Fingerprint Based Bank Locker Security System Using Ring-LWE Cryptography

Rex.V[1], Mrs.Sona.G M.E.[2]
[1]Dept of of Computer Science and Engineering
[2]Assistant Professor, Dept of of Computer Science and Engineering
[1, 2] Government College of Engineering, Tirunelveli, Tamil Nadu, India

Abstract- *Biometric (Fingerprint) systems are replacing traditional password based authentication systems. Fingerprint based biometrics are improving system security and accuracy. This work provides a highly secure fingerprint authentication system using Ring- Learning With Errors(LWE) cryptography for operating the bank safety lockers. To extract the fingerprint features a delay-optimized high accuracy method is proposed to extract the features from fingerprint images. Then the Ring-LWE cryptography scheme using low-latency Number Theoretic Transform (NTT) polynomial multiplications is implemented to improve the Ring-LWE encryption and decryption time. As per observation it shows that, the processing time of the fingerprint authentication systems is considerably reduced, and the fingerprint data are effectively protected.*

Keywords- Authentication, cryptography, encryption, fingerprint features, ring-LWE.

I. INTRODUCTION

1.1 CRYPTOGRAPHY

Cryptography is a method of protecting information and communication by using codes, so that it can only be read and processed by those for whom the information is intended. The word cryptography means that the hiding of information from the unauthorized users. There are four primary functions of cryptography

- Privacy/confidentiality
- Authentication
- Integrity
- Non-repudiation.

1.2.FINGERPRINT AUTHENTICATION

A person's behavioral or physiological characteristics can be identified using the Biometric Techniques. Person's behavioral characteristics (voice, signature etc) can be changed with time. But their physiological characteristics like fingerprint, retina etc. can never be changed. Biometric process is efficient to distinguish the highly secure authorization process among an unauthorized and a genuine person.

1.2.1 Importance of Fingerprint

Fingerprint is an interesting and unique characteristic of the human body, because the Fingerprints can identify the person uniquely and it doesn't changes from birth to death.Even twins fingerprints do not match. As the fingerprint posses persistent and uniqueness property it has been developed in many areas like UID Card, Passport, Criminal Data, etc.

1.2.2 Fingerprint Acquisition Techniques

Fingerprints Acquisition Techniques are categorized into three types

Live Scan Fingerprints

Live Scan Fingerprints are Impressed Fingerprints sometimes referred to as Plastic Prints. The clearance of Fingerprint image available is better than Patent Fingerprint. It can be retrieved using fingerprint scanner, Clay, Wax, and Paint.

Latent Fingerprints

Latent fingerprints is invisible to the eye directly and requires enhancement technique and instruments to check. surface basic powder and chemical techniques are used to extract the fingerprints from surface.

Patent Fingerprints

Patent Fingerprint is also referred to as the Visible Fingerprint. It is formed intentionally by person to prove their identity. At recognition stage, it is still use to record presence

of person. Patent Fingerprints can be formed by blood, grease, ink, or dirt etc.

1.2.3 Fingerprint Classification

The fingerprint classification images are very significant in order to speed up the recognition process in which fingerprints are classified according their shapes of minutiae ridges. Populations around the world have different types of fingerprint patterns that will be discussed are as mentioned in

Figure 1.1

Arch Pattern

The Arch is a type of ridge that starts from one side to the other by forming a wave pattern in the middle. There are two Arch Pattern styles called Plain Arch and Tent Arch.

Loop Pattern

Loop is the special property of fingerprint image. There are many types of loops such as Right Loop, Left Loop, Double Loop, Left Pocket Loop, Right Pocket Loop Pattern. Generally, Right and Left loops are found in fingerprint of human.

Figure 1.1 Fingerprint classification

Whorl Pattern

Whorl Pattern is an pattern in which human fingerprint have at least one ridge that allow to make a complete circuit. Types of Whorl pattern are Plain Whorl, Double Loop Whorl, Central Pocket Loop Whorl, and Accidental Whorl.

