Scientific Research Publishing

International Journal of Intelligence Science, 2018, 8, 75-87
http://www.scirp.org/journal/ijis
ISSN Online: 2163-0356
ISSN Print: 2163-0283

An Image Encryption Method Based on Quantum Fourier Transformation

Ying Liu[1], Bing Zhou[2], Zijing Li[3], Jiangnan Deng[4], Zhengying Cai[3*]

[1]School of Foreign Language, China Three Gorges University, Yichang, China
[2]College of Materials and Chemical Engineering, China Three Gorges University, Yichang, China
[3]College of Computer and Information Technology, China Three Gorges University, Yichang, China
[4]School of Law and Public Administration, China Three Gorges University, Yichang, China
Email: 1311264797@qq.com, 1050015785 @qq.com, 1483613822@qq.com, 1394720486@qq.com, master_cai@163.com

How to cite this paper: Liu, Y., Zhou, B., Li, Z.J., Deng, J.N. and Cai, Z.Y. (2018) An Image Encryption Method Based on Quantum Fourier Transformation. *International Journal of Intelligence Science*, **8**, 75-87.
https://doi.org/10.4236/ijis.2018.83004

Received: February 1, 2018
Accepted: July 27, 2018
Published: July 30, 2018

Abstract

The image security problem is an important area in information security, and image encryption plays a vital role in this day. To protect the image encryption from the attack of quantum algorithm appeared recently, an image encryption method based on quantum Fourier transformation is proposed here. First, the image encryption and Fourier transformation are discussed here, then a encryption function is proposed. Second, a quantum Fourier transformation is introduced to quantum encryption, and the full step of quantum encryption is given as well. Third, the security of the proposed quantum encryption if analyzed, and some propositions are also presented. Lastly, some conclusions are indicated and some possible directions are also listed.

Keywords

Image Encryption, Quantum Encryption, Quantum Fourier Transformation, Quantum Image

1. Introduction

1.1. Related Work

Image encryption technology won great attention recently because of its complexity. [1] adopted a novel chaotic block image encryption algorithm based on dynamic random growth technique. [2] extended a 2D Sine Logistic modulation map for image encryption. [3] gave a new image encryption algorithm based on non-adjacent coupled map lattices. [4] considered a novel chaotic image encryption scheme using DNA sequence operations. [5] concerned an image encryp-

*Referring author.

tion scheme based on elliptic curve pseudo random and Advanced Encryption System.

Image encryption method often includes space encryption and condenses encryption. [6] built a color image encryption based on chaotic systems and elliptic curve ElGamal scheme. [7] studied an optical double-image encryption and authentication by sparse representation. [8] offered a N-phase logistic chaotic sequence and its application for image encryption. [9] implied an impulsive synchronization of reaction-diffusion neural networks with mixed delays and its application to image encryption.

However, the appearance of quantum computing brought a great challenge to classic encryption methods. At the same time, quantum encryption also gives us an absolutely secure encryption method. For example, [10] painted a quantum image encryption based on iterative framework of Frequency-Spatial Domain transforms. [11] displayed a quantum color image encryption algorithm based on a hyper-chaotic system and quantum Fourier transform. [12] discussed the research on an E-mail encryption protocol based on quantum teleportation. [13] featured a quantum image encryption algorithm based on quantum image XOR operations. [14] stated that encryption faces quantum foe. [15] put forward a quantum image encryption based on generalized Arnold transform and double random-phase encoding.

In quantum image encryption, the efficiency of transformation plays an important role, especially the Fourier transformation [11]. [16] discussed the change from fractional Fourier transformation to quantum mechanical fractional squeezing transformation. This paper tried to introduce an efficient quantum Fourier transformation in image encryption to improve the encryption security and efficiency.

1.2. Organization of the Article

Section 2 defines the general notion of privacy for quantum key distribution. Section 3 contains preliminaries, basic rules and the general model used to analyze the protocol. In Section 4, the protocol is described. Section 5 contains the analysis of privacy protection.

2. Image Security and Image Encryption

2.1. Fourier Transformation in Image Encryption

Through bringing the ideal into this work from PD_γ a brilliant estimation of this Fourier transform of PD_γ is required, which denoted by $\eta_{1/r}$. It might be illustrated that since $1/r \ll \tau_1\left(D^*\right)$ one has the estimation

$$\eta_{1/r}(x) \approx \exp\left(-\pi\left(r \cdot \operatorname{dist}\left(D^*, x\right)\right)^2\right) \tag{1}$$

Therefore, $\eta_{1/r}(x) \approx 1$ for any $\chi \in D^*$ (as a matter of fact a par holds) as well as one avoids D^*, its value drop off. For the dot not far from distance, for example, $1/r$ from this fretwork, its significance is still a little positive constant

(approximately $\exp(-\pi)$). As the length from D^* increases, the significance of the purpose quickly changes into triffling. Because the length between any two matrixes in D^* is at any rate $\tau_1(D^*) \gg 1/r$, the normal distribution around each point of D^* are well fell apart.

Let us begin to try to comprehend what the distinguishing difference $P_{D/p,r/p}$ looks like. Point out that this image matrix D/p compound of $p^{\in}$ translates of the primal image matrix D that's to say, as for each $a \in O_p^{\in}$, consider the set

$$D + Da/p = \left\{ Db/p \,|\, b \in O^{\in}, b \bmod p = a \right\} \tag{2}$$

Then, $\left\{ D + Da/p \,|\, a \in O_P^{\in} O \right\}$ establishes a division of D/p. what's more, it could be depicted that since r/p is bigger than the system parameter $\eta \in (D)$, the possibility distributed to each $D + D_{a/p}$ under $P_{D/p,r/p}$ is fundamentally alike, that is, $p^{-\in}$. Intuitively, in addition to system parameter, the normal measure not any more "sees" the discerning construction of D, so distinguished from others, it is not influenced by translations.

