Quantum Matching Algorithm for Biometric Fingerprints

Gabriela Mogos (gabriela.mogos@hotmail.com)
Xi'an Jiaotong-Liverpool University

Research Article

Keywords: biometrics, fingerprint templates, IBM Quantum, quantum image processing

Posted Date: March 15th, 2023

DOI: https://doi.org/10.21203/rs.3.rs-2681592/v1

Abstract

Fingerprints remain constant throughout life. In over 140 years of fingerprint analysis, no two fingerprints have ever been found to be identical, even in identical twins. Each of us is born with a unique set of fingerprints, although experts still don't know with what exactly what we use them for. In information technology terms, biometrics is associated with technologies and techniques designed to secure and confirm identity based on individual, measurable biological characteristics of the person. Fingerprints can be used in systems and schemes designed to gain access to a computer, a room and, why not, a bank account. A verification system authenticates the person's claimed identity by comparing the fingerprints provided by the person at a given point in time with the measures of these features previously stored in the system and associated with the person's claimed identity.

This paper presents a quantum matching algorithm for biometric fingerprints. For this, classical fingerprinting was encoded into quantum states using an adapted Novel Enhanced Quantum model and the quantum circuits, for storage and for matching, were implemented and tested on the IBM Quantum Experience platform and on a local virtual quantum simulator.

I. Introduction

Archaeological evidence suggests that the use of fingerprints to identify a particular person was probably practiced in 6000–7000 BC, for example by Assyrians, Chinese and the inhabitants of Jericho.

In 1686 Marcello Malpighi, professor of anatomy at the University of Bologna, made a study of the design on the fingers and noted that it contained ridges, spirals and curves. In 1923, Joannes Evangelista Purkinje, professor of anatomy at the University of Breslau, published a paper describing nine types of fingerprint patterns. Neither of the two scientists mentioned made any reference to the identifying value of fingerprints, but their observations encouraged further research into fingerprints, including the possibility of using fingerprints to identify individuals. A milestone in the use of fingerprints for identification is the discovery made by Sir William Herschel. During his work in Jungipoor, India, he used prints of the entire palms of people's hands to identify them. Analysing handprints from a large number of people, he realized that that fingerprints did not repeat themselves, thus concluding that they were unique. Fingerprint identification is the most mature biometric method, being implemented at an early stage since 1960. Since 1960, fingerprint identification has become a semi-automatic process. Then, in 1969, the FBI began efforts to create a system to automate the fingerprint identification process, which had become very laborious and required many man-hours. Automated Fingerprint Identification System (AFIS) have been developed since 1981, and the first standard for the sharing of fingerprint detail data was published in 1986. Today [1], the latest technologies of fingerprint identification are based on matching algorithms for measurable minutiae. Each measurable minutiae can be described by some attributes, including its position in the fingerprint, its direction, its type (termination or bifurcation), and a value representing the quality of the fingerprint pattern in its proximity.

This paper addresses some of the critical issues of fingerprint biometric systems related to algorithm complexity and image processing speed. One of the solutions is to change the computing paradigm. Such a new paradigm is offered by the theory of quantum computing which is based on using non-intuitive principles of quantum mechanics to perform computations. Based on the superposition and entanglement properties of quantum states, quantum computation offers parallel processing capabilities and low-complexity quantum circuits.

This research approaches quantum technologies as an opportunity to introduce a fingerprint matching algorithm. In realizing this vision, we used an adapted Novel Enhanced Quantum Representation (NEQR) model for storing a fingerprint image in quantum systems and then the quantum circuits, for storage and matching, were implemented and tested on the IBM Quantum cloud platform and locally on a virtual quantum simulator.

The paper consists of two sections: the first presents the fingerprint image storage model in quantum systems and the second describes the matching algorithm of two biometric fingerprints.

Ii. Quantum Fingerprint Template

A biometric system is a template recognition system through which biological characteristics can be identified. A biometric system contains two functional modules: an enrolment module and an identification module.

The enrolment module, which prepares the data to be used in the system to identify the person, processes the digital representations acquired by the sensors to generate compressed forms of the fingerprints, called templates. A particular user's template can be extracted from a single biometric sample or can be generated by processing several samples. At this stage, we propose storing the fingerprint image in quantum systems using the adapted NEQR model.

