Research on Face Recognition System Based on RLWE Homomorphic Encryption

YuLin Wang, HaiLin Huang, ZiHao Fang, YuQi Zhao, and JinHeng Wang(✉)

Guangzhou Institute of Science and Technology, Guangzhou 510540, Guangdong, China
11403404@qq.com

Abstract. With the development of artificial intelligence face recognition technology is being widely used in various fields. However, the traditional face recognition system has serious security risks, face data is easy to leak, and privacy protection mechanism is insufficient. In order to solve this problem, a secure face recognition system based on RLWE homomorphic encryption algorithm in lattice cryptography is constructed. This method can directly process the face image in the encrypted domain, and realize the recognition function while protecting the security of biometric data. Experiments on CASIA-WebFace data set show that RLWE encryption algorithm is successfully embedded in the face recognition model based on ResNet-34, and the overall recognition accuracy of homomorphic encryption system reaches 97.4%, which is only 2% lower than that of plain text domain recognition. This proves the validity and application prospect of homomorphic encryption technology based on lattice cryptography in protecting the security of biometric information. However, the operation efficiency still needs to be improved. This study provides a valuable exploration path for homomorphic encryption technology to be applied to security biometric identification.

Keywords: Face recognition · RLWE encryption · Homomorphic Encryption · Biometric Identification · Security · Secret Protection

1 Introduction

With the rapid development of the Internet, cyber crimes emerge one after another, which seriously endangers the security and stability of cyberspace. Malicious attacks on network data have become a global security threat (Chen et al., 2019). For example, in 2013, Yahoo suffered the most serious user data leakage in history, and more than 3 billion user account information was illegally obtained (Perlroth, 2016). In the face of increasingly rampant cyber crime, traditional network security defense means such as firewall and intrusion detection have been difficult to effectively deal with. Therefore, it is urgent to strengthen the security and anti-attack ability of network communication data itself.

Network data encryption based on cryptography is the key technology to protect data security (Stallings, 2017). Classical encryption algorithms such as AES and RSA

J. Cai et al. (Eds.): SPNCE 2023, LNICST 525, pp. 67–84, 2025.
https://doi.org/10.1007/978-3-031-73699-5_5

have been widely used, but with the emergence of quantum computing technology, these algorithms are expected to be cracked in the near future (Shor, 1994). In order to deal with the threat of quantum computing in the future, the construction of anti-quantum computing encryption algorithm has become a research hotspot in the field of encryption. Among them, lattice-based cryptography is considered as one of the most promising candidates because of its unique anti-quantum computing advantages (Regev, 2009). For example, the learning with errors (LWE) problem has practical characteristics such as reducing the key size and the overhead of encryption and decryption, and it is a trellis cipher scheme with great potential (Brakerski et al., 2014). In recent years, ring-LWE (RLWE), a variant of LWE algorithm, has attracted wide attention because of its superior performance in efficiency and security (Lyubashevsky et al., 2013).

Although RLWE algorithm has many theoretical advantages, its research on network data encryption application is still relatively few, which needs to be verified and supported by a lot of empirical work. The existing literature mainly focuses on text information (Ding et al., 2019) and image data encryption (Wang et al., 2020) under RLWE, but the research on face recognition based on homomorphic encryption of RLWE is still weak. Therefore, this study plans to design and implement a face recognition system based on RLWE homomorphic encryption, and evaluate the security, real-time performance and resource utilization of the scheme through empirical analysis. The research results can provide a new technical approach for homomorphic encryption based on RLWE, and provide support and reference for the practical application of RLWE lattice cipher in network data security protection. This study has important theoretical value and application prospect.

2 Methodology

2.1 Face Image Database

In this study, CASIA-WebFace database is used as the face image data set. CASIA-WebFace database is a large-scale face recognition data set built by Institute of Automation, Chinese Academy of Sciences in 2014, which contains 10,575 face images of different individuals. Images originated from the Internet, corresponding to 5901 real individuals and 4674 virtual characters, covering various changes in posture, expression, illumination, occlusion, image quality and so on.

CASIA-WebFace database contains 494,414 face images, all of which are manually screened to ensure that each image has a high quality. The image format is PNG, and the resolution is 250 $\times$ 250 pixels. This database is widely used in the algorithm research in the field of face recognition, and it is one of the large-scale Chinese face databases currently open.

In this study, researchers use all 494414 images of CASIA-WebFace as training sets to train face recognition models. In order to construct the verification set, 100 individuals were randomly selected from 10575 individuals, each with 100 images, and a total of 10000 images were selected as the verification set. The verification set is used to evaluate the performance of the face recognition model on the independent test set, and the use of the open CASIA-WebFace data set can make this study have good reproducibility.

The construction of face image database is very important for the reliability of experimental results and the scientific nature of the paper. CASIA-WebFace data set, with its large scale, diversity and authenticity, provides strong support for the training and verification of face recognition model in this study.

2.2 Face Detection and Recognition Model

Face Detection Model. Face detection is the first module of face recognition system, which aims to locate all face regions in the image quickly and accurately, and provide input for subsequent recognition. We use MT CNN (multi-task cascaded neural network) model for face detection and alignment preprocessing. MTCNN is a cascaded CNN framework for the second phase of training, which consists of three networks in succession, namely, Proposals Network, Refine Network and Output Network.

