# CHAPTER 1 INTRODUCTION

* 1. **FINGERPRINT ENCRYPTION**

Fingerprint is an impression left by the friction ridges of a human finger. Fingerprint authentication is a type of biometrics which digitally and compares and verifies two fingerprints. Fingerprint biometrics is known to be effective because of its distinctiveness, permanence, and performance. Such system is based on two believes: No two individuals have the same set of fingerprints and a fingerprint never changes naturally. The purpose of fingerprint authentication is to check the identity of individuals.

Fingerprints are mostly used for authentication purpose. But, these fingerprints are stored in the databases without much encryption. So, many attacks had been taken place. In Adhaar, the fingerprints are stored without or minimal encryptions. As a result many attacks have been taken place. So, to minimize those attacks , fingerprint encryption is much needed.

# SYSTEM OVERVIEW

The system provides encryption to the fingerprint images stored in the database. Normal fingerprint image scanned from the fingerprint scanner will have noise and frequency issues. To remove that, the fingerprint image preprocessing is done to enhance the quality of the image. Then the enhanced image is encrypted using the AES encryption algorithm. This algorithm converts the image into a bytecode. This bytecode will be stored in a text file which will be hidden in another new fingerprint image. This new fingerprint image will be stored in the database.

# SCOPE OF THE PROJECT

Fingerprint images should be generated properly by the fingerprint sensor. The position and orientation of the thumb should be fixed properly. Noises should be removed from the image for more accuracy. Passwords used for archiving the file should be strong. Better key size should be used for the optimal performance.

# CHAPTER 2 LITERATURE SURVEY

1. **High-Secure Fingerprint Authentication System Using Ring-LWE Cryptography(2019)**

This paper presents a high-secure fingerprint authentication system using ring learning with errors (ring-LWE) cryptography to protect users' fingerprint data more securely. A delay-optimized high-accuracy scheme for a fingerprint-features extraction approach is proposed to collect necessary features' information from fingerprint images. In addition, a ring-LWE cryptography scheme using low-latency number theoretic transform (NTT) polynomial multiplications is deployed to speed up the ring-LWE encryption and decryption times. As a result, the processing time of the fingerprint authentication system is significantly reduced, and the fingerprint data are effectively protected. The simulation results show that the proposed NTT multiplication-based ring-LWE cryptography scheme for fingerprint features outperforms the existing works up to 46% and 44% in terms of encryption time and decryption time, respectively. The latency of the whole fingerprint authentication system is less than 160 ms, which makes it suitable for practical applications. Furthermore, performance analysis on entropy and similarity of the encrypted fingerprint features proves the domination of the proposed system compared with the previous systems in terms of confidentiality.

1. **A Delaunay Quadrangle-Based Fingerprint Authentication System With Template Protection Using Topology Code for Local Registration and Security Enhancement(2017)**

Although some nice properties of the Delaunay triangle-based structure have been exploited in many fingerprint authentication systems and satisfactory outcomes have been reported, most of these systems operate without template protection. In addition, the feature sets and similarity measures utilized in these systems are not suitable for existing template protection techniques. Moreover, local structural change caused by nonlinear distortion is often not considered adequately in these systems. In this paper, we propose a Delaunay quadrangle-based fingerprint authentication system to deal with nonlinear distortion-induced local structural change that the Delaunay triangle-based structure suffers. Fixed-length and alignment-free feature vectors extracted from Delaunay quadrangles are less sensitive to nonlinear distortion and more discriminative than those from Delaunay triangles and can be applied to existing template protection directly. Furthermore, we propose to construct a unique topology code from each Delaunay quadrangle. Not only can this unique topology code help to carry out accurate local registration under distortion, but it also enhances the security of template data. Experimental results on public databases and security analysis show that the Delaunay quadrangle-based system with topology code can achieve better performance and higher security level than the Delaunay triangle-based system, the Delaunay quadrangle-based system without topology code, and some other similar systems.

# Fingerprint Combination for Privacy Protection

We propose here a novel system for protecting fingerprint privacy by combining two different fingerprints into a new identity. In the enrollment, two fingerprints are captured from two different fingers. We extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored in a database. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template. By storing the combined minutiae template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen. Furthermore, because of the similarity in topology, it is difficult for the attacker to distinguish a combined minutiae template from the original minutiae templates. With the help of an existing fingerprint reconstruction approach, we are able to convert the combined minutiae template into a real-look alike combined fingerprint. Thus, a new virtual identity is created for the two different fingerprints, which can be matched using minutiae-based fingerprint matching algorithms. The experimental results show that our system can achieve a very low error rate with FRR = 0.4% at FAR = 0.1%. Compared with the state-of-the-art technique, our work has the advantage in creating a better new virtual identity when the two different fingerprints are randomly chosen.

