International Journal for Housing Science and Its Applications
Publish August 6, 2025. Volume 46, Issue 3 Pages 8472-8480

https,//doi.org/10.70517/ijhsa463724

Commercial Cryptographic Security Design for Face Recognition System Based on Improved Quantum Encryption Algorithm

Hai Huang[1,*]
[1] School of Economics and Business Administration, Chongqing University, Chongqing, 400044, China
Corresponding authors: (e-mail: cquhuanghai888@163.com).

Abstract The wide application of face recognition technology in the commercial field puts forward higher requirements for the protection of users' personal privacy data during the recognition process as well as the accuracy of recognition. This paper explains the basic conceptual content of quantum bits and quantum logic gates. Under the theoretical framework, a three-valued XHZ encryption scheme in three-valued quantum states is proposed to complete the construction and optimization of the quantum encryption algorithm. Using the designed quantum encryption algorithm, the public key is generated in the server based on the face feature data, and the private key is used to decrypt in the client, so as to construct the face recognition system based on the quantum encryption algorithm. In the evaluation experiment, the fastest encryption average time is only 2.465ms, and the shortest calculation time for face similarity is only 4.577ms, which shows that the designed system can fully meet the technical requirements of identity authentication while safeguarding the user's personal privacy and security.

Index Terms quantum encryption algorithm, face recognition system, personal privacy security, three-valued XHZ encryption scheme

I. Introduction

Face recognition system with face recognition technology as the core, is an emerging biometric technology, is today's international scientific and technological field of research and development of highly sophisticated technology [1], [2]. It widely adopts the regional feature analysis algorithm, integrates the computer image processing technology and biostatistics principles in one, uses the computer image processing technology to extract the portrait feature points from the video, and analyzes and establishes the mathematical model by using the principles of biostatistics, which has a broad application in the design of commercial cryptographic security [3]-[6].

With the rapid development of information technology, data has become an important part of the core competitiveness of enterprises [7], [8]. In the era of digitization, data security has become a focus of attention for enterprises [9]. In order to protect enterprise information security and improve the information system protection ability, the commercial password application construction has become an urgent task, and commercial passwords, as an important means to ensure data security, its security is directly related to the information security of enterprises [10]-[12]. While commercial cryptographic security is mainly faced with the security of encryption algorithms, key management, system integration, personnel security awareness and other aspects of the challenge, the application of face recognition system is of great significance for enterprises to maintain data security [13]-[15].

At present, many enterprises, institutions and public places have begun to introduce face recognition technology for security design [16]. Face recognition technology has been widely used in remote security control and security control within the entrance and exit places. Compared with traditional keys or combination locks, face recognition technology is more secure, and also more convenient and faster [17]-[19].

This paper firstly describes the conceptual content of quantum bits in quantum computing, as well as the matrix representation and line construction of quantum logic gates, which serve as the theoretical basis for the study of this paper. Secondly, it elaborates the design process and improvement and optimization ideas of the three-valued XHZ encryption scheme in the three-valued quantum state, and forms the encryption algorithm. Based on the proposed quantum encryption algorithm, the registration process and authentication process are successively designed according to the security requirements of users' personal privacy in face recognition. Finally, the performance of the encryption algorithm is tested by comparing the encryption effect and checking the information entropy. The overall cryptographic performance of the designed face recognition system is evaluated by setting up

a comparison with similar encryption schemes in terms of public and private key generation, as well as face similarity calculation. Test the system throughput and web request response time to analyze the system operational performance.