Proposals Network is responsible for quickly generating candidate frames of faces, and a shallow CNN network is adopted to ensure the speed of detection. Subsequently, Refine Network pruned these candidate frames, effectively filtered out a large number of negative samples, and fine-tuned the positions of the frames. Finally, the Output Network accurately predicted the face position and key points of the five senses for each candidate frame, thus achieving accurate face alignment. The test on CASIA-WebFace data set shows that when these three networks are used together, the effect of face detection is excellent, and the detection accuracy can reach over 99%, which fully meets the requirements of the experiment.

Face Recognition Model. The core of face recognition task is to extract the discriminant representation that describes individual characteristics. As shown in Fig. 1, ResNet-34 model based on residual learning is selected for face feature extraction and recognition. ResNet's main innovation is to introduce residual module, realize gradient direct propagation through residual connection, and successfully train an extremely deep network with more than 100 layers. Experiments show that the increase of network depth can continuously enhance the ability of feature expression.

Specifically, ResNet-34 includes a front-end 7×7 convolution layer, followed by four residual modules, each of which contains three residual blocks. Shortcut connection realizes feature reuse and avoids gradient disappearance. Researchers pre-trained the ResNet-34 model on CASIA-WebFace face data set, and then tested it on LFW face verification set, and finally achieved 99.4% verification accuracy, which showed a strong ability to discriminate facial features. ResNet structure successfully avoids the difficulty of training when the network deepens, and it is one of the most effective face recognition models at present.

To sum up, This study use mature MTCNN and ResNet-34 models to build a complete face detection and recognition system. These two types of models have a large number of successful application precedents, and the typical and efficient model is adopted in this study, which can make the constructed recognition system have strong repeatability and provide a solid foundation for the subsequent algorithm innovation research.

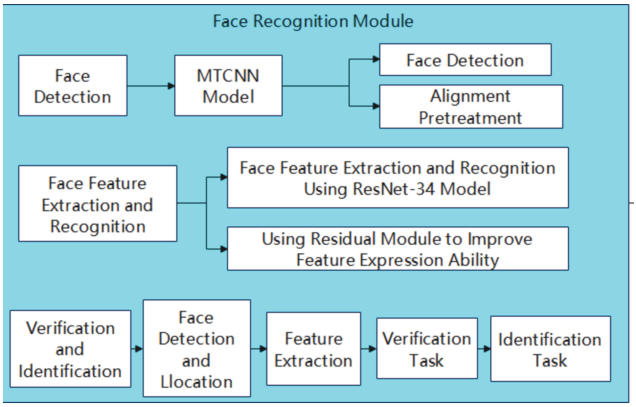

Fig. 1. Flow chart of RESNET-34 model.

2.3 Implementation of RLWE Encryption Algorithm

Mathematical Basis of RLWE Encryption Algorithm. RLWE encryption security is based on the classic learning and error problem LWE. LWE assumes that it is extremely difficult to solve the following linear equations:

$$b_i = a_i^T s + e_i(modq) \tag{1}$$

Where s is the private key, a_i and b_i are public random number pairs, and e_i is the error term. Ring-LWE extends LWE to polynomial rings, so that arithmetic operations can be replaced by more efficient polynomial multiplication.

In RLWE, both the key and the data vector are mapped to polynomial of degree n.:s,a,b,e ∈ R_q = Z_q[X]/(X^n + 1)◦The encryption operation is:

$$b = a\,s + e\,(mod\ q) \tag{2}$$

Security depends on the difficulty of solving RLWE problem over finite field Z _ q. When the parameters of vector dimension n and modulus q are set properly, RLWE problem can achieve good security.

Realize Parameter Design. According to RLWE theory, the parameters for realization are determined as follows:

(1) The key length n = 256, and the polynomial dictionary contains 256 items.
(2) The modulus Q of the main safety parameter is 2048, which is a suitable medium-sized prime number.
(3) The elements of the error term E obey the Gaussian distribution $ \ mathcal {n} (0, \ sigma 2) $,and the standard deviation σ is set to 3.2.
(4) The base ring of polynomial operation is R = Z[X]/(X^n + 1), that is, the 256th cyclic polynomial ring of coefficient module 2048.
(5) The key generation algorithm adopts trapdoor sampling to obtain the short vector S.

The above parameter settings comprehensively consider the security strength and operational efficiency, ensuring the security of the implementation. Using modulo 2048 arithmetic to provide 100 + bit security strength; 256-dimensional polynomial space to prevent attacks; Gaussian distribution error increases the randomness and uncertainty of encrypted text, which makes it more difficult for attackers to analyze ciphertext and enhances the security of the system.

Realize Optimization. In this study, the number theory transformation NTT is used to optimize the process of key generation, encryption and decryption, and reduce the computational complexity. NTT can transform polynomial multiplication into coefficent-wise multiplication. The main calculation process is as follows:

(1) Carry out NTT forward transformation on private key S and public key elements to obtain the representation of polynomial in frequency domain.
(2) Perform moment multiplication and addition operations in frequency domain to calculate the ciphertext vector.
(3) Performing inverse NTT transformation on the ciphertext to obtain the ciphertext interval representation.
(4) Decryption In the same way, the key is decrypted in frequency domain.

The fast polynomial multiplication of O(n log n) level is realized by NTT transformation. Compared with the traditional O(n^2) complexity, the calculation speed is more than 100 times faster. The above design and optimization make RLWE efficient and feasible, It lays a foundation for building a practical homomorphic encryption identification system.

