Security of NEQR Quantum Image by Using Quantum Fourier Transform with Blind Trent

Engin ŞAHİN*, İhsan YILMAZ**

* Department of Computer and Instructional Technologies Education, Faculty of Education, Çanakkale Onsekiz Mart University, Çanakkale, Turkey. e-mail: enginsahin@comu.edu.tr
** Department of Computer and Instructional Technologies Education, Faculty of Education, Çanakkale Onsekiz Mart University, Çanakkale, Turkey. e-mail: iyilmaz@comu.edu.tr

Abstract—In this study, the security of Novel Enhanced Quantum Representation (NEQR) of quantum images are suggested by using the Quantum Fourier Transform (QFT) with blind trent. In the protocol, QFT and keys are used to share signature with recipients. So all members know only their signature information which are encrypted output of the QFT. This improves the security of the protocol. In addition, the security of the protocol is provided by using reorder QFT output qubits with permutation of the blind trent. The security analysis expresses security of the transfer of the image with effective secret key usage.

Keywords—Quantum Image Encryption and Authentication, Quantum Fourier Transform, Quantum Digital Signature.

1. Introduction

Conventional image security techniques, such as digital watermarking and image encryption, are commonly used to protect the image effectively. Possible threats in image transmission are capturing of image by unauthorized persons and authentication of the image. These issues are very important for special applications such as transmission of military satellite images or patient records.

There are many quantum image representations such as the ”Qubit Lattice” representation for encoding a quantum image [1], the ”Real KET” representation [2], Flexible Representation of Quantum Image (FRQI) [3], Multi-Channel Representation for Quantum Images (MCQI) [4], Novel Enhanced Quantum Representation (NEQR) [5], Quantum Image Representation for Log-Polar Images (QUALPI) [6], Simple Quantum Representation of Infrared Images (SQR) [7], Quantum States for M Colors and N Coordinates (QSMC & QSNC) [8], Normal Arbitrary Quantum Superposition State (NAQSS) [9] and Quantum RGB Multi-Channel Representation (QMCR) [10].

Also, in the literature there some studies on the security of quantum images. Iliyasu et. al. [11] proposed the WaQI scheme based on restricted geometric transformations for quantum image watermarking and authentication. Iliyasu et. al. [12] proposed the improved WaQI scheme which is secure, keyless, blind and perfectly usable for authentication of the image owner. Later, Iliyasu et. al. [13] proposed GWaQI scheme with two-tier for greyscale quantum image watermarking and recovery. Yan et. al. [14] proposed MC_WAQI model based on MCQI representation for color quantum images.

In this study, we propose the protocol based on

the QFT with blind Trent for image security and authentication. The paper can be outlined as follows; in Section 2,basic concepts of QFT and $NEQR$ are explained; In Section 3, base stages of the protocol based on QFT with blind trent are introduced. In Section 4, the security analysis of the protocol according to forgery and repudiation concepts are given. In Section 5, in the conclusion, some results are discussed.

2. Related Works

2.1. Quantum Fourier Transform

Quantum Fourier transform is a application of classical discrete Fourier transform to the quantum states [15]. The QFT transform of an orthonormal basis set $|0\rangle, |1\rangle, ..., |N-1\rangle$ can be defined as follows [15]:

$$|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i x y/N} |y\rangle \tag{1}$$

Where $N = 2^n$ and orthonormal basis set is $|0\rangle, |1\rangle, ..., |2^n-1\rangle$. The $|x\rangle$ state can be written in binary form as $x = x_0 x_1 ... x_{N-1}$. The circuit of Quantum Fourier Transform for $|x\rangle$ can be seen in Fig.1. The $|x\rangle$ state is transformed into the phase of qubits as results of the QFT transform.

