International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

A Survey on Fingerprint Authentication Using Various Cryptographic Techniques

Anjali Krishna A[1], Shyma Kareem[2]

[1]PG Scholar, Department of CSE, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India,
[2]Professor, Department of CSE, Musaliar College of Engineering & Technology, Pathanamthitta, Kerala, India

---

Abstract - *Nowadays, the digital information theft is increasing in digital society. Fingerprint authentication is the one of the most reliable and mature biometric recognition techniques. Owing to the distinctiveness and stability that fingerprint can provide compared to other biometrics. This fingerprint authentication system can be applied in system that requires a high security level, such as biometric authentication, medical image transmission and IOT security. This paper reviews a comparison study on fingerprint authentication using various cryptographic techniques. The aim of this paper is to give overview and comparison of fingerprint authentication based on various cryptographic techniques for young learners and researchers.*

Keywords: - Fingerprint Authentication, Cryptography, Ring LWE, AES, RSA, Elliptic curve.

1. INTRODUCTION

Fingerprint Authentication is the act of verifying an individual's identity based on one or more of their fingerprints. Authenticating or scanning fingerprints is a form of biometric technology that allows users to use their fingerprint images to access online services. Due to the distinctiveness and stability that fingerprints can offer compared to other biometrics, fingerprint authentication is one of the most reliable and mature biometric recognition techniques [4]. Fingerprint information stored in a database is also used to confirm individual identities in cases of security checks, medical jurisprudence, or disasters. There are two types of methods of fingerprint authentication, namely, methods based on texture and methods based on minutiae. The latter is more efficient and popular [9]. A fingerprint image with a set of labeled minutiae referring to ridge termination and bifurcation is represented by minutiae-based algorithms. Point pattern matching can be considered for fingerprint matching with the minutiae-based algorithm [13]. The detailed fingerprint-matching operations by minutiae [7]. A digital image of the fingerprint pattern is captured by a fingerprint system using an electronic device. This captured image in fingerprint system is called a live scan which is digitally processed to create a biometric template (finger features). Later, the biometric features will be stored and used for the process of matching. Using various cryptographic techniques such as RSA, DES, LWE cryptography etc. these fingerprint characteristics are encrypted and decrypted. Authentication of fingerprints using different cryptographic techniques. Some of these methods are based on cryptography [6]. The means of transmission may be unreliable. Cryptography techniques are also used to encrypt the data transmitted. In cryptography, using a key in the encryption method (on the sender's side), plain-text is converted into cipher text. The cipher-text is converted into plain-text at the receiver end, using a key via the decryption process. The methods of cryptography are divided in to two symmetrical and asymmetrical categories. In symmetric cryptography, the encryption and the decryption are performed using the same key. Some of the methods of symmetric cryptography are DES, AES, Blowfish, etc. An example of asymmetric cryptography is the RSA algorithm, where the key used for encryption and decryption is different. [1].

2. CRYPTOGRAPHIC TECHNIQUES FOR FINGERPRINT AUTHENTICATION

2.1 A Fingerprint Authentication System using LWE Cryptography

The Fingerprint Authentication System using LWE cryptography presented by TUY NGUTEN [2] in 2019 contained a security system designed to store user fingerprint data in much safer way. This system is a high secure fingerprint authentication system using Ring learning with error (Ring-LWE) cryptography to protect user fingerprint data more securely. For a fingerprint features extraction method, it presents a delay-optimized high-accuracy scheme to collect the necessary features' data from fingerprint images. To speed up the ring-LWE encryption and decryption times, a ring-LWE cryptography scheme using low-latency number theoretic transform (NTT) polynomial multiplications is deployed.

2.2 Fingerprint Authentication for budget application using AES

The fingerprint authentication for Budget application presented by Naomi Easter [3] in 2019 contained a fingerprint authentication algorithm based on the Advance Encryption Standard (AES) and on the Android Keystore System. This technology helps protect personal phone data saved by users. One of the most widely used algorithms for data encryption and security is the AES encryption standard. These new techniques for securing applications are provided by technologies such as facial recognition, iris recoil, and fingerprint recognition. As one of the most reliable forms of authentication, biometric fingerprint readers are increasingly used on mobile phones. Fingerprint algorithms have been embedded in modern mobile devices, for authentication. Nowadays mobile devices use a fingerprint scanner, so fingerprinting algorithms are becoming more widespread.