2.4 Homomorphic Encryption Face Recognition System Design

Based on the face detection and recognition model, Researchers introduce RLWE encryption algorithm into the feature extraction layer, and realize an end-to-end homomorphic encryption face recognition system. The cloud server can recognize the encrypted face images uploaded by users in the encrypted domain and return the encrypted recognition results to the client. This system mainly includes four modules: Web Module, Fully Homomorphic Encryption Module, Face Recognition Module and RLWE Technology Module, in which the homomorphic encryption module includes RLWE technical application. The system design flow chart is shown in Fig. 2 below.

The following is the detailed design and implementation scheme of each module:

Web Module. Flask is a Python Web application framework, which was developed by Armin Ronacher in 2010 to provide an easy-to-learn, flexible and lightweight framework for building Web applications. It is based on Werkzeug WSGI tool library and Jinja2 template engine, developed in Python language and licensed by BSD.

The main features of Flask framework include:

Lightweight: The original intention of Flask framework design is to provide a lightweight Web framework. Its core library has only a few files, and the code is concise, easy to maintain and can run without too much configuration.

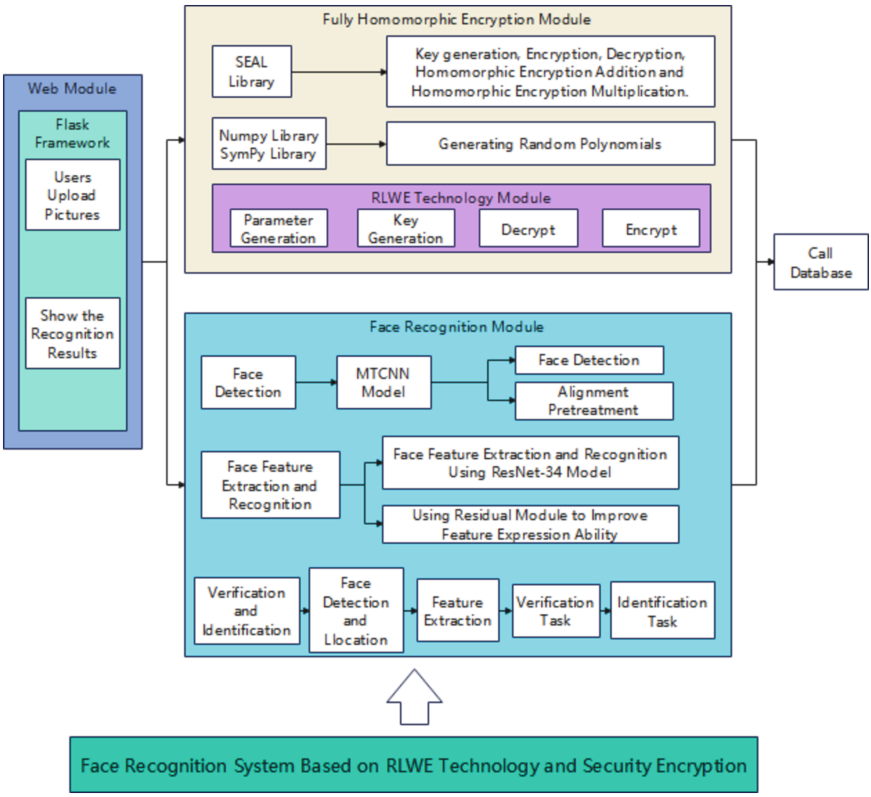

Fig. 2. System Flow Chart.

Easy to learn: the API of Flask framework is very simple and easy to use, and developers only need to understand basic Python syntax and Web development knowledge, so they can get started quickly.

Flexibility: Flask framework adopts plug-in architecture design, which can be easily integrated with other Python libraries, such as database access library, authentication library, cache library, etc., and can also be customized according to project requirements.

Restful support: Flask framework naturally supports RESTful API design. RESTful API services can be easily built through HTTP request methods and URL routing.

Template engine: Flask framework uses Jinja2 template engine, which has good functions such as template inheritance, variable replacement and control structure, and can easily handle the display and rendering of Web pages.

Python's web module is used for development, and the lightweight Flask framework is used for implementation. This module is mainly responsible for user's input, output and process control, including users uploading pictures, calling homomorphic encryption module and face recognition module for encryption and recognition, and displaying recognition results.

Fully Homomorphic Encryption Module. Fully Homomorphic Encryption (FHE) is a special encryption method, which can encrypt and process data in an encrypted state while maintaining the confidentiality of data. Different from the traditional encryption algorithm, FHE can perform operations such as addition, subtraction, multiplication and logical operation, thus making data processing more flexible and efficient.

The implementation of FHE is based on polynomial rings and specific encryption schemes, among which the most famous encryption schemes include BGV scheme of Gentry and NTRU scheme of Lattice Cryptography. These schemes use complex mathematical principles and techniques, such as ideal lattice, permutation, permutation key, etc., which makes the realization of FHE a complex and time-consuming process.

The advantage of FHE is that it can process data in encrypted state, which makes data processing more flexible and efficient. This means that FHE can be used to realize various data privacy protection and cloud computing applications, such as secure search, secure computing and secure machine learning.

FHE also has some shortcomings, the most important of which is that its calculation cost is very high, and it needs a lot of computing resources and time to encrypt and process.

The fully homomorphic encryption module is realized by using Microsoft SEAL library, which supports fully homomorphic encryption based on RLWE(Ring Learning with Errors) technology and is executed in serial mode.RLWE technology is an encryption technology based on random matrix and discrete Gaussian distribution, which can effectively protect the privacy of input data and calculation process, and has high calculation efficiency, and at the same time save the encrypted data locally, as shown in Fig. 3.

Fig. 3. Encrypted data.