II. Face Recognition System Based on Quantum Encryption Algorithm

II. A.Basic Concepts of Quantum Computing

II. A. 1) Quantum bits

It is well known that a bit is the basic concept of classical information and has a state of 0 or 1. Like a classical bit, a quantum bit is the basis of quantum information and has two possible states $|0\rangle$ and $|1\rangle$, where $|\ \rangle$ is the Dirac symbol, and $|0\rangle$ and $|1\rangle$ correspond to the classical bits 0 and 1, respectively. The difference between classical and quantum bits is that the state of a quantum bit can be a linear combination of $|0\rangle$ and $|1\rangle$, often referred to as a quantum superposition state. This can be written as equation (1):

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

where $\alpha, \beta \in C$, $|\alpha|^2 + |\beta|^2 = 1$. α and β denote the probability amplitude of the $|\varphi\rangle$ state on $|0\rangle$ and $|1\rangle$, respectively (It can be seen that quantum bits have a higher information capacity compared to classical bits.). And $|0\rangle$ and $|1\rangle$ can also be expressed in vector form, $|0\rangle = (1,0)$ and $|1\rangle = (0,1)$. The quantum bit can then also be written as equation (2):

$$|\varphi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{2}$$

II. A. 2) Quantum Logic Gates

Similar to the way classical computers are built from circuits containing lines or logic gates, quantum computers are built from quantum circuits containing lines and elementary quantum gates to carry and manipulate quantum information. Single quantum bit gates (e.g., $Pauli-X$, $Pauli-Z$, $Pauli-Y$, and H) are the simplest form of quantum gates, and they can be expressed as a 2×2 matrix as shown in Equation (3):

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{3}$$

Multi-quantum bit gates are also important units in quantum circuits. The more common two quantum bit gates are such as CNOT gate, swap gate and CZ. where the CNOT gate has two input quantum bits called control bit and target bit. If the control ratio is ad hoc 0, the target bit will be unchanged. If the control ratio is ad hoc to 1, the target bit will be flipped.The matrix form and quantum lines of the CNOT gate are shown in Fig. 1.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

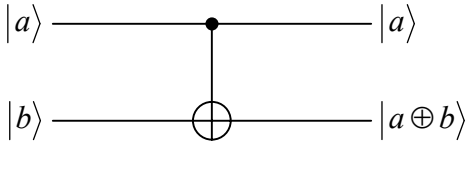


Figure 1: The matrix form and quantum circuit of the CNOT gate

A swap gate, also called a switch gate, inputs two quantum bits and serves to swap the states of the two quantum bits. For example, $|0\rangle|1\rangle \xrightarrow{swap} |1\rangle|0\rangle$. Its matrix form with quantum lines is shown in Figure 2.

$$swap = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

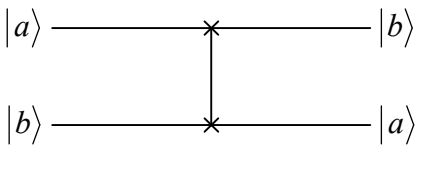


Figure 2: The matrix form and quantum circuit of the swap gate

The CZ gate, also known as a control phase gate, has a control bit and a target bit like the CNOT gate, and if the control ratio ad hoc is 0, the target bit phase is not flipped. Otherwise, it flips.The matrix form and quantum lines of the CZ gate are shown in Fig. 3.

$$CZ=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&-1\end{bmatrix}$$

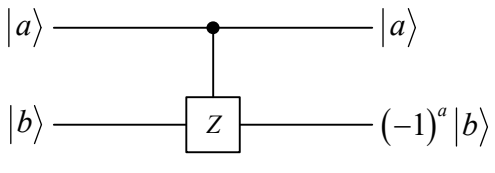


Figure 3: The matrix form and quantum circuit of the CZ gate

In contrast, a three-quantum-bit gate, such as a Toffoli gate, has three input bits and three output bits: two of the quantum-bit bits are control bits that are unaffected by the action of the Toffoli gate. The third bit is the target bit, which is flipped if both control bits are set to 1, otherwise unchanged.