The identification module performs person recognition. The biometric feature of the person to be identified is scanned and converted into a digital representation with the format identical to that of the template used for storage in a database. This representation is known as a feature matcher and is compared against the template stored in the database. The paper [2] states that dactyloscopic researchers, based on studies and practical experience in this field, have concluded that it is impossible to meet two people with identical papillary patterns. Each papillary pattern of each finger has a unique morphology, and no two fingers have identical patterns, even in same person. At this stage, we propose the quantum fingerprint matching algorithm.

II.1. THE FINGERPRINT IMAGE ENROLMENT

We consider a fingerprint image provided by an SDK in a one-byte-per-pixel and grey format (white is 255 and black is 0). Each image is vertically captured and horizontally centered in the field of view.

Figure 1 shows a scanned fingerprint image. The origin is in the upper left corner of the image. The position of the x-axis increases positively from the origin to the right side of the image and the y-axis increases positively from the origin to the bottom of the image. Using Matlab, the fingerprint image has been represented as 8-bit pixel matrix.

To store a 2^n x 2^n classical fingerprint image in quantum systems $|\Psi^{QFI}\rangle$ following the NEQR model [3], is needed 2n + 8 qubits, where *2n* is the number of qubits for storing the pixel position in $|yx\rangle$ format and 8 is the number of qubits for storing the grayscale values. The quantum fingerprint image preparation, in our case, does not require ancillae qubits.

$$|\Psi^{QFI}\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle|y\rangle|x\rangle = \frac{1}{2^n}\sum_{y=0}^{2^n-1}\sum_{x=0}^{2^n-1}|g(y,x)\rangle|yx\rangle \quad (1)$$

To build the quantum circuit a 4 x 4 sample of the fingerprint image was selected. Twelve qubits were used for this: 4 qubits for representing the positions and 8 qubits for storing the grayscale values. The quantum circuit (Fig. 2.) contains Hadamard and conditional X gates. Hadamard gates were applied to the position qubits, and conditional X-gates were applied to the 8-qubits to map the grayscale values. The if statement conditionally executes quantum operations based on the classical register values.

A 6-qubit circuit was run on the IBM Quantum devices: *ibm_nairobi* and *ibm_oslo*, and the 12-qubit circuit was run locally using Qiskit Aer on the QASM simulator. This simulator emulates the execution of a quantum circuit on a real device. We used a system Intel(R) Core (TM) i7-8550U CPU @ 1.80GHz., 16 GB RAM.

The histogram obtained from the QASM simulator is shown below:

For the 4 x 4 quantum fingerprint image (QFI 1), the Eq. (1) can be written as:

$$|\Psi^{QFI1}\rangle = 2^{-2}(|00001011\rangle \otimes |\mathbf{0000}\rangle + |10100101\rangle \otimes |\mathbf{0001}\rangle + |00000111\rangle \otimes |\mathbf{0010}\rangle + |00000111\rangle \otimes |\mathbf{0011}\rangle + |00000000\rangle \otimes |\mathbf{0100}\rangle + |10110100\rangle \otimes |\mathbf{0101}\rangle + |00111111\rangle \otimes |\mathbf{0110}\rangle + |10000111\rangle \otimes |\mathbf{0111}\rangle + |00011111\rangle \otimes |\mathbf{1000}\rangle + |00000000\rangle \otimes |\mathbf{1001}\rangle + |00011111\rangle \otimes |\mathbf{1010}\rangle + |00000000\rangle \otimes |\mathbf{1011}\rangle + |00000000\rangle \otimes |\mathbf{1100}\rangle + |00000000\rangle \otimes |\mathbf{1101}\rangle + |00000000\rangle \otimes |\mathbf{1110}\rangle + |10010001\rangle \otimes |\mathbf{1111}\rangle)$$

The 8-bit group represents the grayscale values and the 4-bit group, the positions in the $|yx\rangle$ format (Fig. 3).

According to [3], the cost for preparation the NEQR model of a $2^n \times 2^n$ fingerprint image with gray range 2^q and enough ancillae qubits, is no more than $O(qn2^{2n})$. For preparation of a 4 x 4 fingerprint image on NEQR model, we have q = 8 and n = 2, and the cost is $O(16x2^4)$.