It guided us to think about the next dispersion, name it P. A example from P is a pair (a, y) from which y is sampled $P_{D/p,r/p}$, and $a \in O_p^{\in}$ is such that $y \in D + D_{a/p}$.

Now the Fourier transform of $P_D + D_{a/p,r/p}$ is presently analyzed. When "a" is zero, the Fourier transform is known as $f_{p/r}$. For universal a, a stock calculation illustrated that the Fourier transform of $P_D + D_{a/p,r/p}$ is granted by

$$\exp\left(2\pi i \left\langle a, T(x) \right\rangle / p\right) \cdot \eta_{p/r}(x) \tag{3}$$

where $T(x) \in O_p$ is outlined as

$$T(x) = \left(D^*\right)^{-1} kD^*(\chi) \bmod p,$$

and $kp^*(\chi)$ gives the only hide vector in D^* to χ. Put differently, $T(x)$ is the vector of constant number of the vector in D^* hide to x when laid out in the foundation of D^*, shrink possibility p. therefore seeing that the Fourier transform $P_D + D_{a/p,r/p}$ is basically $f_{p/r}$, besides that each "hill" has its unique phase as a support for the vector of constant number of the image matrix dot in its center. The visual aspect of those phases is as a termination of a famous dimension of the Fourier transform, given that translation is transmuted with phase to multiplication.

For two real numbers x and $y > 0$, *generally*, x mod y can be defined as $\chi / y \,|\, y$ for $\chi \in R$, $\lfloor \chi \rfloor$ is defined as the integer closest to x or, in case of existing two such integers, the small one of the two. For any integer $p \geq 2$, O_p is written for the cyclic group $\left\{0, 1, p^{-1}\right\}$ with addition possibility p.

As two possibility density functions λ_1, λ_2 on $R^{\in}$, the *statistical length* between them is defined as

$$\Delta(\lambda_1, \lambda_2) = \int_{R^{\in}} \left| \lambda_1(x) - \lambda_2(x) \right| \mathrm{d}x \tag{4}$$

(as this definition observing, the statistical length ranges in $[0, 2]$. A allied definition can be showed for sensible random variables. The statistical length satis-

fies the triangle inequality, it's to say, for any, $\lambda_1, \lambda_2, \lambda_3$

$$\Delta(\lambda_1, \lambda_3) \le \Delta(\lambda_1, \lambda_2) + \Delta(\lambda_2, \lambda_3) \tag{5}$$

Another significant fact is that the statistical length cannot increase by using a possibility function *f*, that's to say,

$$\Delta(\eta(X), \eta(Y)) \le \Delta(X, Y) \tag{6}$$

Retrieve that the *normal distribution* with variance a^2 and mean 0 is the distribution on R illustrated by the density function $\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-1/2\left(\frac{x}{\sigma}\right)^2\right)$ where exp(*y*) denotes e^y. Also see from that the summary of two mean = 0 independent variables with variances σ_1^2 and σ_2^2 is also a normal variable. A vector x and any $\omega > 0$, let

$$Q_w(x) := \exp\left(-\pi \|x/w\|^2\right) \tag{7}$$

be a normal function measured by a component of *s*. *if* denoted *M*1 by *p*. Note that $\int_{R^\in} Q_\omega(x)\mathrm{d}x = \omega^\in$ Therefore,

$$s_\omega := Q_\omega / \omega^\in \tag{8}$$

is an n-dimensional chance density function and like what have mentioned above, if apply *s* to denote s_1. Functions are expended to sets in the normal way; that's to say, $Q_s(A) = \sum_{x\in A} Q_\omega(x)$ for any countable matrix *A*. For any vector $c \in R^\in$, if defined Q_ω, $c(\chi) = Q_\omega(\chi - C)$ to be a shifted version of Q_ω. The next example bounds the sum by which $Q_\delta(\chi)$ can deduce by a little change in χ.

For all $\omega, t, l > 0$ *and* $\chi, y \in R^\in$ *with* $\|\chi\| \le t$ *and* $\|\chi - y\| \le 1$,

$$Q_w(y) \ge \left(1 - \pi\left(2lt + l^2\right)/w^2\right) Q_\omega(x)$$

Using the inequality $\mathrm{e}^{-z} \ge 1 - z$,

$$Q_w(y) = \mathrm{e}^{-\pi\left\|\frac{y}{w}\right\|^2} \ge \mathrm{e}^{-\pi\left(\frac{\|x\|}{w}+\frac{1}{w}\right)^2} = \mathrm{e}^{-\pi\left(2l\frac{\|x\|}{w^2}+\left(\frac{1}{w}\right)^2\right)Q_w(x)} \ge \left(1 - \pi\left(2lt + l^2\right)/w^2\right) Q_\omega(x) \tag{9}$$

2.2. The Encryption Function

As the option of basis is obvious, if write $M(D)$ instead of $M(s_1, \cdots, s_\in)$. For a point $\chi \in R^\in$, $\chi \bmod M(D)$ is defined as the only point $y \in M(D)$ such that $y - x \in D$. if denote by $\det(D)$ the volume of the primal parallelepiped of *D* or equivalently, the determinant' absolute value of the matrix with the basis image matrixes of matrix ($\det(D)$ is an image matrix invariant, to be exactly, it is free from the option of basis). The *double* of a image matrix *D* in $R^\in$, denoted D^*, is the image matrix illustrated by the set of all matrixes $y \in R^\in$ such that $\langle x, y\rangle \in 0$ for all matrixes $x \in D$. In the same way, given a basis $(s_1, \cdots, s_\in)$ of an image matrix, define the double basis as the vector set $(s_1^*, \cdots, s_\in^*)$ such that $\langle s_i\, s_j^*\rangle = \delta_{ij}$ for all $ij \in [\in]$ where ω_{ij} denotes the weight delta, in another word, 1 if $i = j$ and 0 other than. With a little abuse of

notation, people often use D for the $\epsilon\ x\ \epsilon$ matrix whose columns are $s_1, \cdots, s_n$. With this notation, find that $D^* = \left(D^{\mathrm{T}}\right)^{-1}$. Because of that, it shows that $\det\left(D^*\right) = 1/\det\left(D\right)$. At another case, for a point $s \in D$, $D^{-1}s$ is written to illuminate the integer coefficient vector of s.