II. B.Three-valued XHZ encryption scheme

With reference to the quantum one-at-a-time encryption scheme, combined with the three-valued quantum information processing technology, the three-valued XHZ encryption scheme can be designed. Let the you-transform operation used in the encryption scheme be written as equation (4):

$$U_k \in \left\{ X^{\alpha} H^{\beta} Z^{\delta} \mid \alpha,\beta,\delta \in \{0,1,2\}^n \right\} \tag{4}$$

where X , H , and Z are all single-valued triple quantum gates, $X^{\alpha}=\otimes_{i=1}^{n} X^{(\alpha(i))}$, $H^{\beta}=\otimes_{i=1}^{n} H^{(\beta(i))}$, $Z^{\delta}=\otimes_{i=1}^{n} Z^{(\delta(i))}$, the probability of selecting U_k is $p_k = 1/3^{3n}$, and U_k is a $3^n \times 3^n$ You matrix, whose encryption process is represented as equation (5):

$$\left|\psi_c\right\rangle = U_k \left|\varphi\right\rangle = X^{\alpha} H^{\beta} Z^{\delta} \left|\varphi_m\right\rangle \tag{5}$$

And its decryption process is expressed as equation (6):

$$\begin{aligned}\left|\psi_m\right\rangle &= U_k^{\dagger}\left|\psi_c\right\rangle = U_k^{\dagger} X^{\alpha} H^{\beta} Z^{\delta}\left|\varphi_m\right\rangle \\ &= Z^{\delta} H^{\beta} X^{\alpha} X^{\alpha} H^{\beta} Z^{\delta}\left|\varphi_m\right\rangle = \left|\varphi_m\right\rangle\end{aligned} \tag{6}$$

Now, give an explanation of the security of the three-valued XHZ encryption scheme. For an encryption scheme $\{U_k, p_k\}$ for quantum bits, its ciphertext state ρ_c (density matrix representation) satisfies equation (7):

$$\rho_c = \sum_k p_k U_k \sigma_m U_k^{\dagger} = \frac{1}{2^n} I_2 \tag{7}$$

where σ_m denotes the density matrix form of the plaintext quantum state. Equation (7) shows that the encryption scheme $\{U_k, p_k\}$ is perfectly secure. This also means that all plaintext states are mapped to the same ciphertext state through the encryption operator U_k : the maximal mixed state. Moreover, on the inner product space, the encryption operator U_k forms a set of standard orthogonal bases. For a three-valued quantum state encryption scheme $\left\{U_k', p_k'\right\}$, assume that for any $A, B \in \left\{U_k' \mid k = 1,\cdots,3^n\right\}$, there are there is equation (8) holds:

$$tr(AB^{\dagger}) = tr(B^{\dagger}A) = \begin{cases} 0, & A \neq B \\ 3^n, & A = B \end{cases} \tag{8}$$

Then the density operators A and B are said to be orthogonal.

In this way, the encryption operator U_k' can form a set of standard orthogonal bases on the inner product space. But unfortunately, the encryption operator U_k in the three-valued XHZ encryption scheme is partially orthogonal and does not satisfy completeness. So, the three-valued XHZ encryption scheme is not perfectly secure. Two

encryption processes of singleton three-valued quantum states are given to illustrate the partial orthogonality of the encryption operator U_k. One is when $A = X^{(1)}H^{(1)}X$ and $B = X^{(1)}H^{(0)}X^{(1)}$ with equation (9):

$$tr(AB^{\dagger}) = 1.9142 \neq 0 \tag{9}$$

Then A and B are not orthogonal. Another one is when $A = X^{(1)}H^{(2)}X^{(0)}$ and $B = X^{(0)}H^{(0)}X^{(1)}$ with equation (10):

$$tr(AB^{\dagger}) = 0 \tag{10}$$

Then A and B are orthogonal.

Although the three-valued XHZ encryption scheme does not satisfy the message-theoretic security defined by Shannon, it is still highly secure and convenient in practical applications. First, the key used for each encryption is different, similar to the quantum one-at-a-time model. Second, the keys are unconditionally secure because the QKD protocol is used to distribute the keys. Moreover, these received quantum bits are easily converted to binary strings of numbers for storage, avoiding the use of quantum memory and facilitating experimental implementation. As a final point, the basic principles of quantum mechanics, such as the principle of inability to measure and the non-clonability theorem, these techniques are significantly better than traditional methods in protecting private information.

In fact, there are many improvements that can be made to the three-valued XHZ encryption scheme. For example, the combination of the QKD protocol to generate sequences of numbers containing 0, 1, and 2, and the construction of the encryption operator allows this encryption algorithm to achieve message-theoretic security. With these improvements, it is hoped to obtain a perfectly secure encryption scheme for three-valued quantum states.