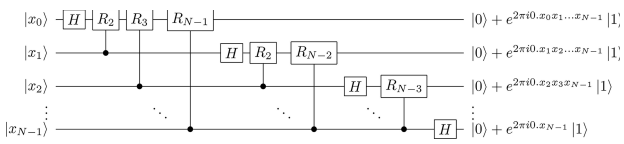

Fig. 1. Quantum Fourier Transform Circuit [15]

2.2. NEQR

NEQR uses the basis states of qubit sequence to store the color values. it represents grayscale images. Suppose the gray scale of images is 2^q. Binary sequence $C_{YX}^0 C_{YX}^1 ... C_{YX}^{q-2} C_{YX}^{q-1}$ encodes the grayscale value $f(Y,X)$ of the corresponding pixel (Y,X) as follows [5]:

$$\begin{aligned} f(Y,X) &= C_{YX}^0 C_{YX}^1 ... C_{YX}^{q-2} C_{YX}^{q-1}, \\ C_{YX}^k \in [0,1], &\quad f(Y,X) \in [0, 2^q - 1] \end{aligned} \tag{2}$$

The representative expression of a quantum image for a $2^n \times 2^n$ image can be written as follows [5]:

$$\begin{aligned} |I\rangle &= \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |f(Y,X)\rangle |YX\rangle \\ &= \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \bigotimes_{i=0}^{q-1} |C_{YX}^i\rangle |YX\rangle \end{aligned} \tag{3}$$

3. The Protocol based on QFT with Blind Trent for NEQR Image

The participants of the protocol are Alice, Bob and Trent. Alice would like to send 2^q grayscale $2^n \times 2^n$ NEQR quantum image $|I\rangle$ to Bob by encrypting.In this case $N = q + 2n$. Blind Trent is assumed as a manager of the protocol. Blind Trent manages some communication to provide security of the protocol. Bob can obtain and verify the image $|I\rangle$ with help of the blind Trent.

The protocol can be described with following phases.

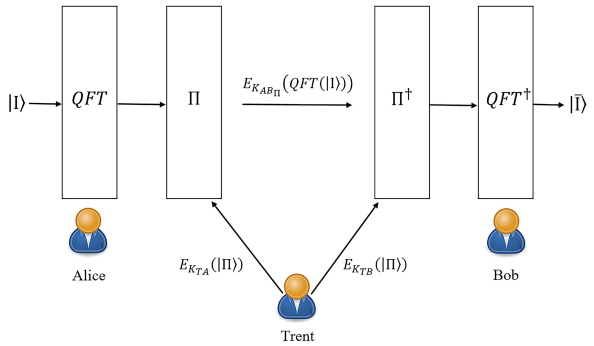

Fig. 2. Security of NEQR quantum images based on QFT with blind Trent

3.1. Initialization Phase

(i) Alice shares secret key K_{AB} with Bob. Also blind Trent shares secret key K_{TA} with Alice and secret key K_{TB} with Bob. Participant's secret keys K_{AB}, K_{TA}, K_{TB} are shared by using quantum key distribution(QKD) protocol [16], [17]. The secret keys are used to encrypt quantum image to prevent any attackers. The encryption algorithm is given in Eq. 10 and Eq. 11. The length of the all keys are $|K| = 8N$. K_{AB}, K_{TA}, K_{TB} secret keys are created only once. Then the secret keys can be divided into 8-bit pieces. Each piece of the secret keys will be applied to every qubit of the QFT output according to the permutation determined by the blind trend. Different K_{AB}, K_{TA}, K_{TB} secret keys are created for each different sessions. If we apply stages in [18] to the NEQR image and use secret keys, we get the following stages.

(ii) Alice prepares her 2^q grayscale $2^n \times 2^n$ image I with NEQR model . We assume that the length of the $|I\rangle$ is $|\,|I\rangle\,| = N$.

$$\begin{aligned}|I\rangle =& \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|f\,(Y,X)\rangle\,|YX\rangle \\ =& \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{q-1}|C_{YX}^{i}\rangle\bigotimes_{j=0}^{n-1}|y_Y^j\rangle\bigotimes_{j=0}^{n-1}|x_X^j\rangle\end{aligned} \tag{4}$$

Where $|C_{YX}^{i}\rangle\,, |y_Y^j\rangle\,, |x_X^j\rangle \in \{|0\rangle\,, |1\rangle\}$.