Because of the iterative step, the algorithm can be expressed as follows. Allow r_i denote $r \cdot \left(\alpha p/\sqrt{\in}\right)^i$ The algorithm begin with producing $\in^c$ samples from $P_{D\gamma 3\in}$ On account of $r3 \in$ is indeed large, this samples can be computed expeditiously by a unproblematic procedure. The next comes the most essential part of the algorithm: for $i = 3 \in, 3 \in -1, \cdots\ 1$ the algorithm applies $ts \in^c$ samples from $P_{D,r'}$ to produce $\in^c$ samples from $P_{D,r_{i-1}}$ by naming the iterative step $\in^c$ times. Finally, it ends up with $\in^c$ samples from $P_{D,r_0} = P_{D,r}$ as well as people finish the algorithm by uncomplicated outputting the initial of them. Note the next essential answer: applying $\in^c$ samples from P_{D,r_i}, there will have the ability to bring forth the same number of samples $\in^c$ from $P_{D,r_{i-1}}$ (actually, people could even give forth more than $\in^c$ examples). The algorithm would not operate if only generate, in another word, $\in^c/2$ samples.

Now eventually get to depict the iterative step by us. Retrieve that as input the $\in$ samples from $P_{D,r}$ and there will be supposed to give forth a sample from $P_{D,r'}$, where $r^1 = r\sqrt{\in}/(ap)$. What's more, r is knowable and assured to be at least $\sqrt{2}Pf_q\left(D\right)$, which can be illustrated to illuminate that $p/r < \tau_1\left(D^*\right)/2$. From what have illustrated in the former passage, the exact lower related to r does not count much for this summary; it's adequate to remember that r is adequately larger than (D), and that $1/r$ is adequately smaller than $\tau_1\left(D^*\right)$

The algorithm composed of two primary parts. In that passage, there will be described as a classical algorithm that applying W and the samples from $P_{D,r}$, solve $\mathrm{CVP}_{D^*,\alpha p/(\sqrt{2}r)}$. There, what illustrate a *encryption* algorithm is that, showed an oracle that solves $\mathrm{CVP}_{D^*,\alpha p/(\sqrt{2}r)}$, outputs a example from $P_{D,r\sqrt{\in}/(\alpha p)}$. This is the unique *encryption* element in this essay. People find that the condition is content since $\left(\sqrt{2}\,r\right) \le 1/f_q\left(D\right) \le \tau_1\left(D^*\right)/2$

3. Quantum Fourier Transformation for Encryption

3.1. A Fast Quantum Fourier Transformation

In a fast quantum Fourier transformation, the first aim is to produce a quantum announcement in relate to $\eta_{1/r}$. with formality, it could be described as

$$\sum_{x \in R^{\in}} \eta_{1/r} \left|x\right\rangle \tag{10}$$

Taking account of some possibility distribution P on some image matrix D and its Fourier transform $f : R^{\in} \to C$, defined as

$$\eta\left(x\right) = \sum_{y \in D} P\left(y\right) \exp\left(2\pi i \left\langle x, y\right\rangle\right) = \underset{y \sim P}{Exp}\left[\exp\left(2\pi i \left\langle x, y\right\rangle\right)\right] \tag{11}$$

where in the second equality. the sum is simply be rewrote as an expectation. By definition, η is D^*-periodic, that's to say, $\eta\left(x\right) = \eta\left(x + y\right)$ for any $\chi \in R^{\in}$ and $y \in D^*$ It can compute an estimation of η to within $\pm 1/\mathrm{poly}\left(\in\right)$. If

$y_1,\cdots,y_N$ are $N=\text{poly}(\in)$ independent samples from *P*, and then

$$f(x)\approx\frac{1}{N}\sum_{j=1}^{N}\exp\left(2\pi i\left\langle x,y_j\right\rangle\right) \tag{12}$$

where the estimation is to within $\pm 1/\text{poly}(n)$ and poses with possibility exponentially just about 1, presuming that *N* is a large adequate multinomial.

Let $q=q(\in)$ *be a negligible function*, $p=p(\in)\geq 2$ *be an integer*, *and* $a=a(\in)\in(0,1)$ *be a real number. presume that way to an oracle W that solves quantum oracle*, *given a multinomial number of examples*. *A*s for an ϵ-dimensional image matrix *D*, some $0<d<\tau_1(D)/2$, and an integer $p\geq 2$, there is an algorithm solves $\text{CVP}_{D,d}^{(p)}$ if, depicted any point $x\in R^{\in}$ within distance *d* of *D*, it outputs $D^{-1}k_1(x)\bmod p\in O_P \mod p\in O_P$, the coefficient matrix to *x* deduced possibility *p*. Here shows a reduction from $\text{CVP}_{D,d}$ to $\text{CVP}_{D,d}^{(p)}$.

There is an effective algorithm for given a image matrix D, *a number* $d<\tau_1(D)/2$ *and an integer* $p\geq 2$, *solves* $\text{CVP}_{D,d}$ *given way to an oracle for* $\text{CVP}_{D,d}^{(p)}$.