II. C.Face Recognition Program Design

II. C. 1) Registration process

In the registration process, first, a registration request is initiated by the user to the client, and the client receives and responds to the request, extracts the user's face features through the camera device, and obtains a collection of face multidimensional feature vectors as in equation (11):

$$A = \{V_1, V_2, \cdots, V_n\} \tag{11}$$

Then, FaceNet face feature extraction is performed on A to obtain a single 128-dimensional biometric feature vector Q. Next, the client passes the extracted biometric feature vector Q to the cloud server, which receives Q and calculates the Euclidean distance by comparing Q with the feature vector of its own server template as in equation (12):

$$M = \{Q_1, Q_2, \cdots, Q_n\} \tag{12}$$

Determines whether it is in its own server template M. If it is present, return to the client that the registration failed. Otherwise, return to the client that the registration was successful and store the Q in M.

II. C. 2) Certification process

In the authentication process, an authentication request is initiated by the user to the client, and the client receives and responds to the request, extracts the user's face features through the camera device, and obtains a set of multidimensional feature vectors of the face as in equation (13):

$$A = \{V_1, V_2, \cdots, V_n\} \tag{13}$$

FaceNet face feature extraction is performed on A to obtain a single 128-dimensional biometric feature vector Q. The client generates the public key public_key for encryption, the private key secret_key for decryption, and the computational auxiliary keys relin_key and gaolois_key. encryptor is generated based on the public key, and decryptor and calculator evaluator are generated based on the private key. At the same time, a cloud server generates a 128-dimensional vector of random numbers R, each element in R is a randomly generated floating point number between $[0.8,1]$, and the cloud server passes R to the client.

The client receives the vector of random numbers R from the cloud server and performs the Hadamard product of Q and R to obtain a new vector N. Encrypt N with the public key to get the encrypted vector N_enc. Send N_enc and the public key to the cloud server at the same time.

After receiving N_enc with the public key, the cloud server encrypts all the vectors of its template as in Eq. (14) using that public key:

$$M = \{Q_1, Q_2, \cdots, Q_n\} \tag{14}$$

The encrypted template is obtained as in equation (15):

$$M\_enc = \{Q_1\_enc, Q_2\_enc, \cdots, Q_n\_enc\} \tag{15}$$

Calculate the Euclidean distance squared by homomorphizing all encrypted vectors in M_enc with N_enc respectively to get n ciphertexts Euclidean distance squared as in equation (16):

$$D\_enc = \{dis(N\_enc, Q_1\_enc), dis(N\_enc, Q_2\_enc), \cdots, dis(N\_enc, Q_n\_enc)\} \tag{16}$$

Pass D_enc to the client.

The client receives D_enc and decrypts it using the private key to get n Euclidean distance squared as in equation (17):

$$D = \{dis(N, Q_1), dis(N, Q_2), \cdots, dis(N, Q_n)\} \tag{17}$$

Find the smallest of these Euclidean distance squares $D_{\min}$, and compare it to the pre-set threshold τ. If $D_{\min} < \tau$, the authentication succeeds. Otherwise, the authentication fails and the authentication result is returned to the user.

The detailed face feature authentication process is shown in Fig. 4.