Iii. Quantum Matching Algorithm

In identification mode, the system recognises a specific person by searching through the templates of all users in the database to find a match. The system performs a one-to-many comparison to determine the identity of a particular person, without the subject claiming a specific identity. In classical systems, the matching techniques are divided into those based on minutiae or correlation based. Those based on minutiae points try to align two sets of minutiae points and determine if they are equal.

In our view, the use of quantum techniques is beneficial in terms of increasing the retrieval speed in searching unsorted database by a given fingerprint as well as the processing speed of the matching algorithm. In classical computing models, searching unsorted databases cannot be done faster than in linear time (only searching through each element is optimal). The Grover algorithm [4] shows that, in the quantum model, the search can be performed faster than in the classical one, its time complexity $O(N^{1/2})$ is asymptotically the fastest possible for searching unsorted databases. However, the quadratic speedup is significant when *N* is large enough.

The proposed quantum algorithm can perform a one-to-many comparison of all fingerprint images in a database, determining the identity of a specific person. The quantum circuit was tested on the IBM Quantum cloud platform [5] and locally, on a quantum simulator [6]. For testing we used two quantum fingerprint images shown in Figs. 3 and 4.

For the second 4 x 4 quantum fingerprint image (QFI 2), the Eq. (1) can be written as:

$$|\Psi^{QFI2}\rangle = 2^{-2}(|10010110\rangle \otimes |\mathbf{0000}\rangle + |00010100\rangle \otimes |\mathbf{0001}\rangle + |01011100\rangle \otimes |\mathbf{0010}\rangle + |00011011\rangle \otimes |\mathbf{0011}\rangle + |00000000\rangle \otimes |\mathbf{0100}\rangle + |10101101\rangle \otimes |\mathbf{0101}\rangle + |10101101\rangle \otimes |\mathbf{0110}\rangle + |00000000\rangle \otimes |\mathbf{0111}\rangle + |00000000\rangle \otimes |\mathbf{1000}\rangle + |00000000\rangle \otimes |\mathbf{1001}\rangle + |00011111\rangle \otimes |\mathbf{1010}\rangle + |00000000\rangle \otimes |\mathbf{1011}\rangle + |00000000\rangle \otimes |\mathbf{1100}\rangle + |00000000\rangle \otimes |\mathbf{1101}\rangle + |00000000\rangle \otimes |\mathbf{1110}\rangle + |11111111\rangle \otimes |\mathbf{1111}\rangle)$$

Similar, the 8-bit group represents the grayscale values and the 4-bit group, the positions in the $|yx\rangle$ format.

In our study, we considered every pixel of the fingerprint image as characterized by the doublet $p = \{|yx\rangle, |g(y,x)\rangle\}$ encoding the position and the grayscale value.

To start, the 4 x 4 samples of each quantum fingerprint image are aligned and then compared qubit by qubit (Fig. 5). The alignment is done according to the value of the position registers $|yx\rangle$.

The quantum matching circuit employs 8 ancillae qubits and uses conditional CC X-gates with *ctrl_state* parameters. These conditional gates perform X-gates on the ancillae qubits (targets), if the states of the qubits belonging to QFI1 and QFI2 (controls) are equal (Fig. 7).

After running the quantum matching algorithm, 100% matching was obtained in 9 out of 16 positions and partial matching for the rest (Fig. 8). In such cases, a 'mismatch' threshold is imposed to compensate the algorithm errors or distortions caused by skin elasticity.

III.1. RESOURCE Costs for fingerprint matching Quantum Circuit

In the following we will calculate the resource cost for the fingerprint matching quantum circuit.

In general, to determine the resource cost for a quantum circuit, it is necessary to consider the following: the total number of qubits required by the circuit, the total number of gates used by the circuit, the number of gate layers in the circuit and the effectiveness of the quantum circuit against errors. A layer is made up of quantum gates that operate in parallel. Also, the circuit depth calculates the longest path between the data input and the data output where each gate is counted as one unit.

The three quantum circuits use Hadamard H-gates, X-gates, and CC X-gates:

Because it acts on two qubits, a C X-gate has a higher error rate than a single qubit gate [7], and a quantum circuit with a large number of C X-gates has a higher risk of computational failure than a circuit with a small number of C X-gates. Therefore, in order to evaluate the performance of our quantum circuits, the number of C X-gates must be determined as well as how many layers the circuit contains. According to [8] to decompose an *n*-qubit Toffoli gate requires *2n* C X-gate and a CC X-gate with a single ancillae qubit is free of garbage output [9].