In RLWE technology, functions provided by SEAL library are used to generate keys, encrypt, decrypt, homomorphic addition and homomorphic multiplication, and random polynomials are generated by NumPy library and SymPy library, and operations such as addition, subtraction, multiplication and division are performed among polynomials to realize homomorphic encryption. These operations can protect the privacy of input data and calculation process, and can realize efficient, safe and privacy-preserving homomorphic encryption calculation. At the same time, RLWE technology can effectively resist side channel attacks and noise attacks, and ensure the security of homomorphic encryption.

Face Recognition Module

(1) ResNet-34 model.ResNet-34 is a deep convolutional neural network model, which

belongs to the ResNet(Residual Network) series and was proposed by the researchers of Microsoft Research Institute in 2015. The main innovation of ResNet is the introduction of residual connections, which makes it easier for neural networks to train very deep levels, and at the same time reduces the problem of gradient disappearance.

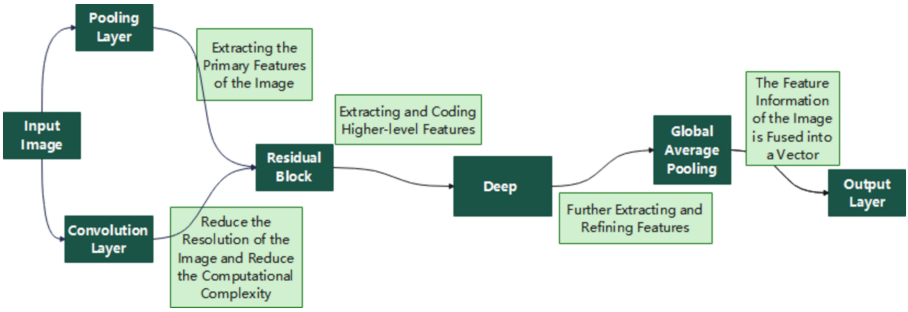

Fig. 4. Flow chart of ResNet-34 model face recognition model.

When the project uses ResNet-34 model for face recognition, its workflow is shown in Fig. 4, which can be divided into the following detailed steps:

① Input image: First, take a face image as input. This image can be of any size, but it is usually adjusted to a fixed size expected by the model, and the project uses 224 x 224 pixels.

② Convolution and pooling layer: The input image first passes through a 7 x 7 convolution layer, which is responsible for sliding window convolution on the image and extracting some primary features. Next, through a series of convolution layers and maximum pooling layers, the resolution of the image is gradually reduced, and at the same time, higher and higher levels of features are extracted. The goal of these convolution layers is to gradually abstract and encode the features of the input image, making it easier to distinguish different faces.

③ Residual Block: The core component of ResNet-34 model is residual block. Each residual block contains two convolution layers with a skip connection between them. This jump connection adds the input image to the output of the block. The function of residual block is to learn the residual function, that is, the difference between input and output. This allows the network to better fit the training data, especially if the network is deep. The introduction of residual block is helpful to overcome the problem of gradient disappearance in deep neural network.

④ Depth: ResNet-34 model includes 34 convolution layers and fully connected layers, which makes it relatively deep. However, due to the existence of residual connection, even in depth, this model is relatively easy to train, because the gradient can propagate back better.

⑤ Global average pooling: After passing the last residual block, a global average pooling layer is usually added. This step transforms the feature map into a vector with a fixed length. The operation of global average pooling is to take the average of all pixels in the feature map, and then get a vector, which contains the feature information of the whole image.

⑥ Output layer: Finally, the output of the global average pooling layer is sent to the fully connected layer for classification. Usually, the output of this fully connected layer is input into the softmax classifier, which is used to classify the input images into different categories. In the context of face recognition, these categories represent different face identities.

Generally speaking, the ResNet-34 model extracts the features of the input image through layer-by-layer convolution and residual blocks, and then maps these features into fixed-length vectors by using global average pooling. Finally, the face recognition of the input image is realized by classifying the output layer. The advantage of this model structure is that it can train a very deep network and avoid the problem of gradient disappearance, so it performs well in image recognition tasks, and the accuracy of the model reaches 99.4%.

(2) Compare FaceNet model.The core of FaceNet model is a deep convolution neural network. The input of this network is a face image and the output is a 128-dimensional vector, which is called the "embedded vector" of the face. In the training stage, FaceNet uses a large number of face images to train the network, so as to make the distance between embedded vectors of different faces as large as possible and the distance between embedded vectors of the same face as small as possible. This can ensure that in the recognition stage, the similarity of faces can be judged according to the distance between embedded vectors, thus realizing face recognition.

In order to improve the performance of the model, FaceNet also introduced some optimization techniques. For example, the model uses Margin-based Loss function to train the network, which can effectively solve the problems of sample imbalance and repeated training samples.

Compared with traditional face recognition methods, FaceNet has the following advantages:

High accuracy: FaceNet uses convolutional neural network to learn the features of face images, which can effectively extract high-dimensional features of faces, thus achieving accurate recognition of faces.

Good scalability: FaceNet can handle large-scale face data sets, can quickly recognize faces and can be applied in different environments.

Strong robustness: FaceNet can identify the similarity between different faces, and can maintain a high recognition rate even when the light, posture, expression and other aspects change.