(iii) Blind Trent creates a permutation P of a set of $\{1, 2, ..., N\}$ as follows [18]:

$$P = \begin{bmatrix} 1 & 2 & ... & N \\ P(1) & P(2) & ... & P(N) \end{bmatrix} \tag{5}$$

$P(i)$ can be expressed in binary string as follows:

$$\begin{aligned}P_{binary}(i) =& P^0(i)P^1(i)...P^{k-1}(i) \\ & P^j(i) \in [0,1]\end{aligned} \tag{6}$$

Where $k = \log_2(P(i))$. Then Blind Trent prepares a quantum state $|P(i)\rangle$ from $P_{binary}(i)$ using by computational bases ($0 \rightarrow |0\rangle$ and $1 \rightarrow |1\rangle$). Then blind Trent prepares a quantum state of $|P\rangle$ as follows:

$$|P\rangle = \bigotimes_{i=1}^{N}|P(i)\rangle \tag{7}$$

Blind Trent creates encrypted versions of that permutation as follows:

$$|P_A\rangle = E_{K_{TA}}(|P\rangle) \tag{8}$$

$$|P_B\rangle = E_{K_{TB}}(|P\rangle) \tag{9}$$

$E_K(.)$ is a quantum one-time pad encryption algorithm which is firstly defined by Kim et. al. [19] and used by Yılmaz [18] to improve security of the protocol against forgery attacks. To further improve the security of this quantum encryption algorithm, we reorganized the algorithm of Zhang et. al. [20] as follows:

$$\begin{aligned}E_K(|I\rangle) = \bigotimes_{i=0}^{N-1} & {\sigma_x}^{K_{8i}}{\sigma_z}^{K_{8i+1}}T{\sigma_x}^{K_{8i+2}}{\sigma_z}^{K_{8i+3}} \\ & T{\sigma_x}^{K_{8i+4}}{\sigma_z}^{K_{8i+5}}T{\sigma_x}^{K_{8i+6}}{\sigma_z}^{K_{8i+7}}|I_i\rangle\end{aligned} \tag{10}$$

$$T = \frac{i}{\sqrt{3}}(\sigma_x - \sigma_y + \sigma_z) \tag{11}$$

Due to using T, encrypted message cannot be forged [19]. Where the key length is $|K| = 8N$. Then, blind Trent sends encrypted $|P_A\rangle$ to Alice via quantum channel.

(iv) Alice decrypts $|P_A\rangle$ and makes measurement to obtain P [18].

(v) Alice applies QFT to NEQR image and obtains following state:

$$QFT\left(|I\rangle\right) = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}$$
$$\left(QFT\left(|c_{YX}^0...c_{YX}^{q-1}y_{YX}^0...y_{YX}^{n-1}x_{YX}^0...x_{YX}^{n-1}\rangle\right)\right)$$
$$= \frac{1}{2^n}\frac{1}{\sqrt{2^N}}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\left(|0\rangle + e^{2\pi 0.x_{YX}^{n-1}}|1\rangle\right)$$
$$\otimes\left(|0\rangle + e^{2\pi 0.x_{YX}^{n-2}x_{YX}^{n-1}}|1\rangle\right)\otimes ...$$
$$\otimes\left(|0\rangle + e^{2\pi 0.c_{YX}^0 c_{YX}^1...x_{YX}^{n-1}}|1\rangle\right) \tag{12}$$

Where $N = q+2n$. Also we show it as follows:

$$\bigotimes_{i=0}^{N-1}|I_i\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}\bigotimes_{i=0}^{q-1}|C_{YX}^i\rangle\bigotimes_{j=0}^{n-1}|y_Y^j\rangle \bigotimes_{j=0}^{n-1}|x_X^j\rangle$$

$$QFT\left(|I\rangle\right) = \frac{1}{\sqrt{2^N}}\bigotimes_{i=0}^{N-1}QFT\left(|I_i\rangle\right)$$