The QFI 1 quantum fingerprint (Fig. 3) circuit contains: X-gate: 52, H-gate: 4, and the circuit depth is 55.

The QFI 2 quantum fingerprint (Fig. 4) circuit contains: X-gate: 51, H-gate: 4, and the circuit depth is 54.

The fingerprint matching quantum circuit uses: CC X-gates: 16, H-gate: 4, and the circuit depth is 6. The Hadamard and X gates are one qubit gates while the CC X-gate is a three-qubit gate (Fig. 9.).

The resource cost of the fingerprint matching quantum circuit is determined by: the total number of qubits (the qubit cost (Q)), the total number of C X-gates used in the circuit (C X-gate cost), the number of C X-gate layers in the circuit (L), and the effectiveness of quantum computing against errors (L x Q).

The total number of the C X-gates used in the quantum circuit is given by the number of the CC X-gate, knowing that each CC X-gate contains 7 C X-gates, and the number of C X-gate layers is 3.

The total number of C X-gates is 16 x 7 = 112 and the number of the C X-gate layers is 16 x 3. The effectiveness of quantum computing against errors L x Q is 28 x 48.

For the qubit cost (Q) we included the ancillae qubits because they hold computations. Q cost = input qubits + ancillae qubits = 4 + 16 + 8 = 28.

The probability of success (S) of the circuit can be determined using the qubit cost (Q) and the number of the C X-gate layers (L):

$$S = \frac{1}{Q \bullet L}$$

If the value of S is less than a threshold value, then a correct calculation is given, otherwise a quantum error correction is required.

Iv. Conclusion

Biometric technologies are in a time of development, and the interest of potential users is focused on the advantages and disadvantages this technology offers in terms of security, economy and comfort. The fingerprint identification using technology is to take an image of the fingerprint. Then the image is processed to get the best possible image for a correct match after verification.

Currently, fingerprint identification requires a verification operation to be carried out first. This verification has a number of particularities, depending on the purpose for which the fingerprint is used. Verification involves comparing a fingerprint with a fingerprint that is already stored in the system. In identification mode, the system recognizes a specific person by searching through templates of all users in the database in order to find a match. Thus, the system conducts a one-to-many comparison to determine the identity of a particular individual (or fails if the subject is not registered in the system's database), without it claims a specific identity. The migration from classical to quantum technologies could bring an important benefit in terms of high processing speed, low complexity algorithms and biometric fingerprint security.

Declarations

Conflict of interest

The author declares no competing interests.

Ethical standards

This work is done in compliance with ethical standard.

Funding

This work is supported by Xi’an Jiaotong - Liverpool University (XJTLU), Suzhou, China under Research Development Fund (RDF-21-02-010).

Availability of data and materials

Not applicable

References

1. B.G. Sherlock, *Computer Enhancement and Modeling of Fingerprint Images*, Automatic Fingerprint Recognition System, Springer-Verlag, 2004
2. Gh. Păşescu, Ion. R. Constantin, *Secretele amprentelor papilare* (in Romanian), Publishing National, 1996.
3. Y. Zhang, K. Lu, Y. Gao, M. Wang, *NEQR: a novel enhanced quantum representation of digital images*, *Quantum Inf. Process*. 12(8), 2833–2860, 2013.
4. L. K. Grover, *A Fast Quantum Mechanical Algorithm for Database Search*, Proc. of 28th Ann. ACM Symp. on the Theory of Computing, p.212-219, 1996.
5. https://www.ibm.com/quantum-computing/. Retrieved 02/2023.
6. https://qiskit.org. Retrieved 02/2023.
7. Rigetti Computing, QPU Specifications - Rigetti 16Q Aspen 4, 2019, available at: https://www.rigetti.com/qpu
8. V.V. Shende, I.L. Markov, *On the CNOT-cost of TOFFOLI gates*, Quant. Inf. Comp. 9(5-6):461-486, 2009.
9. K.-W. Cheng, C.-C. Tseng, *Quantum full adder and subtractor*, Electron. Lett. 38(22), 1343–1344, 2002.