1.2.4 Minutiae features

Features of fingerprint ridges, called minutiae, include

- Ridge ending: The immediate end of a ridge
- Bifurcation: A single ridge dividing into two ridges
- Pore: Human pore
- Island Or Dot: A single ridge inside a small ridge or ended ridge that are not have a path to all other ridges
- Bridge Or Crossover: A short ridge that runs between two parallel ridges
- Delta: A Y-shaped ridge meeting
- Core: A circle in the ridge pattern

Figure 1.2 Minutia Features

1.3 BANK SAFETY LOCKERS

A bank safety locker is used for depositing valuables like gold, jewellery and important documents . It can be hired by individuals, firms, trusts, companies etc. Locker comes in different sizes such as small, medium, large and extra-large. Rent of each locker varies on the basis of size. In spite of all these shortcomings and malfunctions these systems are still prevailing; however, the biometric or fingerprint authentication based recognition is the most efficient and reliable solution for stringent security. Fingerprint authentication is one of the reliable biometric techniques owing to the uniqueness and stability that fingerprints can compared to other biometrics.

1.4 OBJECTIVE

This project aims to provide a complete biometric (fingerprint) based authentication for operating the bank safety lockers. The fingerprint based bank locker system is the replacement of the traditional bank locker system that uses keys. The fingerprint authenticated bank locker system is safe as well as easy to use and maintain.

II. RELATED WORK

Li and Kot [10] proposed a fingerprint authentication system, which uses data hiding and data embedding

technology to embed private user data into a fingerprint template. In this paper a novel data hiding scheme was proposed. In the stage of system registration, a user's identity is hidden into his fingerprint template. The template with hidden identity is stored in a database for succeeding authentication. Since fingerprint information is usually sparse binary images, this technology does not cause visible changes and is not perceived by the vision of the user or attackers. Therefore, during the process of registration, data embedding method does not cause obvious anomalies. During the phase of authentication, query fingerprint is used to match the template stored in an online database. Then, the query identity is compared to the identity hidden in the template for the purpose of authenticating an genuine person. Due to the proposed data hiding scheme, attackers will not be able to obtain the identity and original fingerprint of the stolen templates. However, the security of this method was not proved.but this system achieved a very high accuracy with high-level usability. The EER showed in testing is 0%.But the efficiency of this fingerprint recognition system is not provided.Although it supports a low level of privacy, it does not satisfy the criterion of security.

Li and Kot proposed another fingerprint authentication system in [5]. General fingerprint authentication systems, only need one fingerprint. But in this system, two fingerprint images are collected. The directional features of one fingerprint are combined with the minutiae of another fingerprint to form a composite fingerprint template. Thus, when the template saved in a server database is stolen, a single true fingerprint cannot be exposed, and the user can replace the fingerprint to generate a new composite template. That is perfectly consistent with the criteria of non invertibility and revocability. The experimental results show that the system is excellent in terms of accuracy and achieves an EER of 0.4%. System efficiency is not mentioned in this paper. In addition, this system has a high level of usability, a low level of security and a high level of privacy.

III. PROPOSED WORK

In this work, a fingerprint authentication system using ring-LWE cryptography, the post-quantum cryptosystem, is introduced. By applying novel fingerprint feature extraction and NTT polynomial multiplication in the proposed ring-LWE cryptography-based fingerprint authentication system, the total processing time of the proposed system is much faster than other systems. Additionally, the encrypted data generated by the proposed system is more secure than the obtained results from existing system.

Main contributions of the proposed system are as follows:

- A novel NTT polynomial multiplication scheme is presented by removing bit-reverse operations in conventional NTT multiplication to speed up the time of polynomial ring multiplication;
- An optimal minutiae based algorithm for fingerprint features extraction to reduce processing time and increase accuracy;
- The ring-LWE cryptography system is designed using the proposed NTT polynomial multiplication approach to enhance the encryption and decryption time;
- A fingerprint authentication system is developed using fingerprint-features extraction method and the proposed NTT multiplication based ring-LWE cryptography scheme. The advantages of the proposed system in terms of processing time and security level can be proved by simulation results.

