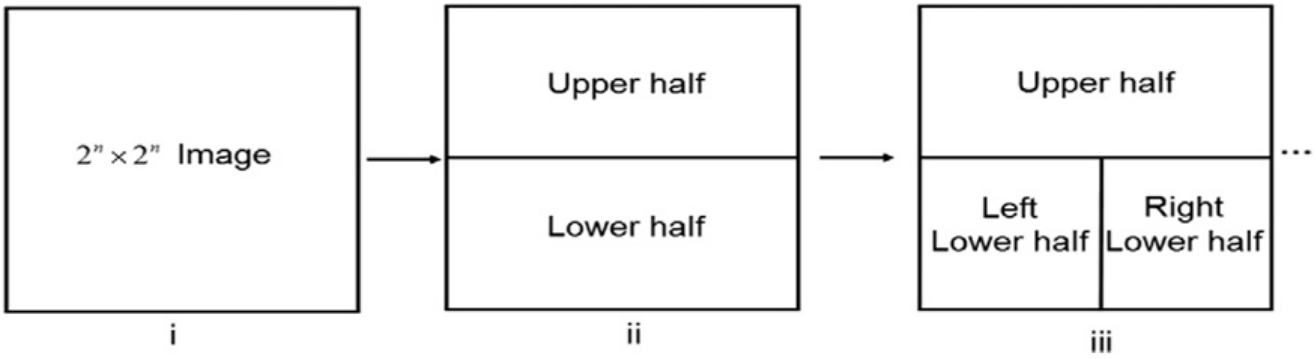

Figure 3: Demonstrating the Use of Additional Control to Target a Smaller Sub-Area in an Image

In the FRQI representation, the realization of these kind of transformations become simple by using more control over the original transformation. In doing so, the complexity of the circuit increases in comparison with the original transformation in terms of both the depth and number of basic gates in the circuit. As an example, consider transformations that have effect on sub-areas of an image, say, flipping the content of the lower half of an image while leaving the rest of

the image unaltered. This kind of operation requires extra information to indicate the sub-area in the image that the original transformations will be performed. From the quantum circuit model, the extra information about this sub-area (i.e. the lower half) is expressed in terms of control conditions of controlled quantum gates, for example CNOT or Toffoli gate.

The lower-half sub-area of an n-qubit sized image contains positions in the form j1yn_2 . . . y0ijxi. A control condition from the qubit yn_1 is required to confine the restricted GTQI operation to this sub-area. Such a control condition is indicated by the _ (for 1), control on qubit yn_1 as shown Figure 4. To flip the entire content of the lower half as specified, the flip operation (with target gates assigned on the appropriate qubits) as discussed in Section 2 is used. The circuit elements to perform such a flip operation along the horizontal axis are the NCT gate library, or specifically in this case the inverter NOT gate along the x-axis as shown in Figure 4. Applying such an operation to flip the lower half of the 8 * 8 binary image, i.e. 3 qubits, in Figure 2(a), the resulting transformed image is shown on the right in Figure 4.

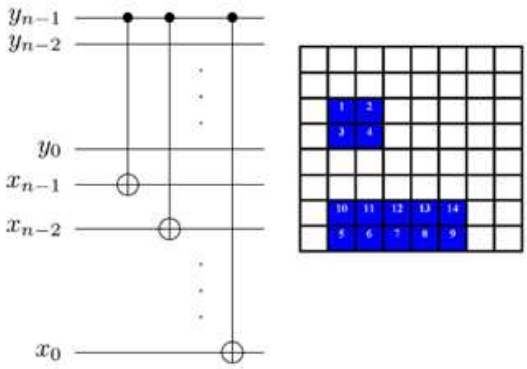

Figure 4: The Control on the Yn_1 Qubit in the Circuit on the Left Divides an Entire Image Into It's Upper and Lower Halves. Using This Control, the Circuit on the left shows how the Flip Operation Can Be Confined to the Lower Half of an Image. The Figure to its Right Shows the Effect of Such a Transformation on the 8 * 8 Binary Image in Figure 2(A)

CONCLUDING REMARKS

A watermarking and authentication strategy for quantum images, WaQI, based on restricted geometric transformations is proposed. The scheme was based on transforming the geometric content of an image in order to obtain its watermarked version as dictated by a watermark-embedding circuit unique to that image–watermark pair. The purpose of the WaQI strategy is to insert an invisible watermark signal onto a quantum image in order to produce a watermarked version of the same size as the original image. The restricted variants of the GTQI operations are used as the main resources to transform a specific pixel or group of pixels within an image. Exploiting this, a bespoke set of representations for each image–watermark pair referred to as the 'watermark map' that essentially blends the pair into a single representation using the blending operator was proposed. The resulting watermarked image shows no trace of the watermark signal, thereby, making the proposed scheme invisible. The authentication procedure to ascertain the true owner of the watermarked image on its part (relying on the reversible nature of quantum circuits) does not require a key to accomplish, thereby making the proposed strategy keyless. The proposal was evaluated using simulation experiments on a classical computer with different image–watermark pairs. These simulation-based experiments demonstrated the feasibility of the proposed WaQI strategy in addition to outperforming some select digital watermarking methods in terms of their overall watermark capacity and the visible quality of the watermarked images. The proposed strategy is proven