Figures

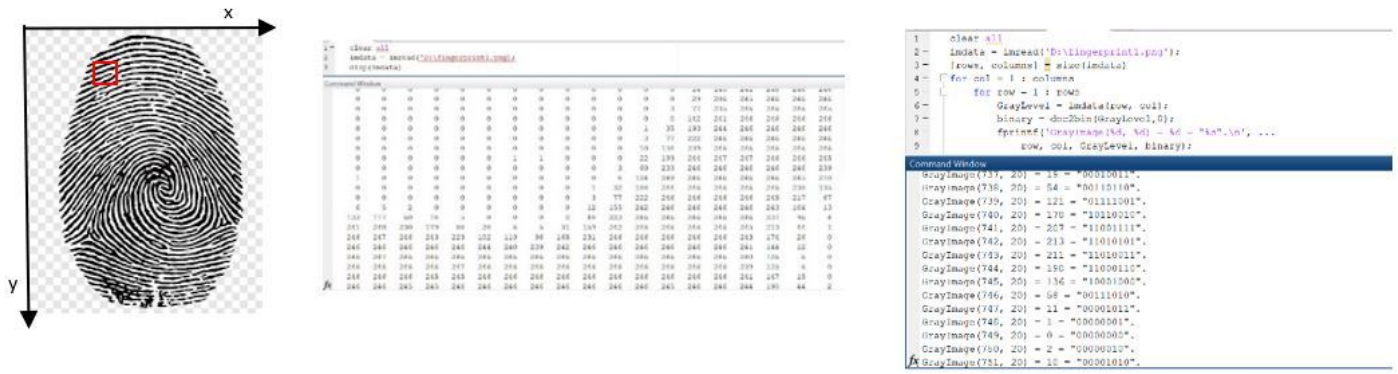


Figure 1

Fingerprint image as a matrix of pixels

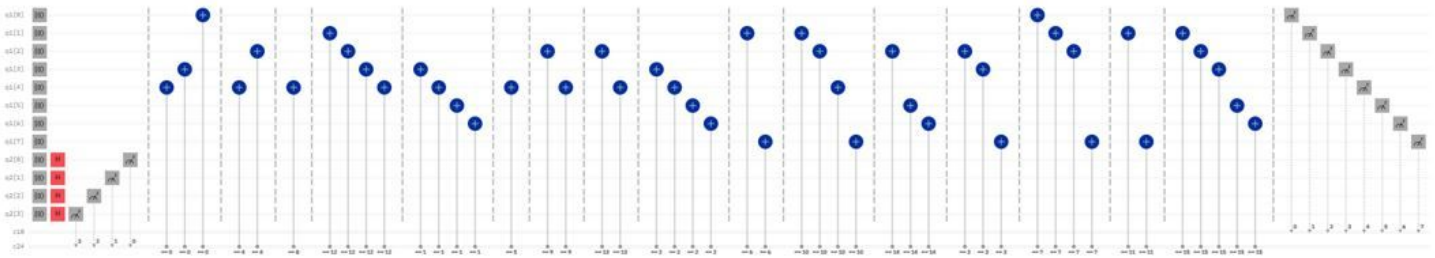
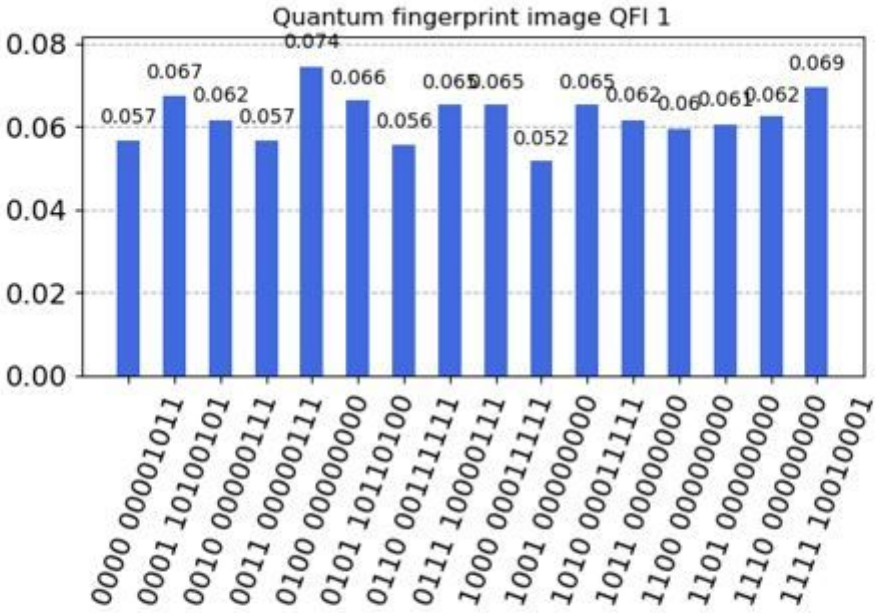