# Public-key encryption indistinguishable under plaintext-checkable attacks

Indistinguishability under chosen-ciphertext attack (IND-CCA) is now considered the *de facto* security notion for public-key encryption. However, this sometimes offers a stronger security guarantee than what is needed. In this study, the authors consider a weaker security notion, termed as indistinguishability under plaintext-checking attacks (IND-PCA), in which the adversary has only access to an oracle indicating whether or not a given ciphertext encrypts a given message. After formalising this notion, the authors design a new public-key encryption scheme satisfying it. The new scheme is a variant of the Cramer-Shoup encryption scheme with shorter ciphertexts. Its security is also based on the plain decisional Diffie-Hellman (DDH) assumption. Additionally, the algebraic properties of the new scheme allow proving plaintext knowledge using Groth-Sahai non-interactive zero-knowledge proofs or smooth projective hash functions. Finally, as a concrete application, the authors show that, for many password-based authenticated key exchange (PAKE) schemes in the Bellare-Pointcheval-Rogaway security model, they can safely replace the underlying IND-CCA encryption schemes with their new IND-PCA one. By doing so, they reduce the overall communication complexity of these protocols and obtain the most efficient PAKE schemes to date based on plain DDH.

# High-Speed Polynomial Multiplication Architecture for Ring-LWE and SHE Cryptosystems

Polynomial multiplication is the basic and most computationally intensive operation in ring-learning with errors (ring-LWE) encryption and "somewhat" homomorphic encryption (SHE) cryptosystems. In this paper, the fast Fourier transform (FFT) with a linearithmic complexity of O(nlogn), is exploited in the design of a high-speed polynomial multiplier. A constant geometry FFT datapath is used in the computation to simplify the control of the architecture. The contribution of this work is three-fold. First, parameter sets which support both an efficient modular reduction design and the security requirements for ring-LWE encryption and SHE are provided. Second, a versatile pipelined architecture accompanied with an improved dataflow are proposed to obtain a high-speed polynomial multiplier. Third, the proposed architecture supports polynomial multiplications for different lengths n and moduli p. The experimental results on a Spartan-6 FPGA show that the proposed design results in a speedup of 3.5 times on average when compared with the state of the art. It performs a polynomial multiplication in the ring-LWE scheme (n=256,p=1049089) and the SHE scheme (n=1024,p=536903681) in only 6.3 μs and 33.1 μs, respectively.

# Post-Quantum Key Exchange for the TLS Protocol from the Ring Learning with Errors Problem

Lattice-based cryptographic primitives are believed to offer resilience against attacks by quantum computers. We demonstrate the practicality of post-quantum key exchange by constructing cipher suites for the Transport Layer Security (TLS) protocol that provide key exchange based on the ring learning with errors (R-LWE) problem, we accompany these cipher suites with a rigorous proof of security. Our approach ties lattice-based key exchange together with traditional authentication using RSA or elliptic curve digital signatures: the post-quantum key exchange provides forward secrecy against future quantum attackers, while authentication can be provided using RSA keys that are issued by today's commercial certificate authorities, smoothing the path to adoption. Our cryptographically secure implementation, aimed at the 128-bit security level, reveals that the performance price when switching from non-quantum-safe key exchange is not too high. With our R-LWE cipher suites integrated into the Open SSL library and using the Apache web server on a 2-core desktop computer, we could serve 506 RLWE-ECDSA-AES128-GCM-SHA256 HTTPS connections per second for a 10 KiB payload. Compared to elliptic curve Diffie-Hellman, this means an 8 KiB increased handshake size and a reduction in throughput of only 21%. This demonstrates that provably secure post-quantum key-exchange can already be considered practical.

1. **A New Algorithm for High-Speed Modular Multiplication Design**

Modular exponentiation in public-key cryptosystems is usually achieved by repeated modular multiplications on large integers. Designing high-speed modular multiplication is thus very crucial to speed up the decryption/encryption process. In this paper, we first explore how to relax the data dependency that exists between multiplication, quotient determination, and modular reduction in the conventional Montgomery modular multiplication algorithm. Then, we propose a new modular multiplication algorithm for high-speed hardware design. The speed improvement is achieved by reducing the critical path delay from the 4-to-2 to 3-to-2 carry-save addition. The resulting time complexity of our development is further decreased by simultaneously performing the multiplication and modular reduction processes. Experimental results show that the developed modular multiplication can operate at speeds higher than those of related work. When the proposed modular multiplication is applied to modular exponentiation, both time and area-time advantages are obtained.