2.3 Fingerprint watermarking and steganography for ATM transaction using LSB-RSA and 3-DWT algorithms

The Fingerprint watermarking and steganography for ATM transaction using LSB-RSA and 3-DWT algorithms presented by Mayank Garg [5] in 2015 contained combination of fingerprint verification methods with watermarking technology to provide copyright protection and authentication of digital images is proposed. Combine DWT with RSA and LSB when proposing techniques for better accuracy. This method provides perfect results from previous work.

2.4 Formation of Elliptic Curve Using Fingerprint for Network Security

Formation of Elliptic Curve Using Finger Print for Network Security presented by B.Thiruvaimalar Nathan [10] in 2010 contained a new method for the secured exchange between an E-passport or E-driving license and the Inspection System is provided. The main objective of this method is to construct an elliptic curve points from fingerprint using MATLAB environment. First, extract minutiae from fingerprints. The elliptic curve is generated from these minutiae by using the generation algorithm of elliptic curve cryptography. Therefore, the elliptical curve is based on biometric data to verify the user's identity has been established. This review confirms that our approach matches the defined security goals.

3. FINGERPRINT AUTHENTICATION SYSTEM

As detailed in Fig-1, consider a standard fingerprint authentication scheme consisting of n local stations connecting to a remote server. Before being sent to a remote server database, users' fingerprints are initially obtained by local sensing devices. Full fingerprint images or limited fingerprint features can be the information sent from local stations to the remote server. Generally, individual identity information sent over a network without any protection solution (such as fingerprint images or fingerprint features) is open to attackers and therefore at risk. Therefore, before sending data to the server, Li and Kot present a method to merge different fingerprints into a new identity. The minutiae positions are extracted from one fingerprint, the orientation from another fingerprint, and the reference points are extracted from both fingerprints. There are, however, concomitant risks associated with this fingerprint data storage and transmitting process. If attackers distinguish a merged template of minutiae from the original template of minutiae, the original fingerprint can be recovered. In order to protect personal information during authentication, storage and transmission, it is therefore necessary to integrate a highly secure solution into the fingerprint authentication system. Cryptosystems, where secret information can only be accessed by authorized users with the correct key, provide a possible solution that can be combined into two forms of cryptography: symmetric and asymmetric cryptography. The former uses the same key for encryption and decryption operations, while the latter uses two different keys for encryption and decryption, called the public key and the private key. Rivest, Shamir and Adleman (RSA), and elliptic curve cryptography are common asymmetric cryptography schemes (ECC). ECC encryption and decryption operations are based on an elliptic curve and Galois-field GF (p) or GF (2m) arithmetic operations, where p and m are prime numbers. In the key generation operation, to determine the ECC point multiplication QS kS PS, the receiver selects a random number for its private key kS and a base point PS. Before sending it to the receiver, the sender uses the receiver's public key to encrypt input data. The original data can be retrieved at the receiver using its secret key and multiplication operations of the ECC point. While ECC uses a much smaller key length to give traditional systems, such as RSA, a similar degree of security, it can be solved by a quantum computer in polynomial time. Post-quantum security and realistic alternatives for the future are required with the rapid advances in cryptanalysis and the unpredictable growth of the quantum computer. Ring-learning with errors (ring-LWE) cryptography is a great candidate to replace these conventional cryptosystems based on the worst-case hardness of well-known lattice problems since there is no known quantum computer that can solve the lattice problem effectively.