3.2. Signing Phase

(i) Alice reorder $QFT\left(|I_i\rangle\right)$ states with permutation of blind Trent.

$$|A(Q)\rangle = SWAP(P(i))(QFT(|I_i\rangle)) \quad i = 0...N-1 \tag{13}$$

(ii) Alice encrypts all qubits of Eq. 13 with secret key K_{AB}.

$$|A(S)\rangle = E_{K_{AB_{P_A(i)}}}(|A(Q)\rangle) \quad i = 0...N-1 \tag{14}$$

(iii) Alice sends $|A(S)\rangle$ to Bob via quantum channel.

(iv) Alice encrypts $QFT(|I_i)\rangle$ with secret key K_{AB} with the encryption algorithm [18] (see references there in) and sends to blind Trent via quantum channel.

$$|AT(S)\rangle = E_{K_{AB}}(QFT(|I_i\rangle)) \tag{15}$$

(v) Blind Trent encrypts the $|AT(S)\rangle$ with the secret key K_{TB}.

$$|TB(S)\rangle = E_{K_{TB}}(|AT(S)\rangle) \tag{16}$$

Then, blind Trent sends the above encrypted state to Bob via quantum channel.

3.3. Verification Phase

(i) Bob decrypts $|TB(S)\rangle$ with the secret key K_{BT} and gets $|AT(S)\rangle$. Then, Bob decrypts the states $|AT(S)\rangle$ with K_{AB} and gets $QFT(|I_i\rangle)$ states. Bob applies QFT^{-1} and measures the $|I_i\rangle$ states as the stage of image retrieving in [5] and saves the results as $\tilde{I}$.

(ii) Bob decrypts $|A(S)\rangle$ by using secret key K_{AB} and obtains $|A(Q)\rangle$.

(iii) Bob asks to blind Trent for permutation. Then, blind Trent sends $|P_B\rangle$ to Bob via quantum channel. Bob decrypts $|P_B\rangle$, makes measurement and obtains P. Bob reorder $|A(Q)\rangle$ states with permutation of blind Trent and obtains $QFT(|I_i\rangle)$.

$$QFT(|I_i\rangle) = SWAP(P(i))(|A(Q)\rangle) \quad i = 0...N-1 \tag{17}$$

(iv) Bob applies QFT^{-1} and gets $|I_i\rangle$, then makes measurement onto that states as stage of the image retrieving in [5] and obtains $\bar{I}$. Bob checks equality of $\tilde{I}$ and $\bar{I}$. If $\tilde{I} = \bar{I}$, Bob will announce that the signature is valid, otherwise the signature is rejected and the protocol is aborted. If the image is valid, then Bob encrypts the valid image I with encryption algorithm.

$$|BT(S)\rangle = E_{K_{BT}}(|I_i\rangle) \tag{18}$$

Then Bob sends $|BT(S)\rangle$ to blind Trent.

(v) Blind Trent decrypts $|BT(S)\rangle$ with secret key K_{BT} and measures the states as the stage of image retrieving in [5] and obtains $\bar{I}$.

(vi) Blind Trent also asks Alice for sending I to him. Alice encrypts the valid image I with encryption algorithm.

$$|AT(S)\rangle = E_{K_{AT}}(|I_i\rangle) \tag{19}$$

Then Alice sends $|AT(S)\rangle$ to blind Trent.

(vii) Trent decrypts $|AT(S)\rangle$ with secret key K_{AT} and measures the states as the stage of image retrieving in [5] and obtains $\tilde{I}$. Blind Trent checks the equality of the $\tilde{I}$ and $\bar{I}$. If they are equal then stores the image I with Alice's identification for later traceability.