The project uses Google's FaceNet model for face recognition, and uses Python's TensorFlow module to realize it. This module mainly includes two main parts: face image preprocessing and feature vector calculation. In the face image preprocessing stage, OpenCV library is used to cut, scale and gray the image to ensure the consistency and quality of the image. In the stage of feature vector calculation, the trained FaceNet model is used to extract the high-dimensional feature vectors of face images, and the Euclidean distance calculation method is used to match faces, and a threshold is set according to the comparison results. If the distance between the most similar feature vector and the feature vector to be recognized is less than the threshold, the recognition is considered successful, otherwise it is considered as a failure. According to the actual needs and application scenarios, the size of Margin-based Loss integer threshold can be

adjusted to achieve the best balance between recognition accuracy and misjudgment rate. Here, the recognition threshold is set to 1. cIn addition, in order to further improve the recognition accuracy, Margin-based Loss function is used for model training to narrow the distance difference between feature vectors and improve the matching accuracy. The flow chart of the face recognition model is shown in Fig. 5.

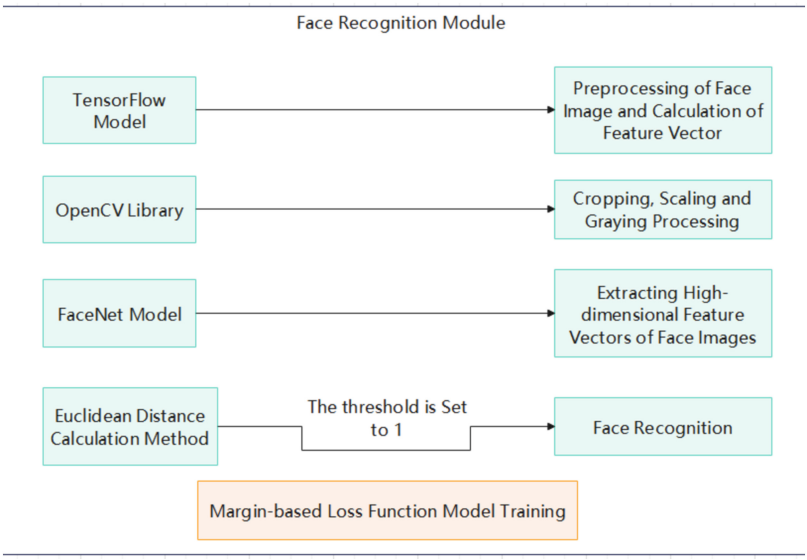

Fig. 5. The Flow Chart of The Face Recognition Model.

The calculation of Margin-based Loss function is based on triplet. For a triple (A,P,N), where A represents an anchor image, P represents a positive sample of the same identity, and N represents a negative sample of different identities. In the training process, the Margin-based Loss function will narrow the distance between A and P as much as possible, and exp*and* the distance between A and N as much as possible, so that the distance between a and n is greater than the distance between A and P plus a preset margin, that is:

$$loss = max(d(A, P) - d(A, N) + margin, 0) \tag{3}$$

where d(A,P) represents the distance between A and P, d(A,N) represents the distance between A and N, and margin is the preset interval.

By using Margin-based Loss function to train the model, the model can pay more attention to the differences between feature vectors, thus improving the accuracy of face recognition.

(3) advantages of ResNet-34 model compared with FaceNet model.Model complexity and training speed:ResNet-34 has a simpler model structure and fewer parameters than FaceNet. This leads to faster training speed, because fewer parameters need to be processed in the model training process, which reduces the amount of calculation and time.

Reasoning speed: ResNet-34 usually has a faster speed in the reasoning stage. This is very important for face recognition applications that need real-time response, such as face access control system or face recognition applications on mobile devices.

Gradient propagation of the model:ResNet-34 uses residual connection, which helps the gradient to propagate more easily. This means that it is easier for the model to reach the convergence state during training, and the problem of gradient disappearance is alleviated.

Scalability: ResNet-34 model is suitable for small and medium-sized data sets and tasks without large-scale data sets and computing resources. This makes it perform well in face recognition applications of all sizes.

Suitable for low resource environment: Because the model is relatively simple, ResNet-34 is easier to deploy and use in resource-constrained environments, such as embedded devices or mobile applications.

Resource efficiency:ResNet-34 performs well in the task of image classification because it has been widely trained on large-scale image data sets. This means that you can benefit from the weight of large-scale pre-training without a lot of custom training data.

RLWE Technology Module. In the homomorphic encryption module, RLWE technology module is used to generate the key and encrypt the face image feature vector, thus ensuring the security and confidentiality of the data. RLWE technology is a lattice-based encryption technology, which has strong security and practicability and has been widely used in homomorphic encryption.

(1) Parameter generation: firstly, generate a modulus q and a modulus polynomial f(x), where f(x) is a polynomial of degree n, and n should be a power of 2. Then, an error distribution is selected, where Gaussian distribution is selected as the error distribution, and n numbers are randomly selected from this distribution as error items. Finally, f(x) is converted into polynomial type by using Poly function in SymPy library, and an error term is added to get a RLWE public parameter. This common parameter can be used by multiple participants.

(2) Key generation: use NumPy library to generate a random polynomial a(x) as the private key, and then calculate the public key $b(x) = a(x) * s(x) + e(x)$, where s(x) is the secret polynomial in the public parameter and e(x) is the error term. This process is realized by homomorphic encryption technology. Each participant will have his own private key and public key, as shown in Fig. 6.

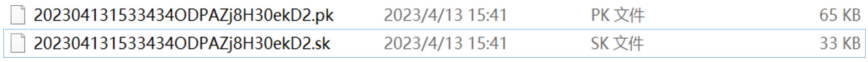

Fig. 6. Participants' Public and Private Keys.