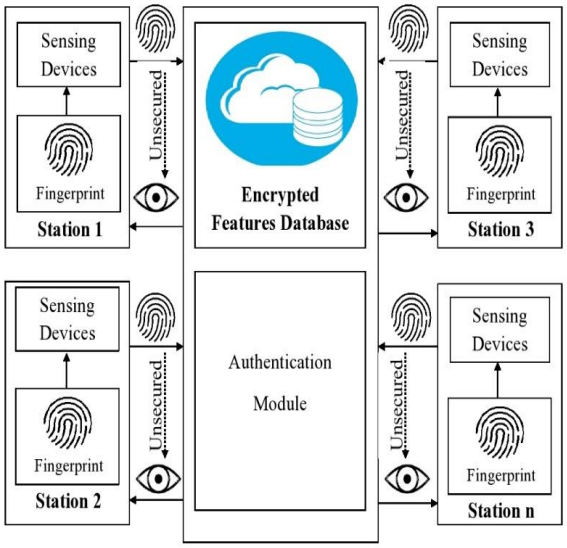

Fig-1: A typical fingerprint authentication system

3.1 Ring LWE Cryptography

Post-quantum security and realistic alternatives for the future are required with the rapid advances in cryptanalysis and the unpredictable growth of the quantum computer. Ring-learning with errors (ring-LWE) cryptography is considered a great candidate for replacing these conventional cryptosystems based on the worst-case hardness of well-known lattice problems since there is no known quantum computer that can effectively solve the lattice problem. The extracted features are encrypted using the ring-LWE cryptography method using the NTT polynomial multiplication approach to improve the time of encryption and decryption in fingerprint authentication using LWE cryptography. Simulation results will prove the advantages of this system in terms of processing time and level of protection.

3.2 Advanced Data Encryption Standard (AES)

The use of the Advanced Encryption Standard to replace the Data Encryption Standard was recommended by the US National Institute of Standards and Technology (NIST) in 1998. AES is a variable bit block encryption that uses 128, 192 and 256 bits of variable key length. AES will perform 9 processing rounds if both the block length and key length are 128 bits. If the block and key are 192 bits, 11 processing rounds are done by AES. If the block and key are 256 bits in duration, 13 processing rounds are taken out[8].

3.2.1 Generate Key

A key used for further encryption, required for transmitting the data from the fingerprint scanner to the device, is generated in this phase. The method utilizes a key generation in our application that needs permission. Using the AES encryption standard, a cipher is generated and then it is checked if the cipher is the same as the key.

3.2.2 Encrypting Key

To generate the encrypted data, this portion of the algorithm is used. This is necessary because the information is encrypted on the phone and stored in it. To use this data, it is necessary to search the phone's memory and obtain all the saved and encrypted information and analyzed it with the newly encrypted data obtained from the scanner.

3.3 Rivest, Shamir, and Adleman (RSA)

RSA stands for Rivest Shamir and Adleman name of three inventors. The most widely used algorithm for public key encryption is RSA [12]. It can be used for both encryption and digital signature applications. Factoring is generally taken into consideration in the protection of RSA. RSA is one of the first functional cryptosystems of the public key and is commonly used for safe data transmission. The encryption key in such a cryptosystem is public and varies from the decryption key that is kept secret. In RSA, this asymmetry is based on the practical difficulty, the factoring problem, of factoring the product of two large prime numbers. The issue for the attacker is that it is assumed that computing the reverse d of e is no easier than factoring n. For a fair level of protection, the key size should be greater than 1024 bits. Size keys, say, the 2048 bits it provides. The fingerprint images with ATM PIN for security purposes in Fingerprint watermarking and steganography for ATM transactions using LSB-RSA. For steganography, take the fingerprint image as an input image in the first step. Take A TM PIN to use the Least Significant Bit method to cover the image. Encrypt the ATM PIN using the RSA algorithm for encryption. Take the stego image (hidden image) as a cover image in the second stage and take the watermark image for watermarking fingerprints.

3.4 Elliptic Curve Cryptography

ECC is the counterpart of modular multiplication in RSA and the counterpart of modular exponentiation is multiple additions. With small keys comparable to RSA and other PKC methods, ECC can deliver security levels. It has been designed for devices such as smart cards with limited processing power and/or memory. The Public-Key Cryptography Standards are specifications produced by RSA Laboratories to accelerate the deployment of public-key cryptography in cooperation with secure systems developers worldwide. First published in 1991, the PKCS documents were widely cited and implemented as a result of meetings with a select community of early adopters of public-key technology. The basics of elliptic curves over finite fields and the applications of cryptography related to

elliptic curves are illustrated briefly. Elliptic Curve Equation y2=(x3+ax+b) mod p[11].

