

PRIVACY PRESERVING FINGERPRINT AUTHENTICATION BASED ON CANCELABLE BIOMETRICS

A Thesis submitted to Gujarat Technological University

for the award of

Doctor of Philosophy

in

Computer/IT Engineering

by

Shaikh Ayeshabanu Sibgatulla

Enrollment No.: 179999913028

under supervision of

Dr. Vibha D. Patel



**GUJARAT TECHNOLOGICAL UNIVERSITY
AHMEDABAD**

September - 2026

PRIVACY PRESERVING FINGERPRINT AUTHENTICATION BASED ON CANCELABLE BIOMETRICS

A Thesis submitted to Gujarat Technological University

for the award of

Doctor of Philosophy

in

Computer/IT Engineering

by

Shaikh Ayeshabanu Sibgatulla

Enrollment No.: 179999913028

under supervision of

Dr. Vibha D. Patel



**GUJARAT TECHNOLOGICAL UNIVERSITY
AHMEDABAD**

September - 2026

© Shaikh Ayeshabanu Sibgatulla

DECLARATION

I declare that the thesis entitled **Privacy Preserving Fingerprint Authentication Based On Cancelable Biometrics** submitted by me for the degree of Doctor of Philosophy is the record of research work carried out by me during the period from May 2018 to February 2024 under the supervision of Dr. Vibha Patel and this has not formed the basis for the award of any degree or diploma, associateship, fellowship, titles in this or any other University or other institution of higher learning.

I further declare that the material obtained from other sources has been duly acknowledged in the thesis. I shall be solely responsible for any plagiarism or other irregularities, if noticed in the thesis.

A.S. Shaikh

Signature of the Research Scholar :

Date : 21/09/2026

Name of Research Scholar : Shaikh Ayeshabanu Sibgatulla

Place : Ahmedabad

CERTIFICATE

I certify that the work incorporated in the thesis **Privacy Preserving Fingerprint Authentication Based On Cancelable Biometrics** submitted by Shaikh Ayeshabanu Sibgatulla was carried out by the candidate under my supervision/guidance. To the best of my knowledge: (i) the candidate has not submitted the same research work to any other institution for any degree/diploma, Associateship, Fellowship or other similar titles (ii) the thesis submitted is a record of original research work done by the Research Scholar during the period of study under my supervision, and (iii) the thesis represents independent research work on the part of the Research Scholar.

Signature of Supervisor :



Date : 21/09/2026

Name of Supervisor : Dr. Vibha D. Patel

Place : Ahmedabad

Course-work Completion Certificate

This is to certify that Ms. Shaikh Ayeshabanu Sibgatulla enrollment no. 179999913028 is a PhD scholar enrolled for PhD program in the branch of Computer/IT Engineering of Gujarat Technological University, Ahmedabad.

(Please tick the relevant option(s))

- ☐ He/She has been exempted from the course-work (successfully completed during M.Phil Course)
- ☐ He/She has been exempted from Research Methodology Course only (successfully completed during M.Phil Course)
- ☐ He/She has successfully completed the PhD course work for the partial requirement for the award of PhD Degree. His/ Her performance in the course work is as follows-

Grade Obtained in Research Methodology (PH001)	Grade Obtained in Self Study Course (Core Subject) (PH002)
BB	AB


Supervisor's Sign:

Dr. Vibha D. Patel

(Name of Supervisor)

Originality Report Certificate

It is certified that PhD Thesis titled **Privacy Preserving Fingerprint Authentication Based On Cancelable Biometrics** by Shaikh Ayeshabanu Sibgatulla has been examined by us. We undertake the following:

- a. Thesis has significant new work / knowledge as compared already published or are under consideration to be published elsewhere. No sentence, equation, diagram, table, paragraph or section has been copied verbatim from previous work unless it is placed under quotation marks and duly referenced.
- b. The work presented is original and own work of the author (i.e. there is no plagiarism). No ideas, processes, results or words of others have been presented as Author own work.
- c. There is no fabrication of data or results which have been compiled / analysed.
- d. There is no falsification by manipulating research materials, equipment or processes, or changing or omitting data or results such that the research is not accurately represented in the research record.
- e. The thesis has been checked using Turnitin (copy of originality report attached) and found within limits as per GTU Plagiarism Policy and instructions issued from time to time (i.e. permitted similarity index <10%).