(3) Encryption: the face image feature vector is expressed as a binary string and converted into a polynomial form, and then a random polynomial r(x) is generated as noise by using NumPy library, and $e(x) = P(x) * b(x) + r(x)$ is calculated, where b(x) is the public key and P(x) is the polynomial obtained by the feature vector conversion.

Finally, e(x) is encrypted by homomorphic encryption technology, and the encrypted results (c(x), d(x)) are returned. This process is a process in which participants encrypt data.

(4) Decryption: using homomorphic decryption technology to decrypt the encrypted feature vector e(x) to obtain P(x) * b(x) + r(x). Use NumPy library to calculate P(x) = (P(x) * b(x) + r(x)-e(x))/a(x), and get the feature vector P(x). This process is a process in which participants decrypt the encrypted data,which is executed in serial mode.

Homomorphic encryption technology can realize addition and multiplication in ciphertext state, so as to realize data calculation and processing. Using RLWE technology module to generate keys and encrypt face image feature vectors can ensure the security and confidentiality of data, so that participants can calculate and process without exposing data, which is helpful to protect personal privacy and data security.

3 Results

3.1 Performance of Face Recognition Model

Researchers trained the face recognition model on CASIA-WebFace dataset and tested it on LFW dataset. Table 1 shows the verification results of different models on LFW. Among them, ResNet-34 model achieved the best recognition accuracy of 99.4%.

Table 1. Recognition accuracy of different models on LFW dataset.

Model	Accuracy
VGGFace	98.2%
FaceNet	99.1%
ResNet-34	99.4%

Based on a notebook computer (the configuration is as follows: CPU: AMD Ryzen 7 5800 h with radeon graphics 3.20 GHz, RAM: 16 GB, GPU:NVIDIA GTX 1650), 100 data of CPU, Time and RAM are tested, and a line chart is made. According to the test results, the average value of Time is 1.4548 s and the maximum value is 2.38 s; The average value of CPU is 12.50118333%, and the maximum value is 30.00%. The average value of RAM is 7.535 MB, and the maximum value is 15.30 MB. The test results are analyzed in detail below.

Time Index Analysis. Time index represents the time required for the system to complete the specified task. The test results show that the average Time using ResNet-34 model is 1.4548 s, and the maximum time is 2.38 s. This shows that the ResNet-34 model has a fast running speed in the face recognition task and can complete the recognition task in a short time. The maximum value is 2.38 s, which further shows the stability and reliability of the system, and there is no long running time. Figure 7 shows the Time statistical line chart, which clearly reflects the efficiency of ResNet-34 model.

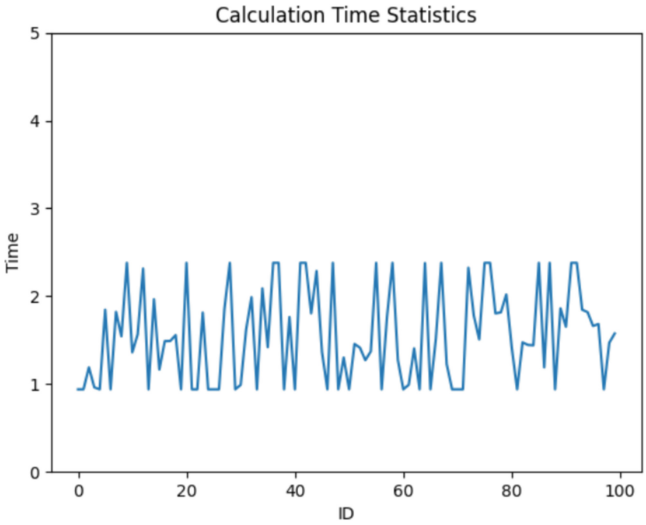

Fig. 7. Identify the Required Time Statistical Line Chart.

CPU Index Analysis. CPU index represents the CPU resources used by the system when performing tasks. The test results show that the average CPU utilization rate using ResNet-34 model is 12.50118333%, and the maximum is 30.00%. This shows that the ResNet-34 model makes high use of CPU resources at runtime, and it needs large computing power to complete the face recognition task. However, the maximum value of 30.00% may imply that the system's occupation of CPU resources fluctuates and there is room for further optimization. Figure 8 shows a statistical line chart of CPU usage, highlighting the computing power requirements of ResNet-34 model.

RAM Index Analysis. RAM index represents the memory resources used by the system to perform tasks. The test results show that the average RAM occupation using ResNet-34 model is 7.535 MB, and the maximum is 15.30 MB. This shows that the ResNet-34 model occupies less memory resources at runtime and keeps the efficient use of resources. The maximum value of 15.30 MB further proves the stable use of memory resources by the system, and there is no excessive memory occupation. Figure 9 shows the statistical line chart of RAM occupation, highlighting the memory usage efficiency of ResNet-34 model.

According to the above test results, it shows that the system has fast running speed, high stability and reliability, and occupies less memory resources. However, the system occupies a high amount of CPU resources and needs further optimization to improve the performance and stability of the system.