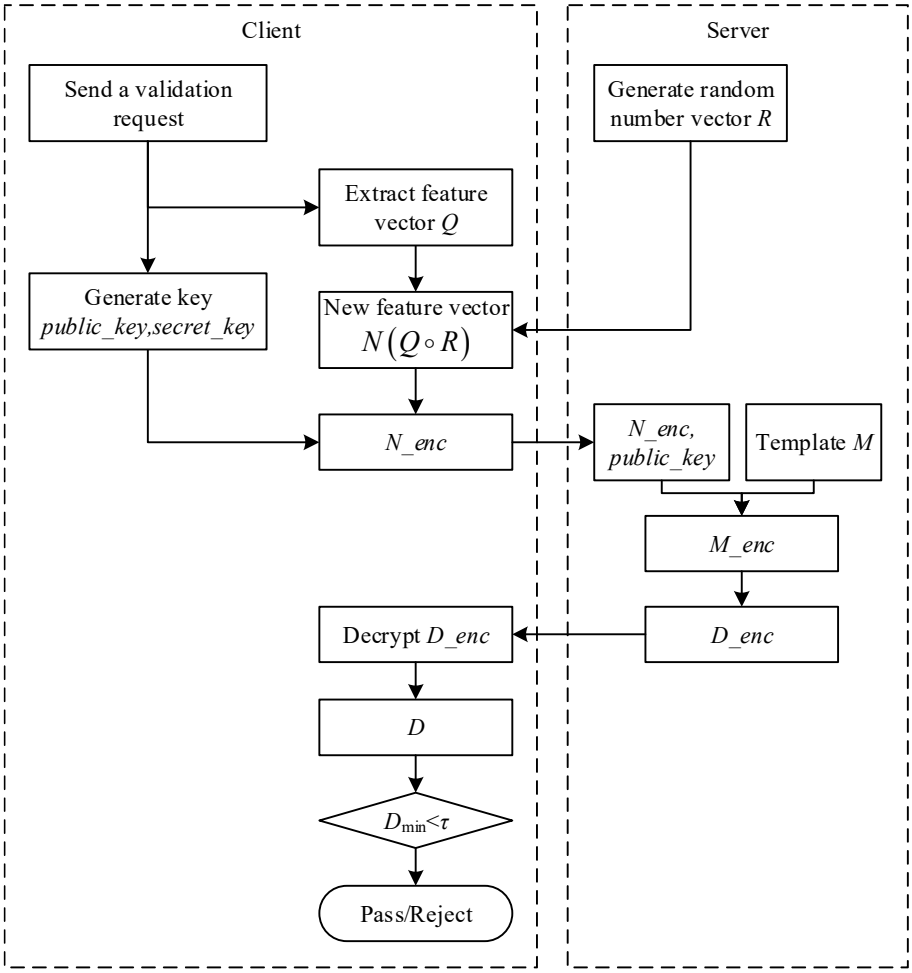


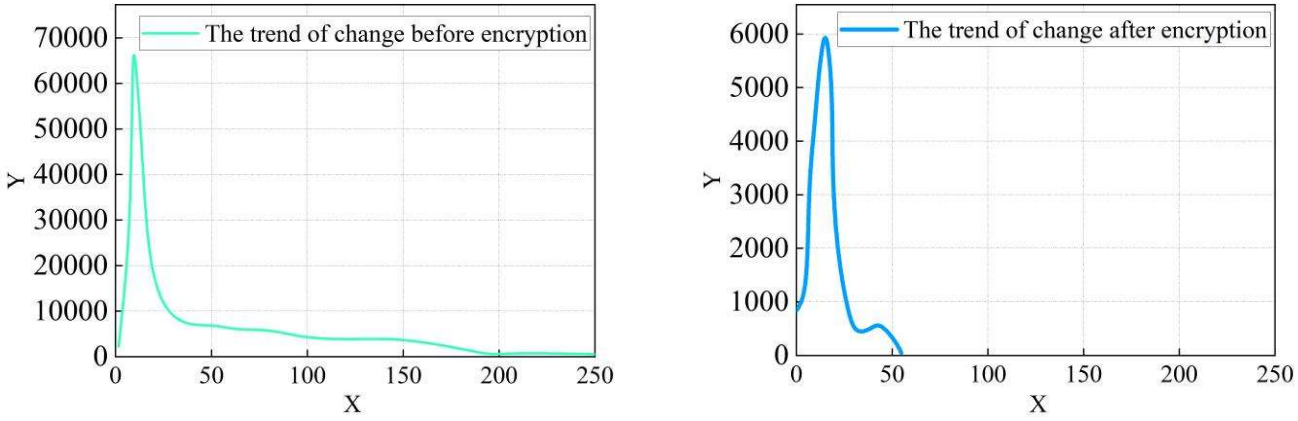
Figure 4: Face feature authentication process

III. Performance Evaluation and Application Inspection of Face Recognition System

III. A. Performance testing of encryption algorithms

III. A. 1) Comparison test of encryption effect

The quantum encryption algorithm designed in this paper compares the effect of an original map before and after encryption in Fig. 5, after the image encryption operation, the high-frequency capability part (>6000) is intercepted by the algorithm, while the low-frequency part is retained, but accordingly a layer of mask is added on the image, so as to make the original image information is effectively preserved.