The proposed fingerprint authentication system is described in **Figure 3.1**

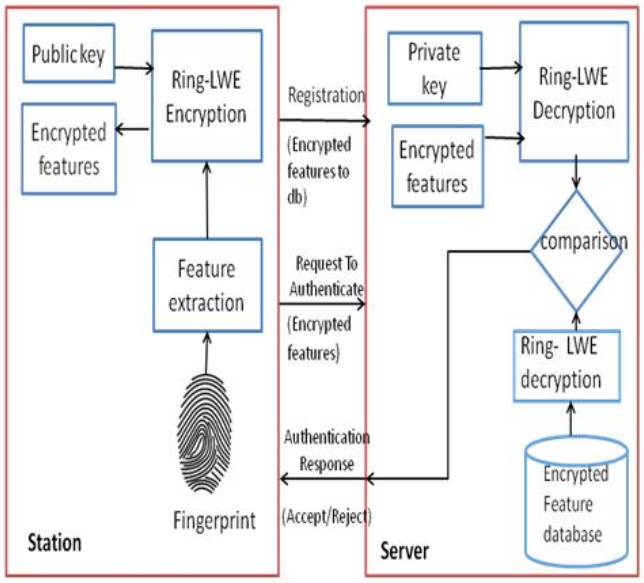

Figure 3.1 Proposed system

3.2.1 Description:

The proposed system consists of n local stations that are equipped with fingerprint sensing devices, and integrated fingerprint-features extraction and Ring-LWE encryption modules. The remote server consists of a database and installed Ring-LWE decryption modules to decrypt the messages received from stations.

The proposed system consists of three main phases.

- Registration phase
- Request-To –Authenticate (RTA) phase
- Authentication response phase

Registration phase:

The first phase is called the registration phase. Users who want to authenticate with the system must initially register their fingerprint data at a corresponding local station. Data collected from sensing devices are then extracted to get the necessary features using the proposed minutiae based fingerprint extraction scheme. In this project,the proposed system uses two main features of the fingerprint, namely

- Ridge ending
- Bifurcation

Ridge Ending: The abrupt end of a ridge

Bifurcation: A single ridge dividing into two ridges

These features are encrypted using the proposed NTT multiplication-based ring-LWE encryption scheme to get the encrypted data. The authentication module at each station sends users' encrypted features to the server where each users' data are stored in the encrypted features database.

Request-To-Authenticate:

In the second phase, once a user needs to perform a fingerprint authentication with the system, a station collects the users' encrypted data and sends it to the server with a Request-To-Authenticate (RTA) message. Upon receiving an RTA message from a user, the server performs decryption of the message using the proposed ring-LWE decryption scheme and compares results with the registered data to decide whether the user has the right to access the system or not.

Authentication Response:

If the RTA sent from a local station is accepted, the server sends an Accept-To-Authenticate (ATA) message in the response to the corresponding station, and allows the user to access the system; otherwise, the server sends a reject message to deny the user access and alerts the bank authorities.

3.3 RING-LWE CRYPTOGRAPHY

RLWE is the studying of Errors over Rings and is simply the greater learning with errors (LWE) problem created to polynomial rings over definite fields.

A block diagram of the ring-LWE cryptosystem is described in **Figure 3.2.**

The ring-LWE public-key cryptosystem operations are participated in a polynomial ring, normally Rq = Zq[x]/ f (x). Polynomial addition, polynomial multiplication, and modulo reduction are the operations performed. Among them, polynomial multiplication is the most computationally intensive and can be efficiently executed using a Number Theoretic Transform (NTT) based polynomial multiplication. In extend to the significant workflow made regarding the theory of lattice-based cryptography, practical implementations of this cryptosystem have recently profited the attention of the research community.