A.S. Sheikh

Signature of the Research Scholar :

Name of Research Scholar : Shaikh Ayeshabanu Sibgatulla

Date : 21/09/2026

Place : Ahmedabad

Signature of Supervisor :

Name of Supervisor : Dr. Vibha D. Patel

Date : 21/09/2026

Place : Ahmedabad

Ayesha Sheikh

Thesis

- Research Thesis
- Research work Personal
- Institute of Technology, Nirma University

Document Details

Submission ID
0900001-13439436288

108 Pages

Submission Date
Dec 9, 2025, 9:36 PM GMT+5:30

32,580 Words

Download Date
Dec 9, 2025, 9:29 PM GMT+5:30

189,831 Characters

File Name
AS-Dec-2025.pdf

File Size
2.1 MB



Page 1 of 118 - Cover Page

Submission ID: 0900001-13439436288

8% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography
- Quoted Text
- Cited Text
- Small Matches (less than 9 words)

Exclusions

- 95 Excluded Matches

Match Groups

- 184 Not Cited or Quoted 0%
Matches with neither in-text citation nor quotation marks
- 0 Missing Quotations 0%
Matches that are still very similar to source material
- 0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation
- 0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

- 0% Internet sources
- 0% Publications
- 0% Submitted works (Student Papers)

Integrity Flags

1 Integrity Flag for Review

- Replaced Characters
48 suspect characters on 26 pages
Letters are swapped with similar characters from another alphabet

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

A. S. Sheikh

PhD THESIS Non Exclusive License to GUJARAT TECHNOLOGICAL UNIVERSITY

In consideration of being a PhD Research Scholar at GTU and in the interests of the facilitation of research at GTU and elsewhere, Shaikh Ayeshabanu Sibgatulla having (Enrollment No.: 179999913028) hereby grant a non-exclusive, royalty free and perpetual license to GTU on the following terms:

- a) GTU is permitted to archive, reproduce and distribute my thesis, in whole or in part, and/or my abstract, in whole or in part (referred to collectively as the “Work”) anywhere in the world, for non-commercial purposes, in all forms of media;
- b) GTU is permitted to authorize, sub-lease, sub-contract or procure any of the acts mentioned in paragraph (a);
- c) GTU is authorized to submit the Work at any National / International Library, under the authority of their “Thesis Non-Exclusive License”;
- d) The Universal Copyright Notice (©) shall appear on all copies made under the authority of this license;
- e) I undertake to submit my thesis, through my University, to any Library and Archives. Any abstract submitted with the thesis will be considered to form part of the thesis.
- f) I represent that my thesis is my original work, does not infringe any rights of others, including privacy rights, and that I have the right to make the grant conferred by this non-exclusive license.
- g) If third party copyrighted material was included in my thesis for which, under the terms of the Copyright Act, written permission from the copyright owners is required, I have obtained such permission from the copyright owners to do the acts mentioned in paragraph (a) above for the full term of copyright protection.

- h) I understand that the responsibility for the matter as mentioned in the paragraph (g) rests with the authors / me solely. In no case shall GTU have any liability for any acts / omissions / errors / copyright infringement from the publication of the said thesis or otherwise.
- i) I retain copyright ownership and moral rights in my thesis, and may deal with the copyright in my thesis, in any way consistent with rights granted by me to my University in this non-exclusive license.
- j) GTU logo shall not be used /printed in the book (in any manner whatsoever) being published or any promotional or marketing materials or any such similar documents.
- k) The following statement shall be included appropriately and displayed prominently in the book or any material being published anywhere: "The content of the published work is part of the thesis submitted in partial fulfilment for the award of the degree of Ph.D. in Computer/IT Engineering of the Gujarat Technological University"
- l) I further promise to inform any person to whom I may hereafter assign or license my copyright in my thesis of the rights granted by me to my University in this nonexclusive license. I shall keep GTU indemnified from any and all claims from the Publisher(s) or any third parties at all times resulting or arising from the publishing or use or intended use of the book / such similar document or its contents.
- m) I am aware of and agree to accept the conditions and reregulations of PhD including all policy matters related to authorship and plagiarism.

Signature of the Research Scholar :

A.S. Sheikh

Name of Research Scholar : Shaikh Ayeshabanu Sibgatulla

Date : 21/09/2026

Place : Ahmedabad

Recommendation of the Supervisor : Recommended

Signature of Supervisor :

Usha

Thesis Approval Form

The viva-voce of the PhD Thesis submitted by Ms. Shaikh Ayeshabanu Sibgatulla (Enrollment No.: 1799999913028) entitled Privacy Preserving Fingerprint Authentication Based On Cancelable Biometrics was conducted on 21/09/2026, Monday at Gujarat Technological University.

(Please tick any one of the following option)

- ☒ The performance of the candidate was satisfactory. We recommend that he/she be awarded the PhD degree.
- ☐ Any further modifications in research work recommended by the panel after 3 months from the date of first viva-voce upon request of the Supervisor or request of Independent Research Scholar after which viva-voce can be re-conducted by the same panel again.