(a) Before encryption (b) Aftre encryption

Figure 5: Comparison of the effects of the original image before and after encryption

III. A. 2) Information entropy test

In this paper, information entropy is used to measure the uncertainty of chaotic sequences. When the distribution of sequence values is equal probability distribution, i.e., the probability of each value between [0,288] is 1/289, it has the maximum entropy lg289=9bit.The information entropy results are shown in Table 1.The information entropy of the sequences E and F is gradually close to the expected value of 9, and with the increase of the length of the sequences, the information entropy is closer to the expected value, indicating that this paper's encryption algorithm has a strong average uncertainty, high degree of chaos, good randomness and no obvious statistical information. The expected value shows that the encryption algorithm in this paper has strong average uncertainty, high degree of chaos, good randomness, and no obvious statistical information.

Table 1: Test results of information entropy of chaotic sequences of different lengths

Sequence length	Entropy of Sequence E	Entropy of Sequence F
1000	5.3858	5.4938
2000	6.8275	7.1168
4000	7.0478	9.0189
8000	7.4751	7.5799
10000	8.1084	6.9271
20000	8.7196	8.1882

III. B. Cryptographic operational performance of the system

In this section, the classical BFV encryption scheme is chosen as a comparison to unfold the comparative analysis with the encryption scheme based on quantum encryption algorithm in terms of public and private key generation performance, overall encryption performance, and face similarity.

III. B. 1) Public and Private Key Generation Tests

The size of the public-private key file of the encryption algorithm is highly correlated with the polynomial mode number and the parameters of the ciphertext coefficient modes, which determines the upper limit of the total bit length of the ciphertext coefficient modes. Therefore, while the number of polynomial modes is determined, the size of the public-private key file is also determined. The larger the number of polynomial modes, the larger the ciphertext is, despite the higher security of the scheme. Therefore, in the test, the parameters of polynomial modulus number are set to 4096 and 8192.In addition, the generation time of the public-private key file is highly

correlated with the polynomial modulus number. Comparing the performance of this paper's scheme and the BFV scheme in terms of public and private key file size and average generation time is shown in Table 2. Under the condition of polynomial modulus parameter of 4096, the average time of generating public and private keys in this paper's scheme is 0.092ms and 0.039ms, respectively, which is faster than that of the average generation time of the BFV scheme. Under the polynomial mode parameter condition of 8192, the average time of generating public and private keys of this scheme is still better than that of the BFV scheme, and the difference is up to 0.003ms.

Table 2: Public and private key file size and average generation time

Program	Textual		BFV	
Polynomial modulo degree	4096	8192	4096	8192
Public Key Size (byle)	184368	643120	184368	643120
Private key size(byle)	86047	315423	86047	315423
Average generation time of public key (ms)	0.092	0.189	0.093	0.199
Average generation time of Private key (ms)	0.039	0.141	0.041	0.144
Count the number of times	100			

III. B. 2) Encryption tests

The maximum dimension of a single plaintext (the number of slots in the plaintext) is the same as the size of the polynomial modulus number, in order to maximize the use of storage space and improve the ability of batch processing, multiple face feature vectors can be encoded into the same plaintext, take the polynomial modulus number of 8192 as an example in this paper's scheme, the number of slots in the plaintext is also 8192, and the dimensionality of a single face feature vector is 1024, so that 16 face feature vectors can be encoded into the same plaintext simultaneously. Therefore, 16 face feature vectors can be encoded into the same plaintext at the same time. After generating the public and private key files, 8000 pairs of faces are encrypted respectively. The performance results of the two schemes on (P1) the number of face feature integers contained in a single name text, (P2) the average encryption time (ms), (P3) the average encryption time of a single encryption (ms), (P4) the size of encrypted file (byle), (P5) the size of a single file (byle), and (P6) the average size of an unencrypted file (byle), a total of six parameters, are shown in Table 3. Where the performance results of the (P2) encryption average time (ms), the fastest scheme in this paper takes only 2.465ms, which is faster than the BFV scheme by 0.458ms.