The input is a point *x* in distance *d* of *D*. A sequence of points is defined as $\chi_1,\chi_2,\chi_3,\cdots$ as follows. Let $a_i=D^{-1}K_D(\chi_i)\in O^{\in}$ be the coefficient image matrix point to x_i. Define. Find that the closest image matrix point to $\chi_{i+1}=\left(x_i-D(a_i \bmod p)\right)/p\in D$ therefore $a_{i+1}=\left(a_i-a(a_i \bmod p)\right)/p$ what's more, the length of x_{i+1} from *D* is at most d/p^i. as well as depicted that this sequence can be computed by applying the oracle.

After $\in$ steps, there is a point $x_{\epsilon+1}$ whose length to the image matrix is at most $d/p^{\in}$. An algorithm is applied for solving the closest matrix. This outputs a image matrix point *Da* within distance $2^{\epsilon}\cdot d/p^{\epsilon}\leq d<\tau_1(D)/2$ of $\chi_{\epsilon+1}$. Therefore, *Da* is the image matrix point closest to $\chi_{\epsilon+1}$ and one tried to retrieve $a_{\epsilon+1}=a$ realizing and $a_{\in} \bmod p$ (by applying the oracle), one can recover $a_{\in}=pa_{\epsilon+1}+(a_{\in} \bmod p)$. proceeding this process, one could recover $a_{\epsilon-1},a_{\epsilon-2},\cdots,a_1$. This finishes the algorithm for Da_1 is the closest point to $x_1=x$

As the option of *r*, ($\alpha p\left(\sqrt{2}r\right)<\tau_1\left(D^*\right)/2$ it's adequate to depict an efficient algorithm for $\text{CVP}_{D^*,\alpha p/(\sqrt{2}r)}^{(p)}$. By combining the discussion above this could be done. Initially, it depicts an algorithm *W'* that, showed samples from A_{s,ψ_β}. The next, it is described how to use *W'* and the shown samples from $P_{D\gamma}$ in order to solve $\text{CVP}_{D^*,\alpha p/(\sqrt{2}r)}^{(p)}$

3.2. Quantum Encryption Step

Repeating the process illustrated above $\in$ times, the system state is described as an $\in$-fold tensor product of the state in Equation (12), which might be understood as

$$\sum_{x\in\left\{-\sqrt{\in}r,\cdots,\sqrt{\in}r\right\}^{\in}}Q_{\sqrt{2}r}(x)\left|x\right\rangle \tag{13}$$

For $O^{\in}\cap\sqrt{\in}r\eta_{\in},\left\{-\sqrt{\in}r,\cdots,\sqrt{\in}r\right\}^{\in}$ it indicates that the state is within l_2 distance $2^{-\Omega(\in)}$ of

$$\sum_{x\in Z^{\in}} \in Q_{\sqrt{2}r}(x)\left|x\right\rangle \tag{14}$$

Therefore, for the goal it can be presumed that it is generated the state in Equation (14).

The next step, applying the LLL foundation reduction algorithm, a base can be acquired for D of length at most $2^{\in}\tau_{\in}(D)$ and let $M(D)$ be brought forth by a new register $M(D)$ Let $y \in M(D)$ denote the state that $\|y\| \le diam(M(D)) < \in 2^{\in}\tau_{\in}(D)$. The state acquired by us after the measurement is

$$\sum_{x\in L+y} Q_{\sqrt{2}r}(x)\left|x\right\rangle \tag{15}$$

In the end, subtract y from the register, and get

$$\sum_{x\in L} Q_{\sqrt{2}r}(x+y)\left|x\right\rangle \tag{16}$$

Therefore assume any $x \in D$ with $\|X\| \le \sqrt{\in}r$. The amplitude squared offered to it in Equation (13) is $Q_r(X)/M_r(D)$ By The denominator is $Q_{\cdot}(D) = \det(D^*)\cdot r^{\in} Q_{1/r}(D^*) \ge \det(D^*)\cdot r^{\in}$ and therefore the amplitude is at most $Q_r(x)/\left(\det(D^*)\cdot r^{\in}\right) = \det(D)s_y(x)$

In another word, the amplitude squared provided to x by the process is $Q_r(X+y)/Q_y(D+y)$. Then the denominator is

$$Q_r(D+y) = \det(D^*)\cdot r^{\in}\sum_{z\in D^*} e^{2\pi i\langle z,y\rangle} Q_{\frac{1}{r}}(z) \le \left(1+2^{-\Omega(\in)}\right)\det(D^*)\cdot r^{\in} \tag{17}$$

To get this inequality, initially observe that by the simple part, $\tau_1(D) \ge 1/\tau_{\in}(D) > \sqrt{\in}/r$, and then apply quantum Fourier transformation. what's more, the numerator is in $\left(1-2^{-\Omega(\in)}\right)Q_y(x)$. Therefore, the amplitude squared provided to x is in $\left(1-2^{-\Omega(\in)}\right)Q_y(x)\det(D)s_r(x)$

The l_2 distance between different states r to

$$\left|s_1\right\rangle = \sum_{x\in\frac{D}{R},\|x\|<\sqrt{\in}} Q(x)\left|x \bmod M(D)\right\rangle, \text{ and}$$

$$\left|s_2\right\rangle = \sum_{x\in\frac{D}{R}} Q(x)\left|x \bmod M(D)\right\rangle = \sum_{x\in\frac{D}{R}\cap M(D)}\sum_{y\in D} Q(x-y)\left|x \bmod M(D)\right\rangle$$

is $2^{-\Omega(\in)}$.

here, consider $\left|s_1\right\rangle$ and $\left|s_2\right\rangle$ as matrixes in $R^{\in}$-dimensional space. Make Z be the l_2 norm of $\left|s_1\right\rangle$. In the next it can be shown that the l_2 length between $\left|s_1\right\rangle$ and $\left|s_2\right\rangle$ is at most $2^{-\Omega(\in)}$ Z. it is adequate to build that the l_2 distance between different states referring to $\left|s_1\right\rangle$ and $\left|s_2\right\rangle$ is exponentially tiny.