(briefly specify the modifications suggested by the panel)

- ☐ The performance of the candidate was unsatisfactory. We recommend that he/she should not be awarded the PhD degree.

(The panel must give justifications for rejecting the research work)

Dr. Vibhe Patel
Name and Signature of Supervisor with Seal

Dr. Kamal Mehta
1) (External Examiner 1) Name and Signature

2) (External Examiner 2) Name and Signature

Dr. Suraj Parakash Agnihotri

ABSTRACT

The IT security paradigm has evolved from secret-based to biometric identity-based. Biometric identification has become gradually more popular in recent years for handheld devices. Privacy preservation is a key concern when biometrics are used in authentication systems in the present world. Nowadays, the declaration of biometric traits has been imposed not only by the government but by many private entities as well. There are no proper mechanisms or assurances that biometric traits will be protected by these entities. The encryption of biometric traits to avoid privacy attacks is a giant problem. Hence, state-of-the-art safety and security technological solutions must be devised to prevent the loss and misuse of such biometric traits. In classical authentication systems, either users need to remember a password (knowledge-based identification system) or must carry ID proof (token-based identification system). Over the last decades, biometric authentication systems have emerged as an alternative to classical authentication systems where your body is your password (e.g., fingerprint, face, or voice). The prime advantage of biometric traits is that they can never be lost or forgotten. On the other hand, if any of the biometric traits get compromised, then the user will not be able to change them like a password. In the real world, while biometric authentication is becoming increasingly popular, privacy and security risks related to its usage are raising several concerns.

Biometric authentication systems have become more popular nowadays because of mobile and other handheld devices since they eliminate the need for a password or pin to remember. The usage of the internet and other handheld smart devices promotes the theft of users' biometric traits, which frequently results in a loss of privacy. If an intruder hacks biometric traits, there is no way to change the biometric traits of any person because they are permanently attached to them. The biometric traits are not replaceable like passwords; hence, the key research area is privacy preservation. To stop such biometric traits from being stolen or used improperly, secure technology solutions must be developed. Protecting biometric template data is essential for preventing the loss of user privacy and identification. An effective and efficient approach that focuses on the security and privacy issues of biometric traits is required. The prime threat associated with biometric authentication is identity theft. Any attack that recovers the biometric template may have a serious impact since

users cannot change their biometric traits. Hence, biometric templates must be protected to thwart any leakage, as biometric traits are extremely susceptible to change. In privacy-preserving biometric authentication systems, the biometric data is stored in a secure form, which transforms the data into a distorted version and matches the trait in the transformed domain at the time of recognition.

The study investigates the fundamental and applied problem of security and privacy of biometric traits. There is a need for secure and non-invertible privacy-preserving biometric authentication systems to address the limitations by developing novel methods of cancelable biometrics using discrete cosine transformation and index of max hashing for securing biometric traits. In the proposed method, index of maximum hashing offers robust concealment of biometric traits, thereby strengthening the non-invertibility guarantee and enhancing overall template security.

In this study, we present a cancelable template generation approach based on index of max hashing, the fast fourier transform, the hadamard product, and speeded-up robust features-based feature extraction. Both theoretical analysis and empirical evidence demonstrate that index of maximum hashing effectively preserves accuracy by maintaining rank correlation properties. The proposed method also satisfies non-invertibility requirements for template protection. Furthermore, with appropriately calibrated parameters, it exhibits strong resistance to several prevalent security and privacy attacks.

In recent years, deep learning algorithms have emerged as some of the most successful artificial intelligence approaches for feature extraction tasks. Among various deep learning methods, convolutional autoencoders have been adopted and have demonstrated substantial performance in the biometric domain. This research proposes methods for non-invertible cancelable biometrics based on convolutional autoencoder to secure biometric traits and address the problem of privacy preservation. All the proposed techniques have been carefully thought out and tested on FVC2002 datasets. The hyperparameters of the models are tuned and thoroughly tested. The outcomes of the suggested procedures are compared with those of the other traditional techniques.

Acknowledgement

To begin with, I must first give gratitude and praise to God, the Almighty, for his numerous blessings that enabled me to successfully complete my research.

I would like to express my sincere gratitude to my advisor Dr. Vibha D. Patel, Professor & Head, Vishwakarma Government Engineering College, GTU, for the continuous support throughout my Ph.D. study and related research through her patience, motivation, and immense knowledge. She has given me all the freedom to pursue my research, while silently and non-obtrusively ensuring that I stay on course and do not deviate from the core of my research. I could not have imagined having a better advisor and mentor for my Ph.D. study.

