Unstructured Fingerprint Database Matching Method based on Grover's Quantum Algorithm

Hui Li

School of Electrical Engineering and Automation, Henan Polytechnic University, Jiaozuo, China
Email: li20042007@163.com

Zhanzhan Zhang

School of Electrical Engineering and Automation, Henan Polytechnic University, Jiaozuo, China
Email: bgzhangzhan@163.com

Abstract—**Traditional fingerprint matching has slow speed and low probability in search rate under large-scale and unstructured database background. In order to solve this problem, an advanced searching method based on Grover's search algorithm is proposed. It improves the Oracle operator in Grover's algorithm and transforms the database one into four registers: index register, quantum bit register which includes target fingerprint's matching value, data register, 1 qubit register. Database two is transformed into including all the records of the matching value between input fingerprint and template fingerprints. Compared with traditional algorithm, this improved method decreases the number of repetitions and raise the probability of success, thus it can effectively improve the search speed and accuracy.**

Index Terms—**quantum parallelism, Grover's searching algorithm, fingerprint matching, Oracle operator**

I. Introduction

Confirmation of personal identity and authority is a very important part of life, especially with the networked era, people have become increasingly demanding security. However, more complicated set of passwords has become a big problem to people, in order to achieve higher security, more complex and more convenient to use a password is a popular choice. Each person's fingerprint pattern is different and unique in patterns, in other words, is the only and same. Depend on this uniqueness and stability, so a person's fingerprints can be complying with himself. Through comparing his fingerprints with his fingerprints stored in advance we can verify the authenticity of his identity [1]. But for large-scale fingerprint database matching system, classical matching algorithm can only search from the template fingerprint database which includes N fingerprints one by one until you find the one which is matched with the input fingerprint. This algorithm needs to find the result continues for $N/2$ times, the probability of success is $1/2$. So for large-scale database, this classical matching algorithm will appears to the problem of lower recognition rate and the more difficult problems [2]. In 1996, Grover proposed the quantum quick search algorithm [3,4], because N quantum bits is in the state of it's superposition, such intervention operation only need to repeat $\sqrt{N}$ times, the chance to obtain the correct answer is close to 1, so it solves the problem of the classical matching algorithm which is inefficient and difficult. Compared with traditional algorithm, Grover algorithm has the square acceleration effect. Applying classical Grover algorithm to search in a structured database has been researched and got good results. For example, classical Grover algorithm has been correctly applied in the field of communication and got excellent outcome [5, 6]. However, applying the Grover's algorithm to the fingerprint matching is an issue of searching for a specific solution in unstructured database [5], the study of original Grover's algorithm in solving these problems has not been reported recently.

This article presented the method of improving the Oracle operator in original Grover's algorithm. We can calculate N numbers of match-score values by using the quantum parallelism only through a single quantum circuit compared to N times of calculation in traditional method. Next we use the improved Grover's searching method to get the location of the target fingerprint which just need to apply $\sqrt{N}$ times of operation compared to N times of calculation in traditional method. The experiment results show that the improved Grover's algorithm can effectively improve the search speed and accuracy. The layout of the article is as follows. In Section II, we introduce the quantum parallel algorithm and classical Grover's quantum search algorithm. In Section III, we discuss the traditional fingerprint matching method based on ridge line calibration. In Section IV, we present the fingerprint matching method based on Grover's quantum algorithm which includes the background of design program and the design project of this method. In Section V, we carry out the simulation experiments with the FVC finger data and give the evaluation results between our method and traditional method. Our concluding remarks appear in Section VI.

II. Grover's Search Algorithm

A. Quantum Bits

The bit is the fundamental concept of classical computation and classical information. A classical bit has a state-either 0 or 1-a qubit also has a state. Two possible states for a qubit are the states $|0\rangle$ and $|1\rangle$, which as you might guess correspond to the states 0 and 1 for a classical bit. Notation like '$|\ \rangle$' is called the *Dirac notation*, and we'll be seeing it often, as it's the standard notation for states in quantum mechanics. The difference between bits and qubits is that a qubit can be in a state other than $|0\rangle$ or $|1\rangle$. It is also possible to form Linear combinations of states, often called super-positions:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{1}$$

The number α and β are complex numbers, although for many purposes not much is lost by thinking of them as real numbers. Put another way, the state of a qubit is a vector in a two-dimensional complex vector space. The special states $|0\rangle$ and $|1\rangle$ are known as computational basis states, and form an orthonormal basis for this vector space.