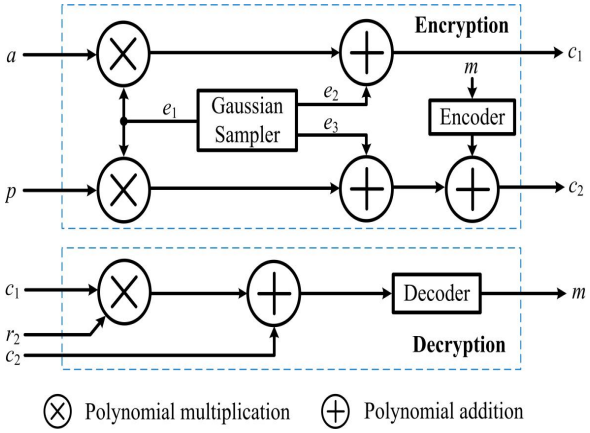

Figure 3.2 Block diagram of ring-Learning With Errors (LWE) cryptosystem

3.3.1. Operations in Ring-LWE Cryptography

The Ring-LWE cryptography, launched in 2005 as a public key cryptosystem, is a machine learning problem that is similar to the worst-case lattice problems.The ring-LWE cryptosystem is built on a polynomial ring Rq = Zq[x]/ f (x), where q 1 mod 2n is a sufficiently large public prime number, and f (x) is the irreducible polynomial. Normally, f (x) = xn + 1, where n is the security parameter with a power of 2. The ring-LWE distribution on Rq × Rq consists of pairs (a, t) with a Ɛ Rq chosen uniformly random, and t = a × s + e Ɛ Rq, where s is a fixed secret element and e is sampled from a discrete Gaussian distribution with a standard deviation s. The procedures of a ring-LWE cryptosystem, including the key generation, encryption, and decryption, are described as follows.

A. Key Generation

This process produces a private key r2 and public key (a, p). The polynomial a is chosen uniformly, and two polynomials r1 and r2 are sampled from the Gaussian distribution . The polynomial r2 becomes the private key, and two polynomials r1 and r2 participate in the public key generation process.

$$p \leftarrow r_1 - a \times r_2$$

B. Encryption

The ring-LWE encryption operation encrypts the input message m to the cipher-text (c1, c2). Initially, the input message m is encoded into the polynomial using an encoder. Depending on the i-th coefficient of m, it is encoded as (q 1)/2 (if m[i] = 1) or 0 (if m[i] = 0). The cipher-text (c1, c2) is calculated based on the public key (a, p), the encoded message, and three error polynomials e1, e2, and e3 sampled from the Gaussian distribution.

$$(c_1, c_2) \leftarrow a \times e_1 + e_2, p \times e_1 + e_3 + m_e$$

C. Decryption

The decryption operation recovers the original message m from the cipher-text (c1, c2). This operation starts with the calculation of the pre-decoded polynomial md

$$m_d \leftarrow c_1 \times r_2 + c_2$$

The original message m is recovered from the pre-decoded polynomial md using a decoder. The i-th coefficient of the message m is changed to 1 if and only if its corresponding value md[i] satisfies the agreement $q/4 \leq md[i] \leq 3q/4$; otherwise, it is converted to 0.

IV. RESULTS AND DISCUSSION

The following figure represents the sample fingerprint image tested with this proposed work.

Figure 4.1 Input Fingerprint image

Pre processing

A preprocessing module is developed before feature extraction for preserving the performance of the system against bad quality samples. Pre processing is a crucial step for fingerprint recognition system. Preprocessing stage is divided into three sub stages such as 1.Image enhancement 2. Image segmentation 3. Thinned image

For Image enhancement the proposed system used three methods such as Contrast enhancement ,Histogram equalization and Gamma correction method. Image enhancement enhances the quality and produces an image in which minutiae can be detected correctly.

Contrast enhancement

Contrast enhancement is a process of creating the image features stand out more clearly by making optimal use of colors available on the display or output device.

Histogram equalization

Histogram equalization is a method of improving the global contrast of an image by adjusting the intensity distribution on a histogram. This allows areas of lower local contrast to gain a higher contrast without disturbing the global contrast. Histogram equalization accomplishes this by effectively spreading out the foremost frequent intensity values.

Gamma correction

In this work proposed to use a gamma correction method to adjust the brightness of the input image based on the state estimated adaptively from the input image. Gamma correction is defined as:

$$S = c \times r^{\gamma}$$

where each pixel r of the input image is transformed to the output level S by powering r to a γ (constant c = 1 in this work). The parameter is adaptively estimated from the grey-scale level of the input image by:

$$\gamma = \frac{\sum I(x,y)}{M \times N \times \frac{L}{2}}$$

where I indicates the input image of size M × N; L is the grey level of I (L = 255 for 8-bit images). For the image of a dry finger, the intensity of the input is high so that γ is greater than 1, leading to the contrast of output image being expended in the direction of reducing the total brightness of the image. The converse is true for a fingerprint image, as illustrated in Figure 4.2. For normal cases, the value of γ is around 1, and therefore the input image is slightly modified.