Initially, get a good approximation of Z. As far as $\tau_1(D) > 2\sqrt{\in}$, each key in the definition of $\left|s_1\right\rangle$, and so

$$Z = \sum_{x\in\frac{D}{R},\|X\|<\sqrt{\in}} Q(x)^2 = q\left(\sqrt{2}D/R \cap \sqrt{2\in}\eta_{\in}\right) \tag{18}$$

By applying the image matrix s_2"D/R, get that

$$\left(1-2^{-2\in}\right)Q\left(\frac{\sqrt{2}D}{R}\right) \le Z \le Q\left(\sqrt{2}D/R\right) \tag{19}$$

It is verified with an upper relate to the l_2 distance between the two matrixes. Applying the normal monotonicity of s,

$$\begin{aligned}
&\left\| s_1\right\rangle-\left| s_2\right\rangle\Big|_2 \le \left\| s_1\right\rangle-\left| s_2\right\rangle\Big|_1 \\
&=\sum_{x\in\frac{D}{R},\|x\|\ge\sqrt{\epsilon}} Q(x) \\
&\le 2^{-2\epsilon} Q\left(D/R\right) \\
&\le 2^{-2\epsilon}2^{\epsilon/2} Q\left(\sqrt{2}\,D/R\right) \\
&\le 2^{-\epsilon} Q\left(\sqrt{2}D/R\right)
\end{aligned} \tag{20}$$

There will be an effective quantum algorithm that, offered any n-dimensional image matrix D, a number $d<\tau_1\left(D^*\right)/2$, *and an oracle that handles* CVP_{D^*d}, *outputs a sample from* $P_{D,\epsilon/\sqrt{2}d}$.

By scaling, presume without decline in amount of generality that $d=\sqrt{\epsilon}$. Let $R\ge 2^{3\epsilon}\tau_\epsilon\left(D^*\right)$ be a big adequate integer, presume that log R is multinomial in the image matrix D. The initial task is to build a state exponentially near to

$$\sum_{x\in\frac{D^*}{R}\cap M(D)}\sum_{y\in D} Q(x-y)\left|x\right\rangle \tag{21}$$

As a state on $\in$ log R qubits, that is a multinomial number in the input scale. In order to do in this way, initially, it is used with $r=1/\sqrt{2}$ and the image matrix D^*/R to make the state

$$\sum_{x\in\frac{D^*}{R}} Q(x)\left|x\right) \tag{22}$$

Then, this is exponentially relate to

$$\sum_{x\in\frac{D^*}{R},\|x\|<\sqrt{\epsilon}} Q(x)\left|x\right) \tag{23}$$

An then, calculate x mod $M(D^*)$ in a new register and get

$$\sum_{x\in\frac{D^*}{R},\|x\|<\sqrt{\epsilon}} Q(x)\left|x,x \bmod M\left(D^*\right)\right) \tag{24}$$

applying the CVP oracle, recover x from x mod $M(D^*)$. This admits us to uncompute the primal register and get

$$\sum_{x\in\frac{D^*}{R},\|x\|<\sqrt{\epsilon}} Q(x)\left|x \bmod M\left(D^*\right)\right) \tag{25}$$

Then, this state is exponentially close to the recommended state (25).

In the next step, apply the quantum Fourier transform. To begin with, applying the mapping between $D^*/RR\cap M\left(D^*\right)$ and O_p^ϵ, rewrite (25) as

$$\sum_{\omega\in O_R^\epsilon}\sum_{r\in O^\epsilon} Q\left(\frac{D^*\omega}{R}-D^*r\right)\left|\omega\right\rangle \tag{26}$$

Then apply the quantum Fourier transform on O_p^ϵ. get a state where the amplitude of t for te, ZR is proportional to

$$\begin{aligned}
\sum_{\omega\in O_R^\epsilon}\sum_{r\in O^\epsilon} Q\left(\frac{D^*S}{R}-D^*r\right)\exp\left(2\pi i\left\langle\omega,t\right\rangle/R\right) &= \sum_{\omega\in O_R^\epsilon} Q\frac{D^*\omega}{R}\exp\left(2\pi i\left\langle\omega,t\right\rangle/R\right) \\
&= \sum_{\omega\in D^*/R} Q(x)\exp\left(2\pi i\left(D^*\right)^{-1}x,t\right) \\
&= \sum_{x\in D^*/R} Q(x)\exp\left(2\pi i\left\langle x,Dt\right\rangle\right) \\
&= \det(RD)\sum_{Y\in RD} Q\left(y-Dt\right)
\end{aligned} \tag{27}$$

where the last equality follows from Equation (26). Therefore, the crucial state can be fairly written as

$$\sum_{x\in M(D)\cap D}\sum_{y\in RD}Q(y-x)|x\rangle \tag{28}$$

Look at that $\tau_1(RD)=R\tau_1(D^*)\geq 2^{\Im\in}$ Therefore, according to the image matrix *RD*, and get that this state is exponentially close to

$$\sum_{x\in D,\|x\|<\sqrt{\in}}Q(x)\big|x \bmod M(RD)\big\rangle \tag{29}$$

Quantify this state and get *x* mod $M(RD)$ for some vector *x* with $\|X\|<\sqrt{\in}$. Since *x* mod $M(RD)$ is within $\sqrt{\in}$ of the image matrix *RD*, and $\tau_1(RD)\geq 2^{\Im\in}$, recuperate *x* by using. The answer of the algorithm is *x*.