4. COMPARISON

The cryptographic techniques and encryptions are used in the authentication methods are shown in Table 1.

Table - 1: Cryptographic technique and Encryption used in Authentication Methods.

Authentication Methods	Cryptographic technique used	Encryption
1. A Fingerprint Authentication System using LWE cryptography	**Ring LWE Cryptography**	Using LWE cryptography the extracted features are encrypted by using the ring-LWE cryptography system using the NTT polynomial multiplication.
2. Fingerprint Authentication for budget application using AES	**AES**	A cipher is generated using the AES encryption standard.Generate a key used for encryption
3. Fingerprint watermarking and steganography for ATM transaction using LSB-RSA and 3-DWT algorithms	**RSA**	A TM PIN to hide into image using Least Significant Bit method. Encrypt ATM PIN using RSA encryption algorithm.
4. Formation of Elliptic Curve Using Fingerprint for Network Security	**Elliptic curve Cryptography**	Minutiae from fingerprints are extracted. From those minutiae, elliptic curve is generated by using elliptic curve cryptography generation algorithm

5. CONCLUSION

This paper reviews a comparison study on the most common used fingerprint authentication using various cryptographic techniques. Some of these methods are based on cryptography. In this study, show the main cryptographic techniques used for fingerprint authentication. As well as this study presents a specific discussion about fingerprint authentication. With the same key size, lattice-based cryptographic algorithms can offer much higher secure compared with conventional public-key algorithms, such as the Rivest–Shamir–Adelman (RSA) cryptosystem, or Elliptic Curve Cryptography (ECC) algorithms. As a result, due to the complexity of Ring LWE encryption approach this paper presents that Ring LWE cryptography-based fingerprint authentication is highly secure.

REFERENCES

[1] Richa Maurya, Ashwani Kumar Kannojiya, Rajitha "An Extended Visual Cryptography Technique for Medical Image Security" 2020

[2] T. N. Tan and H. Lee, "High-secure fingerprint authentication system using ring-LWE cryptography,'' IEEE Access, vol. 7, Feb. 2019

[3] Naomi Estera Costea, Elisa Valentina Moisi "Fingerprint Authentication for Budget Application" 2019

[4] 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* Jul. 2017.

[5] Mayank Garg "Fingerprint watermarking and steganography for ATM transaction using LSB-RSA and 3-DWT algorithms."2015.

[6] Mohammad A, Alia "Cryptography based authentication methods", 2014, San Francisco USA.

[7] R. Gil *et al.*, ``Fingerprint verification system in tests in moodle,'' *IEEE* vol. 8, Feb. 2013

[8] Monika Agrawa, Pradeep Mishra" A Comparative Survey on Symmetric Key Encryption Techniques "IJCSE, Vol. 4 No. 05 May 2012

[9] E. Liu *et al.*, ``A key binding system based on N-nearest minutiae structure of fingerprint,'' *Pattern Recognition.* Apr. 2011.

[10] B.Thiruvaimalar Nathan" Formation of Elliptic Curve Using Fingerprint for Network Security" 2010

[11]W. Stallings "Cryptography and network security", vol. 2 prentice hall, 2003

[12] Ms. Ritu Patidar1, Mrs. Rupali Bhartiya 2 "Modified RSA Cryptosystem Based on Offline Storage and Prime Number", vol.3, 2003.

[13] H. Ogawa, ``Labeled point pattern matching by Delaunay triangulation and maximal cliques,'' *Pattern Recognition.*, vol. 19, May 1986.

BIOGRAPHIES

ANJALI KRISHNA A is doing M Tech at Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India. She has received B Tech degree in Computer Science and Engineering from *APJ Abdul Kalam Technological University*, Thiruvananthapuram, Kerala, India. Her main research area of interest includes Cryptography and Network security.

SHYMA KAREEMis working as Assistant Professor at Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, INDIA.