4. Security Analysis

Main requirements of the quantum digital signature protocols to provide unconditionally security are that the signature should not be repudiated by the signatory, and any attacker cannot forgery signatory's signature.

4.1. Impossibility of Forgery

Firstly, we consider insider attacker for the protocol. We assume that Bob is illegal participant and wants to create a signature of Alice. Even if Bob knows the details of the signature protocol he cannot create Alice's signature because of blind Trent. Bob cannot create Alice's signature without knowledge of blind Trent. After the end of the legal signature protocol, Bob may change correct image I to $\bar{I}$. Because of the knowledge about correct I of blind Trent, Bob cannot achieve forgery.

Secondly, any attacker may try to forge Alice's signature. Any attacker cannot achieve forgery because the states in the results of the $QFT(|I_i\rangle)$ can be reordered with blind Trent's permutation to produce a correct signature of Alice. Even if any attacker can get the permutation, the permutation will be changed by blind Trent for every signature session. Blind Trent must be part of the protocol. So any attacker cannot achieve collective forgery. Further, any attacker may change $QFT(|I_i\rangle)$ state by applying unitary transformation. Then, Bob and blind Trent can decide changed state by comparing I and $\bar{I}$.

4.2. Impossibility of Repudiation

In the protocol, Alice and Bob cannot repudiate the signature because of the management of protocol by blind Trent. Blind Trent controls some communication steps of the protocol. If Alice can send different $|\tilde{I}\rangle$ to the blind Trent and claim that the signature is not mine. Blind Trent can check the equality of the $|\tilde{I}\rangle$ from Alice and $|\bar{I}\rangle$ from Bob. Blind Trent can decide whether the signature protocol is valid or not.

5. Conclusion

Security of NEQR Quantum Image by Using Quantum Fourier Transform with Blind Trent is suggested. Alice expresses the image $|I\rangle$ into phase-space by using QFT. So the image $|I\rangle$ is expressed in phases of the output qubits of QFT. This improves the image security. Alice changes order of the output qubits of the QFT according to permutation information which is sent by blind Trent. So any attacker does not know order of the qubits and also they cannot create a valid signature.

In the encrypting algorithm, the length of keys is increased to the 8-bit to improve the security. Any information (classical or quantum) in the protocol is sent by using encryption algorithm which is robust against forgery by insider/outsider attacker. Furthermore, decoy states can be used to be aware of Eve.

Bob can verify validity of the signature by the help of the blind Trent. Blind Trent must send the

order of the qubits to the Bob to obtain real message $|I\rangle$ by using QFT^{-1}.

The above security analysis implies that given protocol based on QFT provides unconditionally security. In addition, our protocol provides higher efficiency, effective secret key usage and security for the transfer of NEQR images.

References

[1] S. Venegas-Andraca and S. Bose, "Storing, processing, and retrieving an image using quantum mechanics," *Proceedings of SPIE Conference of Quantum Information and Computation*, vol. 5105, pp. 134–147, 2003.

[2] J. I. Latorre, "Image compression and entanglement," *eprint arXiv:quant-ph/0510031*, 2005.

[3] P. Q. Le, F. Dong, and K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," *Quantum Information Processing*, vol. 10, no. 1, pp. 63–84, 2011. [Online]. Available: https://doi.org/10.1007/s11128-010-0177-y

[4] B. Sun, A. Iliyasu, F. Yan, and K. Hirota, "An rgb multi-channel representation for images on quantum computers," *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol. 17, no. 3, pp. 404–417, 2013.