Presume without deprivation of generalization that the vector $(1,0,\cdots,0)$ is or thogonal to *H*. There is,

$$\begin{aligned}
&\underset{X\sim P_{D,r}}{Exp}\left[\exp\left(-\pi(x_1/r)^2\right)\right]\\
&=\frac{1}{Q_r(D)}\sum_{x\in L}\exp\left(-\pi\left(\sqrt{2}x_1/r\right)^2\right)\exp\left(-\pi\left(\sqrt{2}x_2/r\right)^2\right)\cdots\exp\left(-\pi\left(\sqrt{2}x_{\in}/r\right)^2\right)\\
&=\frac{\det(D^*)r^{\in}}{Q_r(D)}\sum_{y\in L^*}\exp\left(-\pi(ry_1/r)^2\right)\exp\left(-\pi(ry_2/r)^2\right)\cdots\exp\left(-\pi(ry_{\in}/r)^2\right)\\
&=\frac{\det(D^*)r^{\in}}{\sqrt{2}Q_r(D)}Q_{\sqrt{2}/r}(D^*)=\frac{\det(D^*)r^{\in}}{\sqrt{2}Q_r(D)}(1+q)
\end{aligned} \tag{30}$$

Let be $\in^2$ matrixes chosen by $P_{D,r}$ For $i=1,\cdots,\in$, let B_i be the event that

$$\dim\operatorname{span}\left(x_1,\cdots,x_{(i-1)\in}\right)=\dim\operatorname{span}\left(x_1,\cdots,x_{i\in}\right)<\in.$$

Obviously, if none of the $B'\omega$ takes place, then $\dim\operatorname{span}\left(x_1,\cdots,x_{\in,}\right)=\in$. Therefore, it is necessary to depict that for all *i*, $M_r[B_i]<2^{-\Omega(\in)}$. Indeed, fix some *i* on condition of $x_1,\cdots,x_{(i-1)\in}$ such that $\dim\operatorname{span}\left(x_1,\cdots,x_{(i-1)\in}\right)<\in$. Then the possibility that

$$x_{(i-1)\in+1},\cdots,x_{i\in}\ \dim\operatorname{span}\left(x_1,\cdots,x_{(i-1)\in}\right)$$

is at most $(9/10)^{\in}=2^{-\Omega(\in)}$. This indicated that $M_r[B_i]<2^{-\Omega(\in)}$, as commanded.

4. Security Analysis and Proposition of Quantum Encryption

Let ϵ be the security parameter of encryption system. The encryption system is parameterized by two integers m , p and *a* possibility distribution *x* on O_p. A parameters setting undertakes both safety and right is the next. pick $P>2$ to be some initial number between $\in^2$ and $2\in^2$ make $m=(1+q)(\in+1)\log p$ for some arbitrary constant $q>2$ The chance distribution *x* is selected to be $\psi_{\alpha(\in)}$ for $\alpha(\in)=O\left(1/\sqrt{\in}\log\in\right)$, that's to say, $a(\in)$ is such that $\lim_{\in\to\infty}a(\in)\cdot\sqrt{\in}\log\in=0$. For instance, it can be chosen as $a(\in)=\sqrt{\in}\log\in$. In the next illustration, all additions are operated in O_n, *i.e.*, possibility *p*.—Private key: select $s\in O_p^{\in}$ uniformly randomly. The private key is ω.

—Public Key: for $i=1,\cdots,m$ select *m* matrixes $a_1,\cdots,a_m\in O_P^{\in}$ from the

uniform distribution. Also select elements $e_1,\cdots,e_m \in O_p$ referring to x. The public key is offered by $(a_i,b_i)_{i=1}^m$ where

$$b_i = \langle a_i,\omega\rangle + e_i$$

In case of encryption, first select a random set S uniformly between all 2^m subsets of $[m]$ The encryption is $\left(\sum_{i\in\omega} a_i, \sum_{i\in\omega} b_i\right)$ if the bit is 0 and $\left(\sum_{i\in\omega} a_i, \left\lfloor \frac{p}{2} \right\rfloor, \sum_{i\in\omega} b_i\right)$ if the bit is 1.

In case of decryption, the decryption of a pair (*a*, *b*) is 0 if $b-(a,\omega)$ is closer to 0 than to possibility *p*. whereas, the decryption is 1.

Apparently, the public key size is $\mu(m\in\log p)=\tilde{\mu}(\in^2)$ and the encryption procedure multiplies the scale of a message by a element of $\mu(\in\log p)=\tilde{\mu}(\in)$. As a matter of fact, it is probable to decrease the size of the public key to $\mu(m\in\log p)=\tilde{\mu}(\in)$. Presume all users of the encryption system partake some fixed (and trustworthy) random options of $a_1,\cdots,a_m$ Next, the public key require just made of $b_1,\cdots,b_m$. This tranformation does not influence the safety of the encryption system.

Next, illustrate that under a sure condition on x, m, and p, the possibility of decryption problem is tiny. Latterly, depict that the option of parameters meets this condition. There exists a desire to insert some additional notation. As for a distribution x on O_p and an integer $k\geq 0$, define x^{*k} as the distribution gotten by adding up k, whose addition is operated in O_p (for $k=0$ we define x^{*0} as the distribution that is incessantly 0). For a chance distribution λ on T define f likely. For an component $a\in O_p$, $|a|$ is defined as the integer a if $a\in\left\{0,1,\cdots,\left\lfloor\frac{p}{2}\right\rfloor\right\}$ and as the integer p - a otherwise. Differently, $|a|$ reshowed the distance of a from 0. likely, for $x\in T$, $|x|$ is defined as x for $x\in[0,1/2]$ and as 1 - x other than.