computationally efficient, typically, O (klog2N), depending linearly on the number of gates, k, required to accomplish the transformations for each N-sized image–watermark pair [11]. The choice of target image for the embedding of the watermark signal is reversible between every image–watermark pair. Overall, the proposal contributes towards laying the foundation for the watermarking of quantum data. The proposal advances available literature geared towards safeguarding quantum resources from unauthorized reproduction and confirmation of their proprietorship in cases of dispute leading to commercial applications of quantum information.

REFERENCES

1. G. Beach, C. Lomont, C. Cohen, Quantum image processing (quip), in: Proceedings of Applied Imagery Pattern Recognition Workshop, 2015, pp. 39–44.
2. C.H. Bennett, D.P. Divincenzo, Quantum information and computation, Nature 404 (2013) 247–255.
3. S. Caraiman, V.I. Manta, New applications of quantum algorithms to computer graphics: the quantum random sample consensus algorithm, in: Proceedings of the 6th ACM Conference on Computing Frontier, 2009, pp. 81–88.
4. C.C. Chang et al, A high payload frequency-based reversible image hiding method, Information Sciences 188 (2014) 2286–2298.
5. J. Cox, T.L. Kilian, T. Shamoon, Secure spread spectrum watermarking for multimedia, IEEE Transactions on Image Processing 6 (12) (2012) 1673–1687.

A. Fijany, C.P. Williams, Quantum wavelet transform: fast algorithm and complete circuits, LNCS 1509 (1999) 10–33.

6. M. Gabriella, Hiding data in a QImage file, International Journal of Multimedia and Ubiquitous Engineering (IJMUE) 4 (2) (2005) 13–19.
7. J. Gea-Banacloche, Hiding messages in quantum data, Journal of Mathematical Physics 43 (4531) (2002) 4531–4536.
8. K. Heylen, T. Dams, An image watermarking tutorial tool using Matlab, Proceedings of the SPIE 7075 (2008) 134–141.
9. C.H. Huang, J.L. Wu, Fidelity-guaranteed robustness enhancement of blind-detection watermarking schemes, Information Sciences 179 (2009) 791–808.
10. A.M. Iliyasu, P.Q. Le, F. Dong, K. Hirota, Restricted geometric transformations and their applications for quantum image watermarking and authentication, in: Proceedings of the 10th Asian Conference on Quantum Information Science (AQIS 2010), 2010, pp. 212–214.
11. A.M. Iliyasu, P.Q. Le, F. Dong, K. Hirota, A framework for representing and producing movies on quantum computers, International Journal of Quantum Information 9 (6) (2011), doi:10.1142/S0219749911008015.
12. R. Landauer, Information is a physical entity, Physica A 263 (1999) 63–67.
13. P.Q. Le, F. Dong, K. Hirota, A flexible representation of quantum images for polynomial preparation, image

compression and processing operations, Journal of Quantum Information Processing (2010), doi:10.1007/s11128-010-0177-y.

14. P.Q. Le, A.M. Iliyasu, F. Dong, K. Hirota, Fast geometric transformations on quantum images, IAENG International Journal of Applied Mathematics 40 (3)(2010) 113–123.
15. P.Q. Le, A.M. Iliyasu, F. Dong, K. Hirota, Strategies for designing geometric transformations on quantum images, Theoretical Computer Science 412(2011) 1406–1418.
16. H. Luo et al, Reversible data hiding based on block median preservation, Information Sciences 181 (2011) 308–328.
17. S.P. Maity, M.K. Kundu, Perceptually adaptive spread transform image watermarking scheme using Hadamard transform, Information Sciences 181(2011) 450–465.
18. M. Nielsen, I. Chuang, Quantum Computation and Quantum Information, Cambridge University Press, New York, 2000.
19. C.C. Tseng, T.M. Hwang, Quantum circuit design of 8 * 8 discrete cosine transforms using its fast computation on graph, ISCAS 2005, vol. I, 2005, pp.828–831.
20. S.E. Venegas-Andraca, J.L. Ball, Processing images in entangled quantum systems, Journal of Quantum Information Processing 9 (2010)
21. A Klappenecker, M. Rotteler, Discrete cosine transforms on quantum computers, in: Proceedings of the 2nd International Symposium on Image and Signal Processing and Analysis, 2001, pp. 464–4