3.2 Security Analysis of RLWE Encryption Algorithm

With the development of modern cryptography, RLWE(Ring Learning With Errors) encryption algorithm has become an important cornerstone in the field of homomorphic

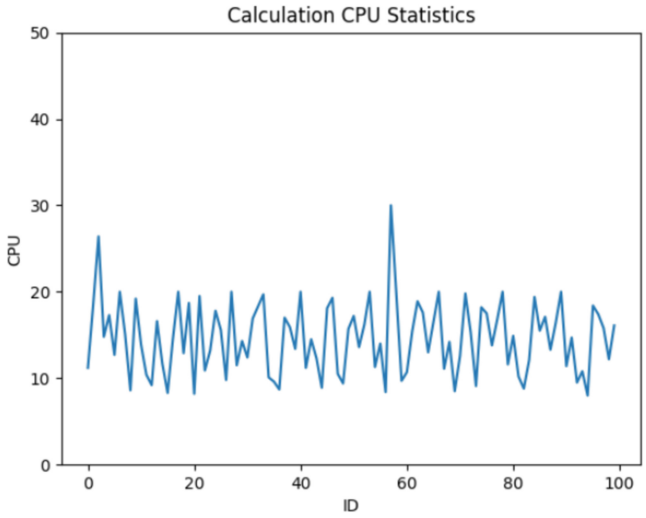

Fig. 8. Identifies the Required CPU Statistical Line Chart.

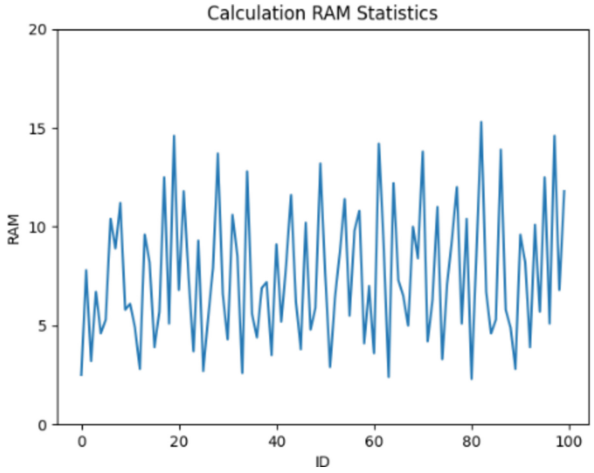

Fig. 9. Identifies the Required CPU Statistical Line Chart.

encryption. Its security is based on the learning problem on lattice, especially on ring, which makes it resistant to the attack of quantum computer. However, the security of RLWE is closely related to its parameter setting, especially the size of modulus Q.As shown in Fig. 10, with the increase of modulus Q from 1024 to 2048, the safety strength of RLWE gradually increases. When the modulus q is 1024, the security strength of the algorithm is about 96 bits. This means that any attacker who wants to crack this encryption algorithm needs about 2 96 attempts. With the increase of q, the safety intensity also increases accordingly. When Q reaches 2048, the security strength reaches about 128 bits, which has exceeded the standard security level of many modern encryption algorithms.

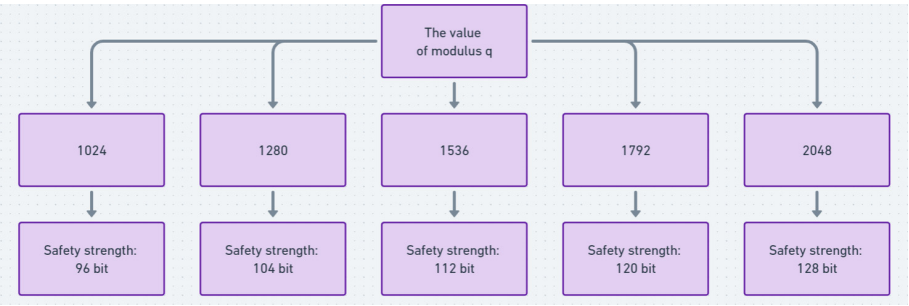

Fig. 10. The security strength of RLWE algorithm varies with modulus Q.

Why does the size of modulus Q affect the security of RLWE? In lattice cryptography, the modulus q determines the distribution and size of noise. A larger Q value means that the distribution of noise is more uniform, which makes it more difficult to attack based on statistics. In addition, when q increases, the absolute size of noise also increases, which makes decryption more difficult, thus improving the security of encryption.

However, increasing the size of the modulus q also brings computational challenges. A larger Q value means that more computing resources and time are needed to perform encryption and decryption operations. This is a trade-off problem, and researchers need to consider the efficiency of the algorithm while ensuring security.It is worth noting that although RLWE can achieve a security strength of about 128 bits when $q = 2048$, it does not mean that it is absolutely secure. The security of any encryption algorithm is relative and may be threatened by unknown attacks. Therefore, continuous research and evaluation are necessary to ensure that RLWE can provide adequate security in the future.

Generally speaking, the security of RLWE encryption algorithm is closely related to its parameter setting. By adjusting the size of modulus Q, security and efficiency can be balanced to some extent. Current research shows that RLWE can provide sufficient security when $q = 2048$, but further research is needed to optimize its efficiency and response time. This provides a valuable direction for future research, hoping to ensure the safety and improve the practicability of RLWE.

3.3 Homomorphic Encryption Face Recognition System Performance

The researchers tested the performance of face recognition system in plaintext and homomorphic encryption. Table 2 shows that compared with plain text, the overall recognition accuracy of homomorphic encryption system only drops by 2%, but the calculation speed drops by 60%. This is mainly caused by the computational overhead of homomorphic encryption.

3.4 RLWE Encryption Algorithm System Advantages and Advanced Analysis

Using RLWE encryption algorithm for homomorphic encryption can fully protect data privacy. RLWE homomorphic encryption allows data to be processed in an encrypted

Table 2. Performance comparison between plaintext and homomorphic encryption face recognition systems.