B. Single Qubit Gates

Classical computer circuits consist of wires and logic gates. The wires are used to carry information around the circuit, while the logic gates perform manipulations of the information, converting it from one form to another. So we can define an analogous quantum *NOT* gate for qubits.

The quantum *NOT* gate acts linearly, that is, it takes the state $\alpha|0\rangle + \beta|1\rangle$ to the corresponding state $\alpha|1\rangle + \beta|0\rangle$ in which the role of $|0\rangle$ and $|1\rangle$ have been interchanged [6, 7].

There is a convenient way of representing the quantum *NOT* gate in matrix form, which follows directly from the linearity of quantum gates. Suppose we define a matrix x to represent the quantum *NOT* gate as follows:

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2}$$

If the quantum state $\alpha|0\rangle + \beta|1\rangle$ is written in a vector

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \tag{3}$$

With the top entry corresponding to the amplitude for $|0\rangle$ and the bottom entry the amplitude for $|1\rangle$, then the corresponding output from the quantum *NOT* gate is:

$$X\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} \tag{4}$$

Notice that the action of the *NOT* gate is to take the state $|0\rangle$ and replace it by the gate corresponding to the first column of the matrix x. Similarly, the state $|1\rangle$ is replaced by the state corresponding to the second column of the matrix x.

C. Quantum Parallel Algorithm

The quantum parallelism is an essential feature of many quantum algorithms, it can make quantum computer evaluate the function $f(x)$ at many different value x at the same time, its basic principle is [8]: let $f(x):\{0,1\} \to \{0,1\}$ is a functions of 1 qubit domain and range. In a quantum computer, a simple approach of calculating the function is to consider the quantum computer whose initial state is two quantum bits. Through the appropriate sequence of logic gates this state can operate as follows:

$$|x, y\oplus f(x)\rangle \tag{5}$$

The symbol $\oplus$ here indicates addition modulo 2, the first register called 'data' register, the second is called the 'target' register, the transformation defined by the map $|x,y\rangle \to |x,y\oplus f(x)\rangle$ a name U_f, and it is easy to prove that it is unitary.

$y = 0$, the final state of the second quantum bit is the value $f(x)$. If the data register is prepared in the superposition $(|0\rangle+|1\rangle)/\sqrt{2}$, which can be created with a Hadamard gate acting on $|0\rangle$. Then we apply U_f, resulting in the state:
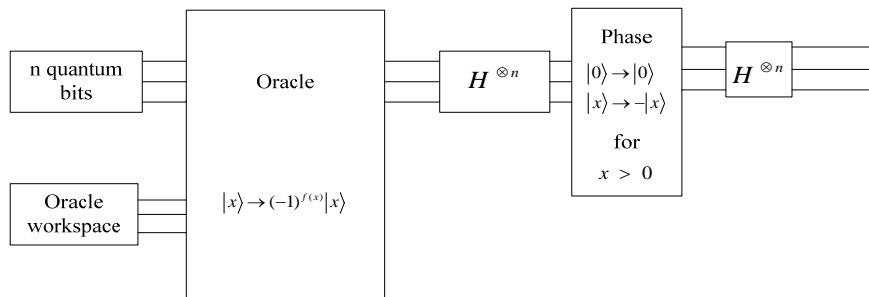

Figure 1. Circuit for the Grover iteration, G.

notation as:

$$\frac{|0,f(0)\rangle + |1,f(1)\rangle}{\sqrt{2}} \qquad (6)$$

The state we have got including different terms contains information about both $f(0)$ and $f(1)$, it is almost as if we have evaluated $f(x)$ for two value of x simultaneously. Here a single $f(x)$ circuit is employed to evaluate the function for multiple value of x simultaneously, by exploiting the ability of a quantum computer to be in superposition of different states.

More generally, the result of performing the Hadamard transform on n quantum bits initially in the all $|0\rangle$ state is:

$$\frac{1}{\sqrt{2^n}} \sum_x |x\rangle \qquad (7)$$

That is, the Hadamard can transform produces an equal superposition of all computational basis states, moreover, it does this extremely efficiently, producing a superposition of 2^n states using just n gates.