1. **Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications**

Recently, considerable research has been performed in cryptography and security to optimize the area, power, timing, and energy needed for the point multiplication operations over binary elliptic curves. In this paper, we propose an efficient implementation of point multiplication on Koblitz curves targeting extremely-constrained, secure applications. We utilize the Gaussian normal basis (GNB) representation of field elements over GF(2 m ) and employ an efficient bit-level GNB multiplier. One advantage of this GNB multiplier is that we are able to reduce the hardware complexity through sharing the addition/accumulation with other field additions. We utilized the special property of normal basis representation and squarings are implemented very efficiently by only rewiring in hardware. We introduce a new technique for point addition in affine coordinate which requires fewer registers. Based on this technique, we propose an extremely small processor architecture for point multiplication. Through application-specific integrated circuit (ASIC) implementations, we evaluate the area, performance, and energy consumption of the proposed crypto-processor. Utilizing two different working frequencies, it is shown that the proposed architecture reaches better results compared to the previous works, making it suitable for extremely-constrained, secure environments.

1. **Better Key Sizes (and Attacks) for LWE-Based Encryption(springer)**

We analyze the concrete security and key sizes of theoretically sound lattice-based encryption schemes based on the “learning with errors” (LWE) problem. Our main contributions are: (1) a new lattice attack on LWE that combines basis reduction with an enumeration algorithm admitting a time/success tradeoff, which performs better than the simple distinguishing attack considered in prior analyses; (2) concrete parameters and security estimates for an LWE-based cryptosystem that is more compact and efficient than the well-known schemes from the literature. Our new key sizes are up to 10 times smaller than prior examples, while providing even stronger concrete security levels.

**[10] Fingerprint-Based Fuzzy Vault: Implementation and Performance**

While cryptography is a powerful tool to achieve information security, one of the main challenges in cryptosystems is to maintain the secrecy of the cryptographic keys. Though biometric authentication can be used to ensure that only the legitimate user has access to the secret keys, a biometric system itself is vulnerable to a number of threats. A critical issue in biometric systems is to protect the template of a user which is typically stored in a database or a smart card. The fuzzy vault construct is a biometric cryptosystem that secures both the secret key and the biometric template by binding them within a cryptographic framework. We present a fully automatic implementation of the fuzzy vault scheme based on fingerprint minutiae. Since the fuzzy vault stores only a transformed version of the template, aligning the query fingerprint with the template is a challenging task. We extract high curvature points derived from the fingerprint orientation field and use them as helper data to align the template and query minutiae. The helper data itself do not leak any information about the minutiae template, yet contain sufficient information to align the template and query fingerprints accurately. Further, we apply a minutiae matcher during decoding to account for nonlinear distortion and this leads to significant improvement in the genuine accept rate. We demonstrate the performance of the vault implementation on two different fingerprint databases. We also show that performance improvement can be achieved by using multiple fingerprint impressions during enrollment and verification.

# CHAPTER 3 SYSTEM ANALYSIS

* 1. **EXISTING SYSTEM**

In the existing database like adhaar, the fingerprint images stored aren’t encrypted securely. So, many attacks were done using this vulnerability. Many fingerprint authentication and recognition algorithm, are present. And methods like ring LWE, post quantum cryptography, Pixel based methods are present. But, the encryption techniques of fingerprint image are not so secure, less accurate and more complex. The encryption of fingerprint images are more important because they are used as unique id to identify the people. Many encryption algorithms like AES, Blowfish and DES are present. MATLAB,

Gnu Octave softwares are used for image preprocessing.

# Disadvantages of the Existing System

* + - * The fingerprint images stored in the database aren’t encrypted making it victims for several attacks like Transmission, Data simulation, Template and Replay ,etc
      * Some algorithms fails mostly for Replay attacks ,that is duplication of fingerprint images of legitimate users.
      * It uses weak encryption algorithms, such that it is easily breakable.

# PROPOSED SYSTEM

In this system, encryption of fingerprint images are done. The image obtained from the fingerprint scanner will contain noises and frequency issues. So, image preprocessing of fingerprint images are done to increase the quality of image for better accuracy. The encryption algorithm AES is used to encrypt the fingerprint image. The bytecode is obtained as a output of the algorithm which is stored in a separate text file. The text file is hidden in another new fingerprint image using Steganography method. The new fingerprint image will be stored in the database.