Table 3: Encryption time statistics and file size before and after encryption

Program	Textual		BFV	
Polynomial modulo degree	4096	8192	4096	8196
Number of plaintext slots	4096	8192	2048	4096
P1	16	32	4	8
P2	2.465	6.891	2.923	8.793
P3	0.212	0.326	0.65	1.002
P4	143522	536738	143522	536738
P5	18738	40116	35135	67890
P6	5260			

III. B. 3) Face similarity calculation time

The computation time comparison of the two schemes for face similarity under different parameters is shown in Table 4, although in the batch computation average time performance, this paper's scheme is slightly inferior to the BFV scheme. However, in the pairwise computation average time, the time required by this paper's scheme is much lower than that of the BFV scheme, and the shortest time required is only 4.577ms under the condition of polynomial mode count of 4096.

III. C. Performance analysis of the system

In this section, the performance test of the system is carried out, the test content is the system throughput and the response time of the web page request, the system test simulates the number of users is 800, and the simulation process is started at the same time in 1 second, the test time is 1 minute 30 seconds. The result of system throughput is shown in Fig. 6, and the response time of web page request is shown in Fig. 7. In the case of 800 users, the throughput is 130 per second on average, and the average response time is 284 ms. It shows that the system in this paper achieves the expected results, and it can run safely and smoothly.

Table 4: The calculation time of face similarity under different parameters

Program	Polynomial modulo degree	Batch calculation average time (ms)	A pair of calculated average times (ms)
Unencrypted			0.628
Textual	4096	15.55	4.577
	8192	62.756	7.011
BFV	4096	15.23	5.831
	8192	62.755	10.205

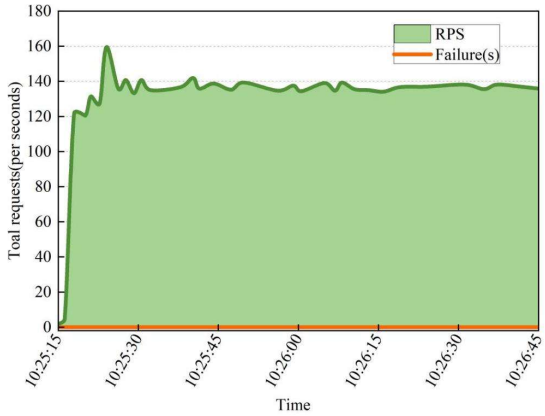


Figure 6: Throughput of system

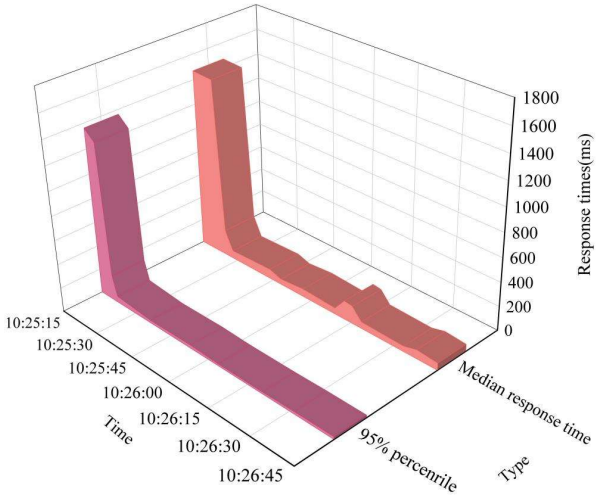


Figure 7: The response time performance of web page requests

IV. Conclusion

In this paper, with the support of quantum encryption algorithm, a face recognition system with both security and practicality is designed to provide an effective technical reference for its application in the commercial field.