D. Grover's Quantum Search Algorithm

The Grover's algorithm begins with the computer in the state $|0\rangle^{\otimes n}$, the Hadamard transform is used to put the computer in the equal superposition state:

$$|\varphi\rangle = \frac{1}{N^{1/2}} \sum_{x=0}^{N-1} |x\rangle \qquad (8)$$

The quantum search algorithm then consists of repeated application of a quantum subroutine, know as the Grover iteration or Grover operator, the Grover iteration, whose quantum circuit is illustrated in Figure 1, can be broken up into four steps [9]:

First, apply the Oracle O;

Second, apply the Hadamard transformation $H^{\otimes n}$;

Third, perform a conditional phase shift on the computer, with every computational basis state except $|0\rangle$ receiving a phase shift of -1:

$$|x\rangle \rightarrow -(-1)^{\delta x_0} |x\rangle \qquad (9)$$

Fourth, apply the Hadamard transformation $H^{\otimes n}$.

III. MINUTIA MATCHING ALGORITHM BASED ON RIDGE LINE CALIBRATION

Before fingerprint pattern match, we should finish the process which includes the fingerprint acquisition, preprocessing and minutiae extraction [10-12]. Next, find a reference point to determine whether this fingerprint which needs to be matched has singular points or not, these singular points are the central and triangular points showed in Figure 2:
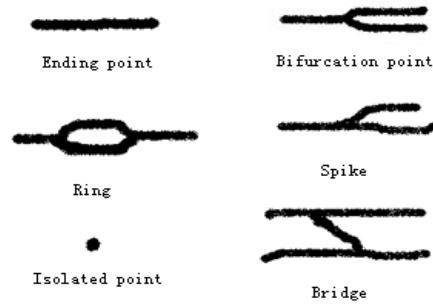

Figure2. The Central Points and Triangular Points.

If it has singular point, we select the nearest ridge line near the singular points, decide if the ridge lines corresponding to these two fingerprints which are needed to be matched are similar, we use these selected singular points as the reference point corresponding to those fingerprints for the next matching step when they are similar. There is the other situation, it does not have any singular points, and then we need to find another point as a reference point. We define two point sets, M and N, where the point set N denotes the L numbers of minutiae extracted from the input fingerprint, another point set M denotes the H numbers of minutiae extracted from the template fingerprints. Respectively expressing as two point sets:

$$M = \left\{ (x_1^M, y_1^M, \theta_1^M), \dots, (x_H^M, y_H^M, \theta_H^M) \right\} \qquad (10)$$

$$N = \left\{ (x_1^N, y_1^N, \theta_1^N), \dots, (x_L^N, y_L^N, \theta_L^N) \right\} \qquad (11)$$

Where $(x_i^M, y_i^M, \theta_i^M)$ and $(x_j^N, y_j^N, \theta_j^N)$ are respectively recorded three pieces of information which are the i th and j th feature points of point sets M and N, three pieces of information are x coordinates, y coordinates and direction.

We need to set two reference points respectively from the template minutia set and the input minutia set as origins of the corresponding polar coordinates, so we can convert minutiae into polar coordinates [13]. Because we do not know the corresponding relationship between the template minutia set and the input minutia set in advance, we will consider all possible pairs of reference points.

Each point of the template point set is $M_i = (1 \le i \le H)$ and each point from the input point set is $N_i = (1 \le i \le L)$, the $Rrotate[i][j]$ is defined as the rotation angle from input image to template image when we treat M_i and N_j as reference points. If M_i and N_j can be considered as a pair of corresponding points, that is to say, their corresponding ridge line are similar to a certain extent, then $Rrotate[i][j]$ will take a value between 0 to 360 degrees. Otherwise the value of $Rrotate[i][j]$ equal to 400 degrees, it represents that M_i and N_j are not a pair of corresponding points.

Next, determine the similarity of ridge line. Ridge line corresponding to minutiae M_i is defined as T, Ridge line corresponding to minutiae N_i is defined as t. Then determine weather t and T are matched, with the following formula to calculate the difference between the two ridge lines:

$$Diff\_dist = \frac{1}{S}\Sigma_{i=0}^{S}\left|T(d_i)-t(d_i)\right| \tag{12}$$

$$Diff\_ang = \frac{1}{S}\Sigma_{i=0}^{S}\left|T(\alpha_i)-t(\alpha_i)\right| \tag{13}$$