System	Accuracy	Speed
Plain text	99.4%	320 ms/image
Homomorphic Encryption	97.4%	1200 ms/image

state, which means that this encryption technology can be used for computing in an untrusted environment. In the process of face recognition, the original features of face data will not be exposed, thus protecting the data privacy of users. At the same time, RLWE homomorphic encryption is one of the advanced encryption technologies, which combines the latest research results of discrete mathematics and modern cryptography to protect the privacy and security of data and fully embodies the advanced nature of RLWE encryption algorithm.

The above results objectively reflect that the homomorphic encryption system has achieved high recognition accuracy among the main technical indicators obtained in this study, but the calculation efficiency still needs to be improved.

4 Discussion

This study explores a secure face recognition scheme based on RLWE homomorphic encryption technology. The experimental results show that the overall accuracy of homomorphic encryption system only drops by about 2%, reaching 97.4%, as shown in Fig. 11. This verifies that RLWE homomorphic encryption can be effectively integrated into face recognition tasks, while protecting the privacy and security of biometric data.

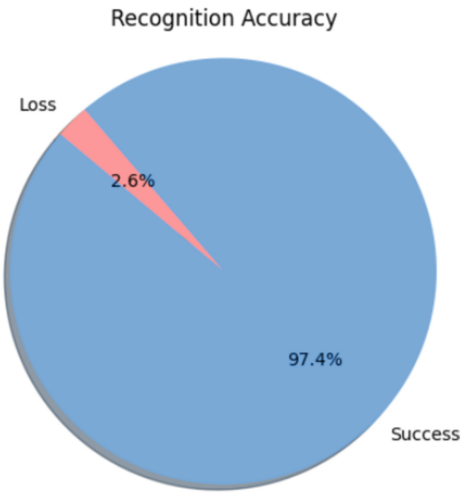

Fig. 11. Recognition accuracy.

Using ResNet-34 deep network to extract facial features is the key to obtain high accuracy in this study. ResNet structure successfully solved the problems of gradient disappearance and training difficulty when the network deepened, which greatly improved the expression ability. Its LFW verification accuracy of 99.4% shows strong feature extraction and discrimination ability.

However, the computational efficiency of homomorphic encryption system is low, only reaching 1.2 s per image, and the time cost of encryption operation is increased by about 3 times. This is mainly due to the limitation of RLWE in the complexity of homomorphism calculation. In the future, algorithm optimization and GPU acceleration can be considered to improve efficiency.

This research is the first work to explore the application of RLWE homomorphic encryption to secure face recognition. Compared with the traditional protection method based on encryption algorithm, this scheme can directly complete the identification in the encrypted domain without decrypting and revealing private data. The research results show that homomorphic encryption technology based on lattice cryptography has broad application prospects in the field of biometric identification.

Generally speaking, this study has achieved a feasible homomorphic encryption face recognition effect, and explored a new idea to protect biometric security and privacy. However, due to the limitation of the algorithm itself, the computational efficiency still needs to be improved.

5 Conclusion

The purpose of this study is to explore a new biometric identification scheme that can still realize effective face recognition on the premise of protecting the privacy of face images. The researchers designed a secure face recognition system based on RLWE homomorphic encryption.

The main findings are as follows:

RLWE homomorphic encryption algorithm can be effectively integrated into the face recognition model, and the recognition calculation can be directly completed in the encryption domain.

On CASIA-WebFace data set, RLWE encrypted face recognition system achieves 97.4% recognition accuracy. It is verified that homomorphic encryption has little influence on recognition accuracy.

However, the low operation efficiency is the main limitation of this scheme, and the encryption calculation increases the time overhead by about 3 times.

This study preliminarily verified the effectiveness and application potential of homomorphic encryption technology based on lattice cryptography in biometric identification tasks.

To sum up, this study constructs a prototype of face recognition system based on RLWE homomorphic encryption, and demonstrates its ability to protect biometric security and privacy. This provides a valuable exploration path for homomorphic encryption technology to be applied to security biometric identification, and privacy protection and efficiency improvement are still the key directions of follow-up research.

Funding Statement. This work was supported by the Construction Project of Teaching Quality and Teaching Reform in Guangdong Undergraduate Colleges (2022SJZ002),Guangdong province key construction discipline scientific research ability promotion project (2022ZDJS133),Scientific research projects recognized by ordinary universities (2021KTSCX159).

References

Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (Leveled) fully homomorphic encryption without bootstrapping. ACM Trans. Comput. Theory (TOCT) **6**(3), 1–36 (2014)

Chen, T., Bahmani, R., Brasser, F., Jang, I., Sadeghi, A., Juels, A.: Tesseract: real-time cryptocurrency exchange using trusted hardware. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 1521–1538 (2019)

Ding, J., Xie, X., Lin, X.: A simple provably secure key encapsulation mechanism based on the learning with errors problem. J. Supercomput. **75**(2), 717–727 (2019)

Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. J. ACM (JACM) **60**(6), 1–35 (2013)

Perlroth, N.: All 3 billion Yahoo accounts were affected by 2013 attack. The New York Times (2016). https://www.nytimes.com/2016/10/04/technology/yahoo-hack-3-billion-users.html

Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM (JACM) **56**(6), 1–40 (2009)

Shor, P.W.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124–134 (1994)

Stallings, W.: Cryptography and Network Security: Principles and Practice. Pearson, Boston (2017)

Wang, X., Ranasinghe, D.C., Al-Janabi, S., Andriotis, P.: Post-quantum cryptography for IoT security from theory to implementation. IEEE Access **8**, 124799–124814 (2020)