# Advantages of the Proposed System

* + - * The fingerprint images in the database are encrypted.
      * This system overcomes security attacks like Transmission, Template, Data Simulation, Replay, etc.
      * Since, the algorithm used is very simple, it is fast.
      * Forgeries can be easily detected and it is hard to break the encryption algorithm.

# REQUIREMENTS SPECIFICATION

* + 1. **Hardware Requirements**
* Hard Disk: 40GB and above
* RAM: 512MB and above
* Processor: Pentium IV and above

# Software Requirements

* Windows operating system XP and above
* Matlab
* Win-Rar
* JRE (Java Runtime Environment)

# LANGUAGE SPECIFICATION

# 3.4.1 MATLAB

MATLAB (*matrix laboratory*) is a multi-paradigm numerical computing environment and proprietary programming language developed by MathWorks. MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages.

Although MATLAB is intended primarily for numerical computing, an optional toolbox uses the MuPAD symbolic engine allowing access to symbolic computing abilities. An additional package, Simulink, adds graphical multi-domain simulation and model-based design for dynamic and embedded systems.

The fingerprint image obtained from the fingerprint scanner will contain noises and frequency issues. To remove that, image preprocessing has to be done which is done with the Matlab. The original image is sharpened to remove the noises and to enhance the quality of the image. Better accuracy can be achieved.

# CHAPTER 4

**SYSTEM DESIGN**

* 1. **SYSTEM ARCHITECTURE**

Rotation of Fingerprint Image

Encryption of rotated binary image

Image Hiding

Stored in Database

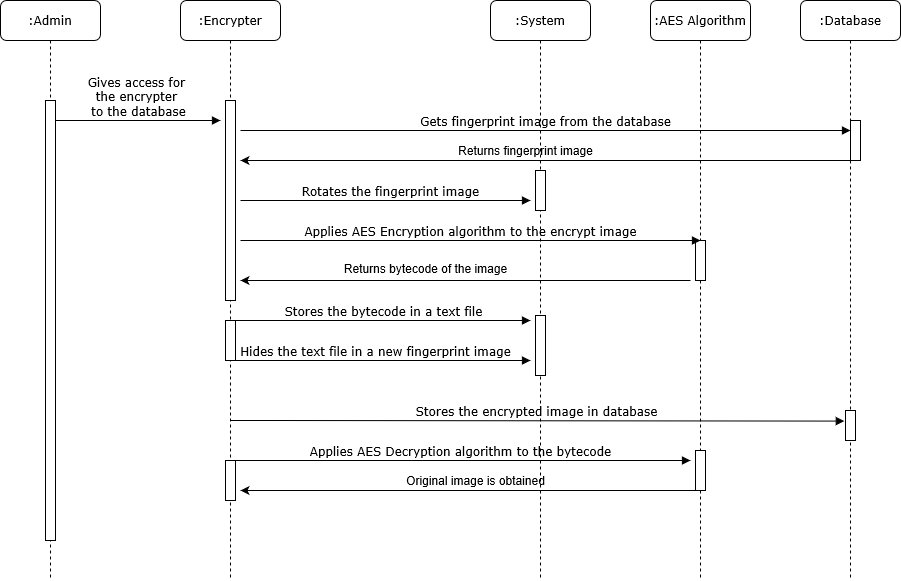
Image Pre-processing

Fingerprint Scanner

Fingerprint Image

In the figure 4.1,the fingerprint scanner generates the fingerprint image. Now, the image is converted into the binary format. The converted binary format will be rotated to a certain angle and both the images, the original binary image and the rotated binary image will be encrypted using the cryptographic algorithm, Advanced Encryption Standard. The encrypted fingerprint image will be stored in the database.

* 1. **SEQUENCE DIAGRAM**



From the above diagram, the sequence of actions can be known. Administrator gives access to the encrypter to access the fingerprint images. The encrypter obtains the image and encrypts it using AES algorithm, and converts it into a bytecode and stores it in another fingerprint image and the new image gets stored in the database**.**

**CHAPTER 5**

**MODULE DESCRIPTION**

* 1. **MODULES**

The modules are

* + - Image preprocessing
    - Rotation
    - Encryption
    - Image hiding
    - Decryption

# PRE PROCESSING

The original fingerprint image consists of noise and unwanted data. It may be due to improper inking or not placing the finger in a correct position. These noise should be removed from the image by preprocessing it. Preprocessing involves several methods like binning, smoothing, scaling, thinning and so on to convert the image into fine enhanced image . The ridges and furrows will be represented more clearly. This will be done by some programming code

# ROTATION

The converted binary image will be rotated to a certain angle using certain code. The angle for rotation is determined with the help of random function that generates any random number and this random value is considered for the angle using gnu octave. This is again set as a key for decryption. After rotation the image rotated at a particular angle is obtained.