Where s is recorded number of points in ridge line, $T(d_i)$ and $t(d_i)$ respectively mean the distance from point i on ridge line T and t to the corresponding minutiae, $T(\alpha_i)$ expresses the angle between that two lines, one of these two lines is the connection between point i on the ridge line T and the associated minutia, the other one is the connection between previous sample and corresponding minutia. $t(\alpha_i)$ is the expression of the angle between two lines, one of these two lines is the connection between point i on the ridge line t and the associated minutia, the other is the connection between previous sample and corresponding minutia. If $Diff\_dist < W_d$, at the same time $Diff\_ang < W_\alpha$, W_d and W_α are selected as thresholds, then M_i and N_j are treated as a pair of corresponding minutia, the calculation method of $Rrotate[i][j]$ is:

$$Rrotate[i][j] = \beta\_in - \beta\_temp \tag{14}$$

where β_in and β_temp, respectively mean the angles between the connection of N_j and M_i with the first sampling point and the horizontal direction.

We got the reference points of template and input minutia set in advance, we will set the rest of the feature points in template set N and input set M transiting to the polar with treating N_i and M_i as origin. The former records the transforming template minutia coordinates, the reference point coordinates, minutia representation in polar coordinates; the latter one, records entering minutia coordinates, entering reference coordinates, minutia representation in polar coordinates, at the same time, draw rotation angle of the entered reference minutia which relative to template reference minutia[14, 15].

Set an matching score *match-score* whose initial value is 0, the matching condition to determining the y th input fingerprints minutia and the i th template fingerprints minutia is: give three thresholds, r_a, e_a, θ_a. Two minutiae should be satisfied with the following relationship:

$$\begin{aligned}\left|r_{yi}-r_{xj}\right|&\leq r_a\\\left|e_{yi}-e_{xj}\right|&\leq e_a\\\left|\theta_{yi}-\theta_{xj}\right|&\leq\theta_a\end{aligned} \tag{15}$$

Match-score plus by 1. Classical matching algorithm flow chart is showed in Figure 3.
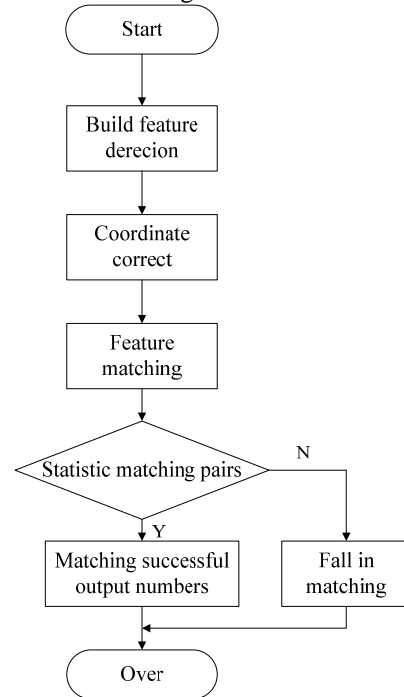

Figure3. Classical matching algorithm flow chart.

IV. FINGERPRINT MATCHING METHOD BASED ON GROVER'S QUANTUM ALGORITHM

A. Background of Design Program

Since quantum state has a high degree of parallelism calculation property, it can generate 2^n numbers of operation results at one time equate to 2^n times conventional computer operations. Grover's quantum algorithm is the quantum which can fully reflect the quantum parallelism and effectively solve the complexity problem of classical computing theory. Therefore, this chapter presents an assumption based on quantum parallelism calculation characteristic and fingerprint matching algorithm by using improved Grover's algorithm, this assumption reduces the computational complexity of the fingerprint matching algorithm effectively [16].

According to the analysis of previous chapter, we classical know that fingerprint minutia matching algorithm based on ridge line correction is used to match between the minutia of input fingerprint and template fingerprint database. Finally, we get the total numbers of matching minutia, *match-score*, and then search in template fingerprints to find out which one has the bigger minutia matching numbers than a certain threshold. We

can say that the input fingerprint and this template fingerprint are from the same finger. In this article we will extract a fingerprint A from template as the input fingerprint B, after getting all the numbers of *match-score* between fingerprint A and all the template fingerprints, search the minutia number of all the fingerprints in template, whose minutia number are the same with *match-score* is fingerprint A, then we can extract the fingerprint A from template database.