Figure 2

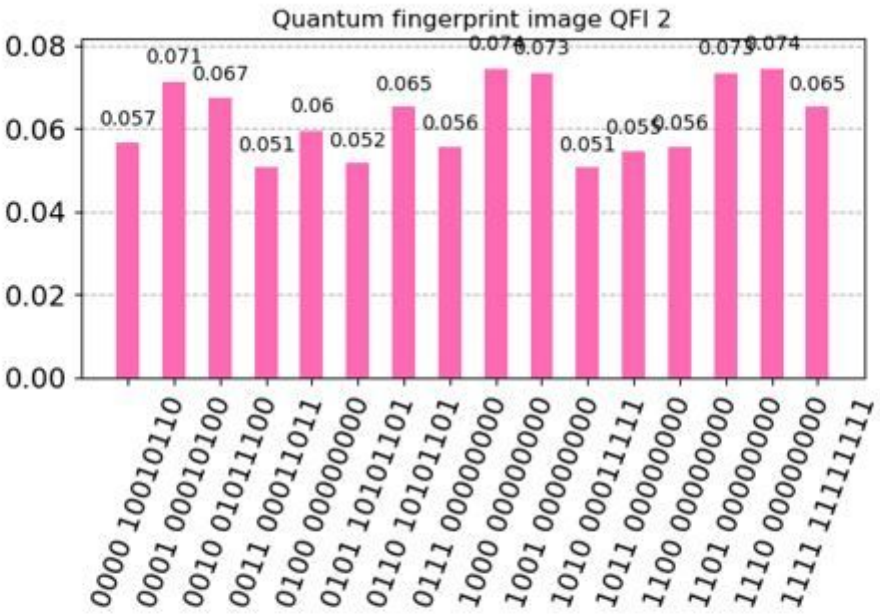
Quantum circuit on IBM Quantum cloud platform



y \ x	00	01	10	11
00	00001011	10100101	00000111	00000111
01	00000000	10110100	00111111	10000111
10	00011111	00000000	00011111	00000000
11	00000000	00000000	00000000	10010001

Figure 3

Quantum fingerprint image QFI 1



y \ x	00	01	10	11
00	10010110	00010100	01011100	00011011
01	00000000	10101101	10101101	00000000
10	00000000	00000000	00011111	00000000
11	00000000	00000000	00000000	11111111