# 

# Figure 5.1.2 Image Rotation

# ENCRYPTION

The original image and rotated image will be encrypted using Advanced Encryption standard. AES follows four major steps and they are add round key, mix columns, substitute byte, shift rows .AES can be implemented with either 128 bit or 256 bit. We use 256 bit i.e.32byte and key generated from random function is used to encrypt the processed and rotated image. It is based on substitution permutation network structure and consists of block sizes of 128 bits. It consists of 10,12 or 14 rounds based on the key size and each round follows all the three operations.

**5.1.4. IMAGE HIDING**

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. Steganography includes the concealment of information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. For example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.So, in our project, we combine the encrypted text and it is combined with a normal fingerprint image to confuse the hackers. The hackers might consider it as the original image but that image consists of some encrypted text and that text is decrypted and rotated to get the actual fingerprint image.

**5.1.5 DECRYPTION**

When the image is to be retrieved it can be decrypted using the same algorithm as that of used for encryption.The sane key randomly generated is used for decryption and the same four steps are followed and then the decrypted image is finally rotated to that particular angle which was mentioned and set earlier.This gives a final enhanced original fingerprint image used.

**CHAPTER 6**

**CONCLUSION AND FUTURE ENHANCEMENT**

* 1. **CONCLUSION**

For an image, preprocessing is necessary. The fingerprint image is preprocessed to enhance its quality. And the pre-processed image is rotated and encrypted using AES algorithm and GNU octave. The AES algorithm is the one of the most powerful cryptographic algorithms and even for more security, the output returned by that algorithm is hidden in a normal fingerprint image and that image is stored in the database.

# FUTURE ENHANCEMENT

As future work, we are trying to extract features that is minutiae extraction and try to encrypt them which will increase the further encryption process and also to use efficient steganographic algorithm for hiding the image or text in other fingerprint image.

**REFERENCES**

[1] Anil K. Jain*, Fellow, IEEE*, Salil Prabhakar, Lin Hong, and Sharath Pankanti, ” Filterbank-Based Fingerprint Matching”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 9, NO. 5, MAY 2000

[2] Qinghan Xiao,“Security Issues in Biometric Authentication”, Proceedings of the *2005* IEEE Workshop on Information Assurance and Security United States Military Academy, West Point

[3] Metodi P. Yankov, Member, IEEE, Martin A. Olsen, Mikkel B. Stegmann, Søren Sk. Christensen, and Søren Forchhammer, Member, IEEE,” Fingerprint Entropy and Identification Capacity Estimation Based on Pixel-level Generative Modelling” ,Journal of Latex Class Files, Vol 14, No. 8,August 2015

[4] Arun Pratap Srivastava, Shashank Awasthi, Awanish Kumar Kaushik, Shubham Shukla,” Fingerprint Recognition System using MATLAB”, 2019 International Conference on Automation, Computational and Technology Management (ICACTM)

Amity University

[5]Naomi Estera Costea, Elisa Valentina Moisi,” Fingerprint Authentication for Budget Application”, 15th International Conference on Engineering of Modern Electric Systems (EMES),2019

# [6] Tuy Nguyen Tan ,Hanho lee ,” High-Secure Fingerprint Authentication System Using Ring-LWE Cryptography “,IEEE Access ( Volume: 7 ), 2019

# [7] Michel Abdalla , Fabrice Benhamouda , David Pointcheval , Public-key encryption indistinguishable under plaintext-checkable attacks, IET Information Security,( Volume: 10), 2016

[8] Wencheng Yang,Jiankun Hu and Song Wang, “ A Delaunay Quadrangle-Based Fingerprint Authentication System with Template Protection Usong Topology Code for Local Registration and Security Enhancement”, July 2015

[9] Joppe W Bos, Criag Costello and Michael Naehrig,” Post- Quantum Key Exchange for the TLS Protocol from the Ring learning with Errors Problems,2016

[10] Reza Azarderaksh, Kimmo U.Jarvinen and Mehran,” Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications “, January 2015