This is a quantum searching algorithm in non-structure database, unlike the previous case that the database is structured. Structure database issue is to detect the sending sequence in modern communication and data in this kind of database is stored in the form of disorder but whole arrangement. When we calculate the Oracle operator we can constitute a corresponding relationship between the 2^k numbers of quantum registers and 2^n numbers of sending sequences. Next we can use an effective algorithm to detect the minimum judgment value and get the sending sequence. But the problem in this paper we are going to solve is that 2^n numbers of selected fingerprints can't form a corresponding relationship with 2^k quantum registers. Because what we has extracted is the minutiae from 2^n numbers of fingerprints, each fingerprint's minutia is different, if the qubit of the maximum minutia number has whole arranged, it may certainly contain many qubit sequence of fingerprints minutia numbers which is not belong to the template fingerprint database. If applying the previous Oracle operator which is used in modern communications in striking the sending signal sequence to this study, it may detect out the fingerprint which is not included in the template fingerprint database, resulting in an error.

B. Unstructured Fingerprint Database Matching Method

This chapter presents an assumption based on quantum parallelism calculation characteristic and fingerprint matching algorithm by using improved Grover's algorithm, The principle diagram of this assumption is showed in Figure 4.

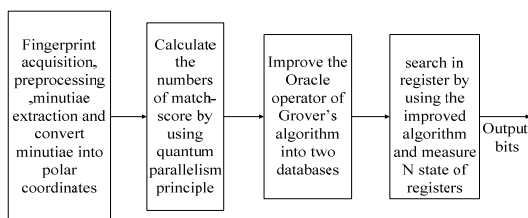The working principle of the system are described as:

Figure4. Principle diagram based on the quantum parallelism and quantum Grover algorithm fingerprint database search methods.

For the two qubit input and single-bit output $f(x)$ function of quantum computing parallelism, it can be implemented by using a quantum circuit as Figure 5.
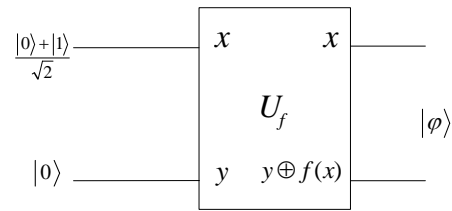

Figure 5. Quantum circuits for both compute $f(0)$ and $f(1)$ simultaneously.

The symbol U_f takes input $|x, y\rangle$ into $|x, y \oplus f(x)\rangle$, resulting in the state:

$$\frac{|0, f(0)\rangle + |1, f(1)\rangle}{\sqrt{2}} \quad (16)$$

Different item contains information about both $f(0)$ and $f(1)$, it is almost as if we have calculated $f(x)$ for two value of x simultaneously.

The same way in quantum parallel compute of n qubits input x for single-bit output $f(x)$ function can be used to achieve the following quantum circuit as Figure 6.
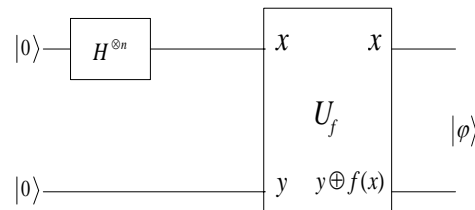

Figure6. Quantum circuits both compute $f(0)$ and $f(2^n - 1)$

Prepare the $n + 1$-bit state $|0\rangle^{\otimes n} |0\rangle$, the former n-bit apply Hadamard transformation and connect to the quantum lines used to implement U_f, the result state is:

$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n - 1} |x\rangle |f(x)\rangle \quad (17)$$

The concrete steps for calculating:

(1)Prepare the $n + 1$ qubit state $|0\rangle^{\otimes n} |0\rangle$ and then apply the Hadamard transform to the first n qubits;

(2)Let the prepare the $n + 1$ qubit state followed by the quantum circuit implementing U_f, this quantum circuit is to calculate the number of matched fingerprint match-score;

(3)Then we can get the starte $\frac{1}{\sqrt{2^n}} \sum_x |x\rangle |f(x)\rangle$, we apparently only evaluated f and get all the match-scores between input and template fingerprint.