Let a > 0. *Presume that for any* $k\in\{0,1,\cdots,m\}$, *x' meets that*

$$\underset{e\sim x^{*k}}{Mr}\left[|e|<p/2\right]/2>1-\delta \tag{31}$$

Next, the possibility of decryption error will be decreased. In another word, for any bit $c\in\{0,1\}$, *if apply the protocol above to pick private and public keys, encrypt c, and then decrypt the answer, then the final result is c with possibility at least* 1 - δ.

Initially, think about an encryption of 0. It is offered by (*a*, *b*) for $a=\sum_{i\in\omega} a_i$ and

$$b=\sum_{i\in\omega} b_i = e_i + \sum_{i\in\omega}\langle a_i,\omega\rangle = \langle a,\omega\rangle\sum_{i\in\omega} e_i + \langle a,\omega\rangle \tag{32}$$

Therefore, $b-\langle a,\omega\rangle$ is exactly $\sum_{i\in\omega} e_i$, with distribution function $x^{*|\omega|}$. referring to the supposal, $\left|\sum_{i\in\omega} e_i\right|$ is less than $\left\lfloor\frac{p}{2}\right\rfloor/2$ with possibility at least 1 - δ. From the aspect, it is closer to 0 than to $\left\lfloor\frac{p}{2}\right\rfloor$ and hence the decryption is

right.

For the option of parameters it contains that for any $k \in \{0,1,\cdots,m\}$,

$$\underset{e\sim\overline{\Psi}_{\alpha}^{s_k}}{Mr}\left[|e| < p/2\right]/2 > 1-\delta(\in) \tag{33}$$

for some trifling function $\delta(\in)$.

For a selection $g=(g_1,\cdots,g_l)$ of *l* components from *G*, let M_g be the distribution sum of $g_1,\cdots,g_l$, *i.e.*, 1

$$M_g(h)=\frac{1}{2^l}\left\{b\in\{0,1\}^l \mid \sum_i b_i g_i = h\right\} \tag{34}$$

By way of showing that this distribution is near uniform, compute its l_2 norm, and observe that it is very approach to $1/|G|$. From this it will keep up that the distribution must be approach to the distribution function. The l_2 norm of M_g is given by

$$\begin{aligned}\sum_{h\in G} M_g(h)^2 &= \underset{b,b'}{Mr}\left[\sum b_i g_i = \sum b_i' g_i\right] \\ &\le \frac{1}{2^l} + \underset{b,b'}{Mr}\left[\sum b_i g_i = \sum b_i' g_i \mid b\neq b'\right]\end{aligned} \tag{35}$$

In the end, the expected length from the uniform distribution is

$$\begin{aligned}\underset{g}{Exp}\left[\sum_h M_g(h)-\frac{1}{|G|}\right] &\le \underset{g}{Exp}\left[|G|^{\frac{1}{2}}\left(\sum_h\left(M_g(h)-\frac{1}{|G|}\right)^2\right)^{\frac{1}{2}}\right] \\ &\le \sqrt{|G|}\,\underset{g}{Exp}\left[\sum_h\left(M_g(h)^2-\frac{1}{|G|}\right)^{\frac{1}{2}}\right] \le \sqrt{\frac{|G|}{2}}\end{aligned} \tag{36}$$

For $\omega q O_p^{\in}$, let $p_0(\omega)$ be the possibility with input $\left((a_i,b_i)_{:-1}^m,(a,b)\right)$ where $(a_i,b_i)_{:-1}^m$ are selected from $A_{\omega x}$, and (a,b) is an encryption of 0 with the public key $(a_i,b_i)_{i=1}^m$. likewise, define $P_u(\omega)$ to be the acceptance possibility of W', where $(a_i,b_i)_{:-1}^m$ are selected from $A_{\omega x}$, and (a,b) is now selected randomly from $O_P^{\in}O_p$. The assumption on W' says that

$$\begin{aligned}&\left|Exp_{\varsigma}\left[p_0(\omega)\right]Exp_{\varsigma}\left[p_{\mu}(\omega)\right]\right| \ge \frac{1}{2\in^c} \\ &Y=\left\{s\left|p_0(\omega)-p_u(\omega)\right|\ge\frac{1}{4\in^c}\right\}\end{aligned} \tag{37}$$

By an averaging line of reasoning in $\frac{1}{4\in^c}$ of the s are in *Y*. Therefore, it is adequate to show a distinguisher *Z* that separates between *U* and $A_{\omega x}$ for any ω *q Y*.

In the next, describe the distinguisher *Z*. distribution gives a *R* that is either *U* or $A_{\omega x}$ for some *s q Y*. *m* samples is taken from $(a_i,b_i)_{:}^m$, from *R*. Let $p_0(a_i,b_i)_{:-1}^m$ be the possibility with input $\left((a_i,b_i)_{i=1}^m,(a,b)\right)$ where the possibility is picked on (a,b) with the public key $(a_i,b_i)_{i=1}^m$ as an encryption bit 0.

Likewise, let $p_{\mu}\left(a_i,b_i\right)_{i=1}^{m}$ be the possibility with input $\left(\left(a_i,b_i\right)_{i=1}^{m},(a,b)\right)$ where the possibility is picked over the option of (a,b) as a uniform component of $O_n^{\in}*O_n$. While W' is applied as a multinomial number of times, the distinguisher Z reckon both $p_0\left(\left(a_i,b_i\right)_{i-1}^{m}\right)$ and $p_{\mu}\left(\left(a_i,b_i\right)_{i-1}^{m}\right)$ up to an habit-forming error of $\frac{1}{64\in^c}$. If the two estimation is different from each other more than $\frac{1}{64\in^c}$, Z will be accepted, or Z will be rejected.