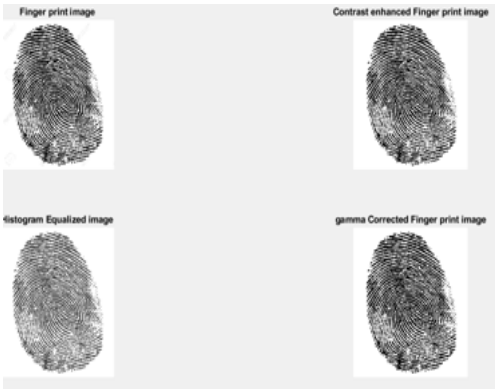

Figure 4.2 Image enhancement

Image segmentation

Segmentation of images involves converting an imag e to a collection of regions of pixels represented by a mask or a labeled image. By dividing an image into segments we can process only the important segments of the image. Image segmentation is the partition of the fingerprint region or extraction of the presence of ridges from the background of the initial stage.

Figure 4.3 segmented fingerprint image

Ridge Thinning

The ridge thinning process is used to remove the redundant pixels of ridges till the ridges are just up to one pixel wide. This is done by using the following thinning function.bwmorph(binaryImage,'thin',Inf)

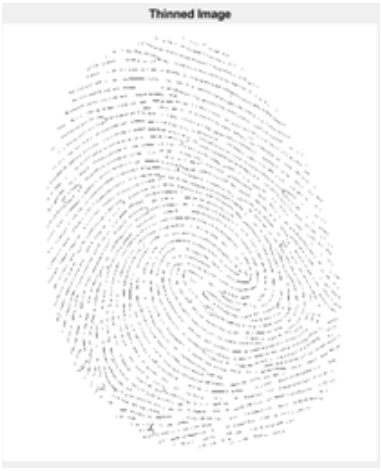

Figure 4.4 Thinned image

Feature extraction

In this feature extraction step the minutiae features has been extracted. Minutiae points are the most important features of a fingerprint image and are used in the matching of fingerprints. These minutiae points are used to determine the distinctiveness of a fingerprint image. In this work , ridge ending and ridge bifurcation features of the fingerprint image have been extracted and taken into consideration for processing.

Figure 4.5 Feature extraction

Ring-LWE cryptography encryption

In this step, fingerprint image has been encrypted using Ring-LWE cryptography. The histogram of the encrypted fingerprint is much different from the original one. Furthermore, since the distribution of the appearance probabilities of the grey levels is equitable, it is extremely difficult to predict information from the encrypted image.

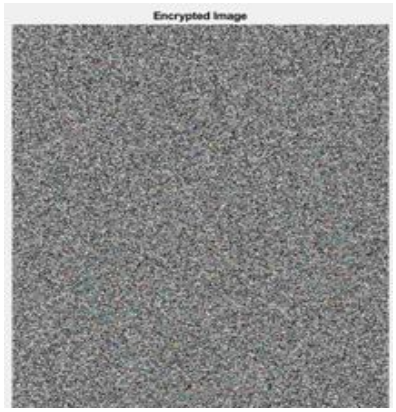

Figure 4.6 Encrypted image

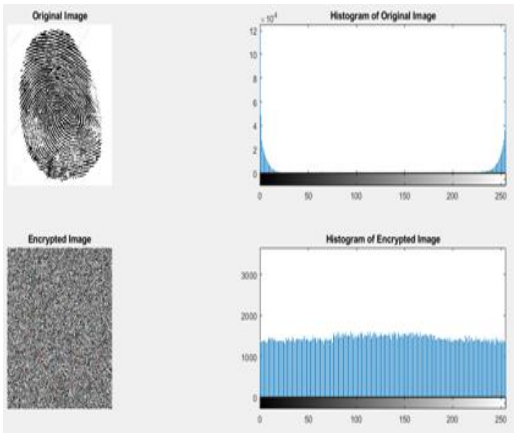

Figure 4.7 Histogram of fingerprint and its encrypted image

Figure 4.8 Decrypted image

Matching and Comparison

When extracting all minutiae points of two finger print images in selected region of interest.Now, Minutiae matching are performed for authentication. Basically, minutiae matching is a process which is composed of two steps

1. To find Total minutiae Points:

This step is used to determine the total number of ridge and Bifurcation points separately. And it compares the computed value with the original image values.