Where $f(x)$ is equivalent to the classical method of striking *match-score* between the input fingerprint and one of the template fingerprint, unlike classical parallelism whose each multiple circuits built to compute *match-score* are executed simultaneously, to seek out all of the *match-score* between template fingerprint and input fingerprints need to loop 2^n times, but here, use quantum algorithm's ability to strike a *match-score* of a single line in different states of superposition state, it is used to simultaneously calculate x's multiple value of

match-score, using quantum lines shown above to strike, we can find out all the value, so it can speed up the computational efficiency. Implemented flow chart is showed in Figure 7.
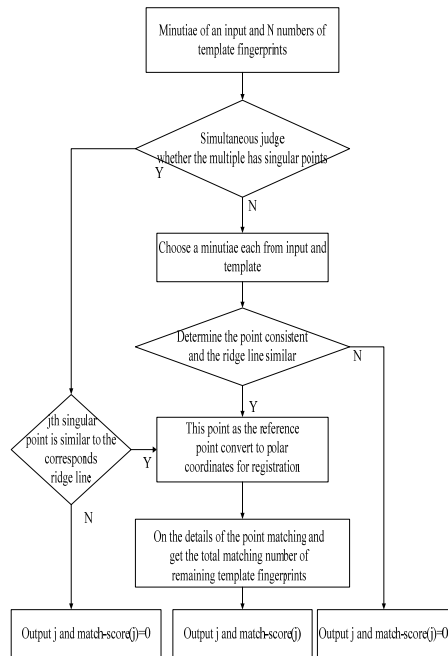

Figure 7. Improved to flow chart of striking match-score(j).

There are 2^n numbers of *match-score* have been calculated above, establish a matching scores database including these match-score values, then we can use quantum parallelism principle and quantum quick search algorithm to get the template fingerprint which is matched with the input fingerprint.

The total numbers of template fingerprints are $N = 2^n$, we extract a fingerprint from them as an input fingerprint, so we can find only one in template fingerprint database which is the same with this input fingerprint, what's more, the list of template fingerprints is not ordered in any obvious way. we get every binary strings of all the *match-score*, let the maximum one's length is l bits, the whole number of the input fingerprint minutiae is represented as a binary string s, these N numbers of template fingerprints are labeled from 1 to N, all these *match-score* we have obtained from the input fingerprint can be expressed as $d_0,...,d_{N-1}$, we need to construct two databases:

Database one contains four registers:

1) An n qubit 'index' register initialized to $|0\rangle$;

We know that for the single bit case, the quantum ground state are $|0\rangle$ and $|1\rangle$, but this quantum qubit not only has that two states $|0\rangle$ and $|1\rangle$ but also has continuous state which falls between $|0\rangle$ and $|1\rangle$, this state is a linear combination of those two states called superposition, like follows:

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{18}$$

Multi-qubit is like the assumption of the above n qubit, its ground state of the quantum system are $\underbrace{|00...00\rangle}_{n}\underbrace{|00...01\rangle}_{n}...\underbrace{|11...10\rangle}_{n}\underbrace{|11...11\rangle}_{n}$ of 2^n numbers, these just the N subscript of $d_1,...,d_N$ in database two needed to be structured, these N numbers of value can be addressed by an index x. The quantum state can load in this ground state's superposition state, so x can be in a superposition of multiple value. n Hadamard gates act in parallel on n qubit whose initial state is $|0\rangle$. The parallel action of n Hadamard gates is denoted as $H^{\otimes n}$, this produces the state:

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle \tag{19}$$

Symbol x is in a superposition of multiple value, we can index many value at one time, so it can increase the search speed.

2) An l qubit register initialized to $|s\rangle$ and remaining in that state for the entire computation;

3) An l qubit 'data' register initialized to $|0\rangle$;

4) A 1 qubit register initialized to $(|0\rangle - |1\rangle)/\sqrt{2}$.

Database two include $N = 2^n$ registers, each unit consists of l qubit, it saves $N = 2^n$ numbers of *match-score* calculated in advance, the template fingerprint whose *match-score* is the same with the number of input fingerprint minutiae is the match fingerprint which we are searching for.