The encryption algorithm of the designed face recognition system has a strong average uncertainty, a high degree of chaos and good randomness. Comparing with similar encryption schemes, the average time for generating public and private keys under the condition of polynomial modulus count of 4096 is 0.092ms and 0.039ms, respectively, and the average time for encryption is only 2.465ms, and the shortest time for the calculation of face similarity is only 4.577ms. In the overall performance performance, the throughput is an average of 30 per second, and the average response time is 284ms.

References

[1] Kortli, Y., Jridi, M., Al Falou, A., & Atri, M. (2020). Face recognition systems: A survey. Sensors, 20(2), 342.

[2] Oloyede, M. O., Hancke, G. P., & Myburgh, H. C. (2020). A review on face recognition systems: recent approaches and challenges. Multimedia Tools and Applications, 79(37), 27891-27922.

[3] Zhao, X., & Wei, C. (2017, August). A real-time face recognition system based on the improved LBPH algorithm. In 2017 IEEE 2nd international conference on signal and image processing (ICSIP) (pp. 72-76). IEEE.
[4] Sharma, S., Bhatt, M., & Sharma, P. (2020, June). Face recognition system using machine learning algorithm. In 2020 5th International Conference on Communication and Electronics Systems (ICCES) (pp. 1162-1168). IEEE.
[5] Salama AbdELminaam, D., Almansori, A. M., Taha, M., & Badr, E. (2020). A deep facial recognition system using computational intelligent algorithms. Plos one, 15(12), e0242269.
[6] Ramachandra, R., & Busch, C. (2017). Presentation attack detection methods for face recognition systems: A comprehensive survey. ACM Computing Surveys (CSUR), 50(1), 1-37.
[7] Gürdür, D., El-khoury, J., & Nyberg, M. (2019). Methodology for linked enterprise data quality assessment through information visualizations. Journal of Industrial Information Integration, 15, 191-200.
[8] Desai, P. B., & Goel, O. (2025). Scalable Data Pipelines for Enterprise Data Analytics. International Journal of Research in All Subjects in Multi Languages, 13(1), 174.
[9] Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: causes, challenges, prevention, and future directions. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 7(5), e1211.
[10] Kolenko, V., Nakonechna, V., & Anosova, Y. (2021). Commercial secret of the enterprise protection based on steganographic algorithms. Visnyk KrNU, 1, 59-65.
[11] Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. Computers & Security, 61, 130-141.
[12] Sriramya, P., & Karthika, R. A. (2015). Providing password security by salted password hashing using bcrypt algorithm. ARPN journal of engineering and applied sciences, 10(13), 5551-5556.
[13] Knierem, B., Zhang, X., Levine, P., Breitinger, F., & Baggili, I. (2017). An overview of the usage of default passwords. Computer Science, 1, 6-2018.
[14] Zhang, Y., Zhang, X., Zhao, D., He, M., & Jiang, X. (2024, January). Research on Commercial Password Design and Unified Password Monitoring Platform Based on Hash Function. In Proceedings of the 2024 3rd International Conference on Cryptography, Network Security and Communication Technology (pp. 47-51).
[15] Gürfidan, R. (2023). Analyzing User Passwords Worldwide in Terms of Cyber Threats. International Journal of Engineering and Innovative Research, 5(3), 201-210.
[16] Al Zaabi, S., & Zamri, R. (2022). ENHANCING PHYSICAL SECURITY PERFORMANCE IN THE OIL AND GAS INDUSTRIES THROUGH THE INTEGRATION OF FACIAL RECOGNITION TECHNOLOGY. Journal of Engineering and Technology (JET), 13(1), 45-72.
[17] Bein, A. S., & Williams, A. (2023). Development of deep learning algorithms for improved facial recognition in security applications. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 5(1), 19-23.
[18] Cifaldi, G. (2022). Government surveillance and facial recognition system in the context of modern technologies and security challenges. Soc. & Soc. Work Rev., 6, 93.
[19] Pati, B. (2020). ISS: Intelligent Security System Using Facial Recognition. Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019, Volume 1, 1198, 96.