5. Conclusions

Besides, to some very fundamental definitions referring to image matrixs, it must be made from the *normal distribution on D of width r*, denoted p_{Dr} The possibility of distribution image matrix of each $x\in D$ is partial to exp $\left(-\pi\left\|x/r\right\|^2\right)$. It is mentioned here the *system parameter (D)*. This is a positive real number related to any image matrix $D_{(q)}$ is an error parameter can be safely omitted here. Inaccurate to say, it lets the smallest r beginning with which p_{Dr} like a continuous normal distribution. For example, for $r>f_a(D)$, matrixes picked from p_{Dr} have norm about $r\sqrt{\in}$ with high possibility. By comparing, for enough small r, p_{Dr} offers almost all its mass to the primal 0, whereas not commanded for this part, a clear list of definitions can be seen in part 2.

The key of the encryption algorithm is called as the iterative step. Its input form a number r which is promised to be larger than $\sqrt{2}pf_{\in}(D)$, and n^c examples from p_{Dr} in which c is stable. Its output is an example from the distribution p_{Dr}, for $r'=r\sqrt{\in}/(\alpha p)$. Find that since $\alpha p>2\sqrt{\in}$, $r'<r/2$ to make the shifting matrixes of *norm* $\sqrt{\in}r$ into smaller matrixes of *norm* $\sqrt{\in}r$, the process prefers to using the quantum oracle.

Acknowledgements

This research was supported by the National Natural Science Foundation of China (No. 71471102), and Yichang University Applied Basic Research Project in China (Grant No. A17-302-a13).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Wang, X.Y., Liu, L.T. and Zhang, Y.Q. (2015) A Novel Chaotic Block Image Encryption Algorithm Based on Dynamic Random Growth Technique. *Optics and Lasers in Engineering*, **66**, 10-18. https://doi.org/10.1016/j.optlaseng.2014.08.005

[2] Hua, Z.Y., Zhou, Y.C. and Pun, C.-M. (2015) 2D Sine Logistic Modulation Map for Image Encryption. *Information Sciences*, **297**, 80-94. https://doi.org/10.1016/j.ins.2014.11.018

[3] Zhang, Y.-Q. and Wang, X.-Y. (2015) A New Image Encryption Algorithm Based on Non-Adjacent Coupled Map Lattices. *Applied Soft Computing*, **26**, 10-20.

https://doi.org/10.1016/j.asoc.2014.09.039

[4] Wang, X.-Y., Zhang, Y.-Q. and Bao, X.-M. (2015) A Novel Chaotic Image Encryption Scheme Using DNA Sequence Operations. *Optics and Lasers in Engineering*, **73**, 53-61. https://doi.org/10.1016/j.optlaseng.2015.03.022

[5] Toughi, S., Fathi, M.H. and Sekhavat, Y.A. (2017) An Image Encryption Scheme Based on Elliptic Curve Pseudo Random and Advanced Encryption System. *Signal Processing*, **141**, 217-227. https://doi.org/10.1016/j.sigpro.2017.06.010

[6] Wu, J.H., Liao, X.F. and Yang, B. (2017) Color Image Encryption Based on Chaotic Systems and Elliptic Curve ElGamal Scheme. *Signal Processing*, **141**, 109-124. https://doi.org/10.1016/j.sigpro.2017.04.006

[7] Mohammed, E.A. and Saadon, H.L. (2016) Optical Double-Image Encryption and Authentication by Sparse Representation. *Applied Optics*, **55**, 9939-9944. https://doi.org/10.1364/AO.55.009939

[8] Liu, L.F., Miao, S.X., Hu, H.P. (2016) N-Phase Logistic Chaotic Sequence and Its Application for Image Encryption. *IET Signal Processing*, **10**, 1096-1104. https://doi.org/10.1049/iet-spr.2015.0522

[9] Chen, W.-H., Luo, S.X. and Zheng, W.X. (2016) Impulsive Synchronization of Reaction-Diffusion Neural Networks with Mixed Delays and Its Application to Image Encryption. *IEEE Transactions on Neural Networks and Learning Systems*, **27**, 2696-2710. https://doi.org/10.1109/TNNLS.2015.2512849

[10] Wang, H., Wang, J. and Geng, Y.-C. (2017) Quantum Image Encryption Based on Iterative Framework of Frequency-Spatial Domain Transforms. *International Journal of Theoretical Physics*, **56**, 3029-3049. https://doi.org/10.1007/s10773-017-3469-5

[11] Tan, R.-C., Lei, T. and Zhao, Q.-M. (2016) Quantum Color Image Encryption Algorithm Based on A Hyper-Chaotic System and Quantum Fourier Transform. International Journal of Theoretical Physics, **55**, 5368-5384. https://doi.org/10.1007/s10773-016-3157-x

[12] Wang, Y.-Q., She, K. and Huang, R.-F. (2016) Optimal Symmetric Ternary Quantum Encryption Schemes. *International Journal of Theoretical Physics*, **55**, 4709-4722. https://doi.org/10.1007/s10773-016-3094-8

[13] Gong, L.-H., He, X.-T. and Cheng, S. (2016) Quantum Image Encryption Algorithm Based on Quantum Image XOR Operations. *International Journal of Theoretical Physics*, **55**, 4631-4632. https://doi.org/10.1007/s10773-016-3107-7

[14] Cesare, C. (2015) Encryption Faces Quantum Foe. *Nature*, **525**, 167-168. https://doi.org/10.1038/525167a

[15] Zhou, N.R., Hua, T.X. and Gong, L.H. (2015) Quantum Image Encryption Based on Generalized Arnold Transform and Double Random-Phase Encoding. *Quantum Information Processing*, **14**, 1193-1213. https://doi.org/10.1007/s11128-015-0926-z

[16] Lv, C.-H., Fan, H.-Y. and Li, D.-W. (2015) From Fractional Fourier Transformation to Quantum Mechanical Fractional Squeezing Transformation. *Chinese Physics B*, **24**, 020301. https://doi.org/10.1088/1674-1056/24/2/020301