The key part of implementing the quantum searching algorithm is realization of the Oracle, which must flip the phase of the index which locates s in the memory. Suppose the first database is in the state:

$$|x\rangle|s\rangle|0\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{20}$$

Now the index register is in the state $|x\rangle$, this state is the superposition of each ground state, the data register is in the state $|0\rangle$, then the contents d_x of the x th memory cell are added to the data register: $|0\rangle \to |0 \oplus d_x\rangle$, where the addition $\oplus$ is done bitwise, modulo 2. That is to say the data register state at this time is:

$$|x\rangle|s\rangle|d_x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{21}$$

The state of second register in the first database is s, the state of the third register is $|d_x\rangle$, compare with second and third registers, if they are the same value, then a qubit flip is applied to register 4; otherwise nothing is changed. The effect of the operation is

$$|x\rangle|s\rangle|d_x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}} \to \begin{cases} -|x\rangle|s\rangle|d_x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}, d_x = s \\ |x\rangle|s\rangle|d_x\rangle\frac{|0\rangle - |1\rangle}{\sqrt{2}}, d_x \neq s \end{cases} \tag{22}$$

Then we add the contain d_x of the x th register in the second database to the data register: $|d_x\rangle \rightarrow |d_x \oplus d_x\rangle$, we can see that the date register of the first database is restored to the state $|0\rangle$. We can use quantum search algorithm to determine the position of s in the database, where this operation has used only $O(\sqrt{N})$ times in adding the content of database to the data register, but the classical way with the control need this operation N times. After those steps above, the overall effect is that, if $d_x = s$, the state of register one is changed from $|x\rangle$ to $-|x\rangle$, and to leave the register alone otherwise. Thus the first step Oracle operator in Grover's algorithm has been achieved. The total action of the Oracle thus leaves registers 2, 3 and 4 unaffected and unentangled with register 1, the location of these N states and in front of the establishment of a database match scores correspond to position.

Use an operation known as Hadamard transform on the N states of register 1 unitary transform, by using matrix D on the probability amplitude vector of all states in registers 1 have a unitary transformation, rotating average value of all the states to greatly reduce the probability of finding out the target range of quantum states. Enlarge the probability of quantum state amplitude, matrix D is defined as:

$$Dpq = \begin{cases} \frac{2}{N}, p \neq q \\ -1+\frac{2}{N}, p=q \end{cases} \quad (23)$$

Expressed in matrix form is:

$$\begin{vmatrix} -1+\frac{2}{N} & & & \\ & -1+\frac{2}{N} & \frac{2}{N} & \\ & & \cdots & \\ & \frac{2}{N} & -1+\frac{2}{N} & \\ & & & -1+\frac{2}{N} \end{vmatrix} \quad (24)$$

Finally, the index register can be measured on the location of the target quantum state, thus the location of the target fingerprint can be searched.

V. EXPERIMENT RESULTS AND ANALYSIS

In this section, we compare our fingerprint matching method based on Grover's quantum algorithm with traditional fingerprint recognition method.

We use the recognition rate to performance evaluation of an automated fingerprint identification algorithm. The performance evaluation has two indexes. The FRR is false reject rate and the FAR is false accepted rate. Calculation formula is shown below

$$FAR = falsenum / (correctnum + falsenum) \times 100\% \quad (25)$$

$$FRR = rejectnum / (correctnum + falsenum) \times 100\% \quad (26)$$

FRR is defined as the ratio of false rejects to total attempts at verification, which is how many times you have a mismatch when you should have match. While FAR is defined as the ratio of false rejects to total attempts at verification, which is the number of times you get match (with some else's fingerprint) when you should not be matched. These test results allow us to calculate the FRR and FAR, and based on these assess the quality of different algorithms. In this paper, all algorithms are programmed in MATLAB. We use the FVC fingerprint data to verify the effectiveness of our algorithm. We extract 256 fingerprint images to create a fingerprint template database. A fingerprint is selected from the template database as the identifying one. Our experiment purpose is to find out the location of this fingerprint in database. The experiment result is given bellow.

TABLE I.
EXPERIMENTAL RESULTS OF TRADITIONAL ALGORITHM AND OUR ALGORITHM

Algorithm	Traditional Algorithm	Our Algorithm
Matching Numbers	256	16
Matching Time(ms)	2.96	1.70
FAR(%)	3.98	1.05
FRR(%)	2.41	2.38
Matching accuracy (%)	93.6	96.57

The results in table I shows the different matching results between our algorithm and traditional algorithm. We can see that the improved Grover matching method has lower matching numbers and the square root of the traditional algorithm matching numbers. Moreover, our matching time has an obvious advantage on efficiency which just needs almost the a half of traditional matching time. At the same time, the matching accuracy is improved by using our algorithm.