Figure 4

Quantum fingerprint template QFT 2

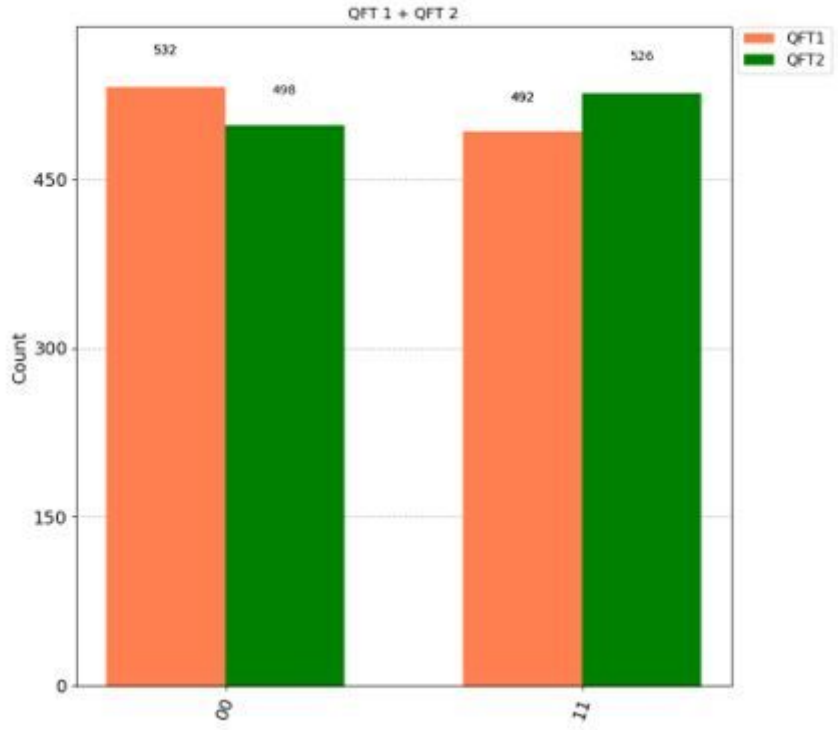


Figure 5

Align two quantum fingerprint images.

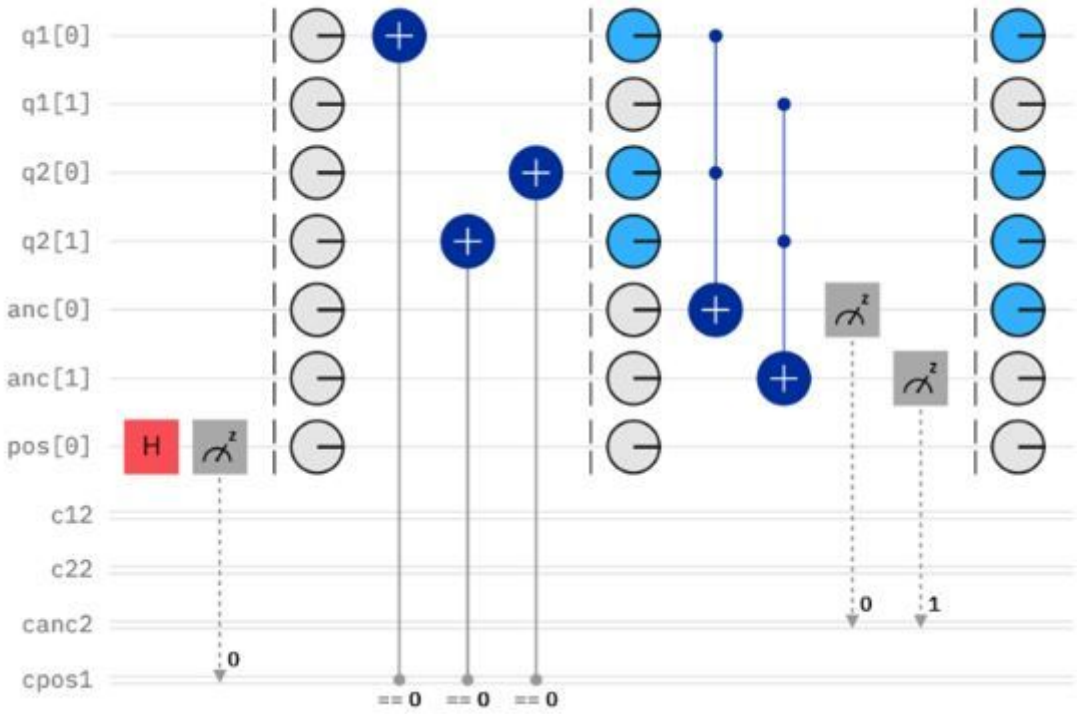


Figure 6

Simplified quantum matching circuit on IBM Quantum platform.