2. To find Location of Minutiae point:

It works on the basis of minutiae matching process. Simply when minutia points are marked on the image, it also stores the location of the point. This stored information is used to compare two different images at verification process. If both the images belong to the same person then the position of ridge/bifurcation will match. Otherwise matching of fingerprint images is unsuccessful.

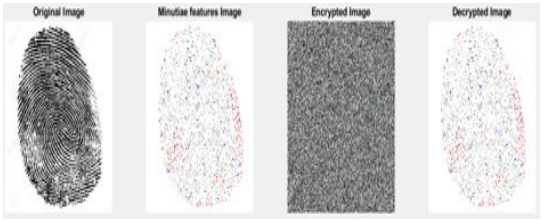

Figure 4.9 Matching and comparison

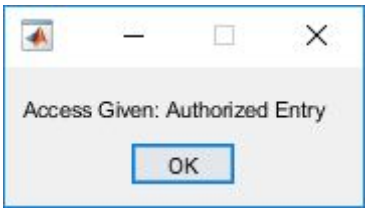

Figure 4.10 Access given message

Thus the system shows that the given fingerprint belongs to an authorized user.

V. CONCLUSION

A novel high-security fingerprint authentication system using Ring-LWE cryptography is presented in this project. By using the novel NTT multiplication and feature extraction approach, the processing time of the proposed system is improved remarkably. Simulation results show that the proposed system achieves low processing times, and can be used in real-time authentication systems. In addition, with the high level of security offered by Ring-LWE cryptography, users' personal fingerprints are completely protected. Therefore, the proposed fingerprint authentication system developed for bank safety lockers is observed to be more secure for user identification.

REFERENCES

[1] W. Yang, J. Hu, and S. Wang, "A Delaunay Quadrangle-Based Fingerprint Authentication System with Template Protection using Topology Code for Local Registration and Security Enhancement," IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1179–1192, Jul. 2017.

[2] E. Liu, H. Zhao, J. Liang, L. Pang, M. Xie, H. Chen, Y. Li, P. Li, and J.Tian, "A Key Binding System Based on N-Nearest Minutiae Structure of Fingerprint," Pattern Recognition Letters, vol. 32, no. 5, pp. 666–675, Apr.2011.

[3] Ogawa, "Labeled Point Pattern Matching by Delaunay Triangulation and Maximal Cliques," Pattern Recognition, vol. 19, no. 1, pp. 35–40, May1986.

[4] R. Gil, G. D. Orueta, M. Tawfik, F. G. Loro, A. P. Martin, E. Sancristobal,S. Martin, and M. Castro, "Fingerprint Verification System in Tests in Moodle," IEEE J. Latin American Learning Technologies, vol. 8, no. 1,pp. 23–30, Feb. 2013.

[5] S. Li, A.C. Kot, "Fingerprint Combination for Privacy Protection," IEEETrans. Inf. Forensics Security, vol. 8, no. 2, pp. 350–360, Feb. 2013.

[6] M. Abdalla, F. Benhamouda, and D. Pointcheval, "Public-key Encryption Indistinguishable under Plaintext-Checkable Attacks," IET Inf. Security,vol. 10, no. 6, pp. 288–303, Oct. 2016.

[7] F. Heuer, T. Jager, S. Schage, and E. Kiltz, "Selective Opening Security of Practical Public-Key Encryption Schemes," IET Inf. Security, vol. 10, no.6, pp. 304–318, Oct. 2016.

[8] T. N. Tan, H. Lee, "A Delay-Efficient Ring-LWE Cryptography Architecture for Biometric Security," in Proc. IEEE Int. Symp. Circuits Syst.,Baltimore, MD, USA, May 2017, pp. 2210–2213.

[9] X. Huang, W. Wang, "A Novel and Efficient Design for an RSA Cryptosystem with a Very Large Key Size," IEEE Trans. Circuits Syst. II, vol.62, no. 10, pp. 972–976, Oct. 2015.

[10] S. Li and A. C. Kot, ''Privacy protection of fingerprint database,'' IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011.