VI. CONCLUSION

Quantum computation and quantum information has taught us to think physically about computation, and this approach yields many new and exciting capabilities for information processing and image processing, information theorists and MCS specialist have been gifted with a new and rich paradigm for exploration. I propose a improved Grover's search algorithm, the issue of applying this algorithm to fingerprint search is the problem of applying quantum computation to image search. By improving the Oracle operator of Grover's algorithm and combining with classical algorithm we can solve unstructured fingerprint matching problem. The next step is to use this improved Grover's algorithm to solve other image problem and apply it to the image search on the Internet.

REFERENCES

[1]   S. Yoon, J. Feng, A. K. Jain, "On latent fingerprint enhancement," in: Proc. SPIE, *Biometric Technology for Human Identification*, vol. VII, 2010.

[2]   Aiyan. Wu, Shize. Wei, "A large-scale network based on fingerprint data retrieval method," *Computer science*, 2005, pp. 196-199.

[3]   L. K. Grover, "Quantum mechanics helps in searching for a needle in a haystack," *Phys. Rev. Lett*, 1997, pp. 128-129.

[4]   L. K. Grover, "A fast quantum mechanical algorithm for database search," *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing*, 1996, 212-219.

[5]   X. B. Lu, "Design signal detection project of MIMO communication systems based on improved Grover algorithm," *Lect. Notes Electr. Eng*, vol. 113 LNEE, pp. 13-21, July 2011.

[6]   F. Li, L. Z. Zhou, L. Liu, and H. B. Li, "A quantum search based signal detection for MIMO-OFDM systems," *Int. Conf. Telecommun. ICT*, pp. 276-281, May 2011.

[7]   Michael. A. Nielsen, Isaac. L. Chuang, *"Quantum Computation and Quantum Information*, England: University of Cambridge, 2000.

[8]   A. Lambert-Mogiliansky, S. Zamir and H. Zwirn, "Type indeterminacy: A model of the KT (Kahneman Tversky)," *Man. J. Math. Psych.*, 2009, pp. 349–361.

[9]   B. Prieto, Galiana, P. A. Postigo, C. Algora, L. J. Martínez and I. Rey-Stolle. *Appl. Phys. Lett.*, 2009.

[10] P. W Shor, Polynomial-time algorithms for jprime factorization and discrete logarithms on a quantum computer, Slam Joumal on Computing, 1997, pp. 201-203.

[11] L. K. Grover, "A fast quantum mechanical algorithm for estimating the median," *Technical Report*, 1996.

[12] C. T. Hsieh, E. Lai, Y. C. Wang. "An effective algorithm for fingerprint image enhancement based on wavelet transform, " *Pattern Recognition*, 2003, pp. 303-312.

[13] Jingguang. Fu, Gang. Xu. Yuguo, "Fingerprint minutiae extraction based on binary image," *Journal of Computer Research and Development*, 2004, pp. 720-727.

[14] Tao Mei, Bin Wang, Xiangsheng Hua, Heqin Zhou, Shipen li, "Probabilistic Multimodality Fusion for Event Based Home Photo Clustering," Canada, 2006, pp. 1757-1760.

[15] Jiang. Xudong, Yau. Weiyun and Wee. Ser, "Minutiae extraction by adaptive tracing the gray level ridge of the fingerprint image," I*EEE 6th International Conference on Image Processing*, Japan, 1999, pp. 852-856.

[16] A. K. Jain, S. Pankanti, S. Prabhakar, et al, "Recent advances in fingerpint verificartion," Proc. 3rd Int'l Conf. Audio-and-Video-Based Biometric Person Authentication, Lecture Notes in *Computer Science* 2091. Berlin: Springer, 2001, pp. 182-191.

[17] Q. Zhao, L. Zhang, D. Zhang, N. Luo, "Direct pore matching for fingerprint recognition," in: *Proceedings of ICB'09*, 2009, pp. 97–606.

[18] J. Galbally, R. Cappelli, A. Lumini, G.G. de Rivera, D. Maltoni, J. Fierrez, J. Ortega-Garcia and D. Maio, "An evaluation of direct attacks using fake fingers generated from iso templates," *Pattern Recognit. Lett.*, 2010, pp. 725–732

Hui Li was born in 1976. He received the doctor's degree in information and communication engineering in 2008 from Nanjing University of Science and Technology. He is currently working as a teacher in Henan Polytechnic University. His research interests are quantum information and computation.

Zhanzhan Zhang is master degree candidate for Henan Polytechnic University, major in image processing. Her research interests are quantum algorithms and image processing.