[5] Y. Zhang, K. Lu, Y. Gao, and M. Wang, "Neqr: a novel enhanced quantum representation of digital images," *Quantum Inf Process*, vol. 12, pp. 2833–2860, 2013. [Online]. Available: https://doi.org/10.1007/s11128-013-0567-z

[6] Y. Zhang, K. Lu, Y. Gao, and K. Xu, "A novel quantum representation for log-polar images," *Quantum Information Processing*, vol. 12, no. 9, pp. 3103–3126, 2013. [Online]. Available: https://doi.org/10.1007/s11128-013-0587-8

[7] S. Yuan, X. Mao, Y. Xue, L. Chen, Q. Xiong, and A. Compare, "Sqr: a simple quantum representation of infrared images," *Quantum Information Processing*, vol. 13, no. 6, pp. 1353–1379, 2014. [Online]. Available: https://doi.org/10.1007/s11128-014-0733-y

[8] H.-S. Li, Z. Qingxin, S. Lan, C.-Y. Shen, R. Zhou, and J. Mo, "Image storage, retrieval, compression and segmentation in a quantum system," *Quantum Information Processing*, vol. 12, no. 6, pp. 2269–2290, 2013. [Online]. Available: https://doi.org/10.1007/s11128-012-0521-5

[9] H.-S. Li, Q. Zhu, R.-G. Zhou, L. Song, and X.-j. Yang, "Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state," *Quantum Information Processing*, vol. 13, no. 4, pp. 991–1011, 2014. [Online]. Available: https://doi.org/10.1007/s11128-013-0705-7

[10] M. Abdolmaleky, M. Naseri, J. Batle, A. Farouk, and L.-H. Gong, "Red-green-blue multi-channel quantum representation of digital images," *International Journal for Light and Electron Optics*, vol. 128, no. 1, pp. 121–132, 2017. [Online]. Available: https://doi.org/10.1016/j.ijleo.2016.09.123

[11] A. Iliyasu, P. Le, F. Dong, and K. Hirota, "Restricted geometric transformations and their applications for quantum image watermarking and authentication," *Proceeding of the 10th Asian Conference on Quantum Information Sciences*, pp. 96–97, 2010.

[12] A. M. Iliyasu, P. Q. Le, F. Dong, and K. Hirota, "Watermarking and authentication of quantum images based on restricted geometric transformations," *Information Sciences*, vol. 186, no. 1, pp. 126 – 149, 2012. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0020025511004853

[13] A. Iliyasu, P. Le, F. Yan, B. Sun, J. A. S. Garcia, F. Dong, and K. Hirota, "A two-tier scheme for greyscale quantum image watermarking and recovery," *Int. J. Innov. Comput. Appl.*, vol. 5, no. 2, pp. 85–101, 2013. [Online]. Available: http://dx.doi.org/10.1504/IJICA.2013.053179

[14] F. Yan, A. Iliyasu, B. Sun, S. Venegas-Andraca, F. Dong, and K. Hirota, "A duple watermarking strategy for multi-channel quantum images," *Quantum Inf. Process*, vol. 14, no. 5, pp. 1675–1692, 2015.

[15] M. A. Nielsen and I. L. Chuang, "Quantum computation and quantum information," *10th Anniversary Edition, Cambridge University Press*, 2010.

[16] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, vol. 175, no. 6, pp. 661–663, 1984.

[17] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, p. 8, 1991. [Online]. Available: https://doi.org/10.1103/PhysRevLett.67.661

[18] I. Yılmaz, "Quantum group proxy digital signature based on quantum fourier transform by using blinded and non blinded trent," *International Journal of Information Security Science*, vol. 6, no. 4, pp. 79 – 86, 2017.

[19] T. Kim, J. W. Choi, N. S. Jho, and S. Lee, "Quantum messages with signatures forgeable in arbitrated quantum signature schemes," *Physica Scripta*, vol. 90, no. 2, p. 025101, 2015. [Online]. Available: http://stacks.iop.org/1402-4896/90/i=2/a=025101

[20] W. Zhang, D. Qiu, and X. Zou, "Improvement of a quantum broadcasting multiple blind signature scheme based on quantum teleportation," *Quantum Information Processing*, vol. 15, no. 6, pp. 2499–2519, 2016. [Online]. Available: https://doi.org/10.1007/s11128-016-1289-9