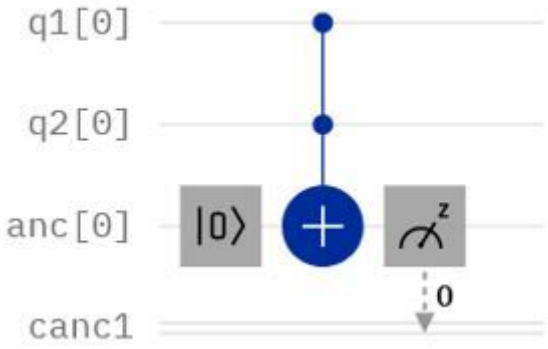


Figure 7

Conditional X-gate with *ctrl_state* parameters

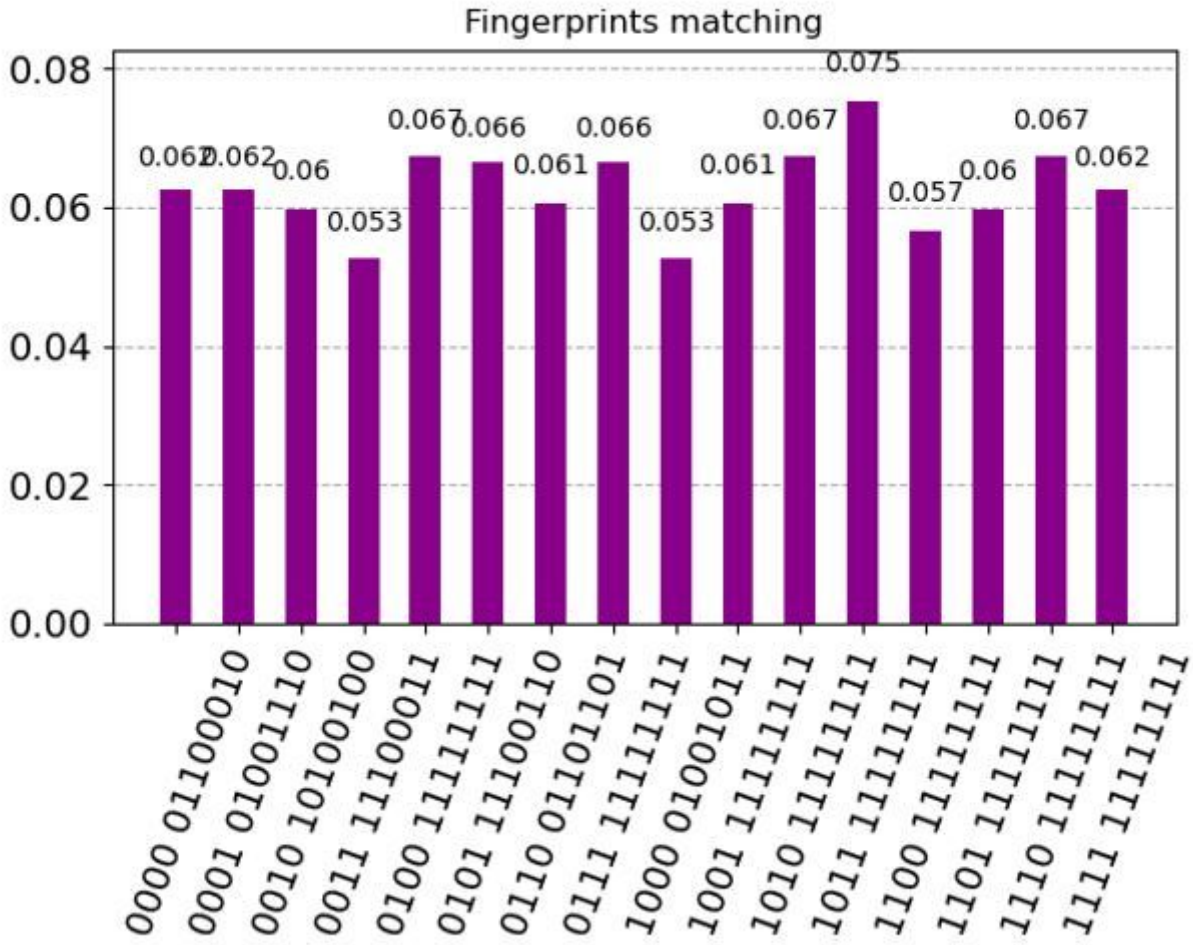


Figure 8

The outputs of the matching circuit

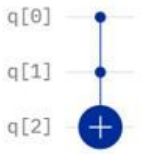
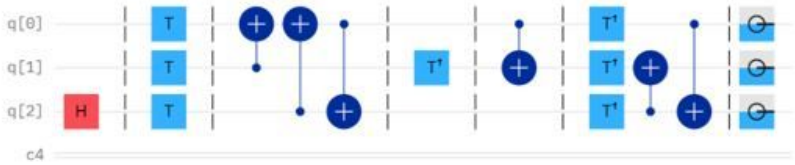
	Hadamard H-gate = $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$
	X-gate = $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$
  3-qubit Toffoli gate decomposition (no ancilla) Hadamard gate (H), 6 C X-gates, T = exp $(\frac{i\pi\sigma_z}{8})$ and T† gates	

Figure 9

Gates used in the quantum matching circuit.