I prolong my sincere thanks to my DPC member, Dr. Mehul S. Raval, Professor and Associate Dean - Experiential Learning, Dept. of IT/CE, Ahmedabad University. He critically evaluated my work with thoughtful suggestions and timely assessment with genuine review comments. I would also like to thank my DPC member, Dr. Mukesh A. Zaveri, Associate Professor, SVNIT, Surat for his insightful comments and encouragement, which motivated me to widen my research from various perspectives.

My sincere thanks also go to the IT Department, Charusat University and R. C. Technical Institute which provided me an opportunity to access the library, and research facilities. Without their precious support, it would not be possible to conduct this research. I thank my colleagues for stimulating discussions in the last five years. Also, I would like to thank my friends Prof. Bela Shrimali, Prof. Ankita Kapadia and Prof. Usha Patel. My acknowledgment would be incomplete without thanking the biggest source of my strength, my family. I would like to thank my family: my parents, my husband-Mohsin, my daughter-Ayzal, my sister-Nabila, my brother-Zafar, my sister-in-law-Anisha and my nephews-Eshal and Qindeel for supporting me spiritually throughout writing this thesis and my life in general.

Shaikh Ayeshabanu Sibgatulla

Contents

List of Figures	xvi
-----------------	-----

List of Tables	xvii
----------------	------

1	Introduction	1
1.1	Overview of fingerprint authentication system	1
1.1.1	Biometric authentication system	1
1.1.1.1	Privacy-preserving biometric authentication	2
1.1.1.2	Vulnerabilities and possible solutions of biometric authentication systems	3
1.1.1.3	Biometric template protection	5
1.1.2	Applications	8
1.1.3	Challenges	9
1.2	Research problem and objectives	10
1.2.1	Problem statement	10
1.2.2	Objectives	10
1.3	Contributions	10
1.4	Outlines of thesis	11
2	Background and literature review	13
2.1	Background	14
2.1.1	Dataset	14
2.1.2	Evaluation Metrics	14
2.2	Literature review	15
2.2.1	Biometric Template Protection	15
2.2.2	Objectives of Biometric Template Protection	18
2.2.3	Methodology of Biometric Template Protection	18
2.2.3.1	Cancelable Biometrics	20

Contents

2.2.3.2	Biometric Cryptosystem	28
2.3	State of the Art: Biometric Template Security	31
2.3.1	Security Analysis of Biometric Template Transformation	35
2.4	Summary	37
3	Cancelable biometrics based fingerprint template protection using discrete cosine transform and index of max hashing	38
3.1	Introduction	38
3.2	Cancelable biometric template protection	39
3.2.1	Methods for Generating Cancelable Templates	39
3.2.2	Preliminaries	40
3.2.2.1	Discrete cosine transform	41
3.2.2.2	Locality sensitive hashing	42
3.2.2.3	Index of max hashing	43
3.3	Methodology	44
3.4	Experiment and analysis	46
3.5	Summary	51
4	Cancelable biometrics for fingerprint template security based on speeded up robust feature, fast fourier transform and index of max hashing	52
4.1	Introduction	52
4.2	Cancelable fingerprint biometric template protection	53
4.2.1	Preliminaries	54
4.2.1.1	Speeded-up robust features	54
4.2.1.2	Fast Fourier Transform	55
4.2.1.3	Index of Max Hashing	56
4.3	Methodology	56
4.4	Experiment and analysis	58
4.5	Summary	61
5	Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing	62
5.1	Introduction	62
5.2	Learning based biometric template protection	63
5.2.1	Machine/deep learning-based feature learning approaches	66
5.2.1.1	Supervised machine/deep learning approaches	66

5.2.1.2	Unsupervised machine/deep learning approaches	70
5.3	Methodology	75
5.3.1	Architecture and training	77
5.3.2	Cancelable template generation	78
5.4	Experiment and analysis	79
5.5	Summary	83
6	Conclusion and Future Work	84
6.1	Conclusion	84
6.1.1	Future Work	85
	References	86
7	List of Publication	93

List of Figures

1.1	Privacy Preserving Biometric Authentication System	2
1.2	Biometric system vulnerabilities and underlying causes	4
1.3	List of template protection schemes in the biometric system	6
2.1	FVC2002 DB1 and FVC2002 DB2 Fingerprint Datasets	13
2.2	Biometric template protection schemes	19
2.3	Fingerprint images (a) different fingerprint feature points (b) feature points and singular point (c) example of distorted fingerprints	20
3.1	Distortion transform based on feature perturbation	39
3.2	Diagram of the proposed cancelable biometrics scheme	45
3.3	EER (%) vs k on FVC2002(DB1)	47
3.4	EER (%) vs k on FVC2002(DB2)	48
3.5	EER (%) vs m-independent hash functions on FVC2002(DB1)	48
3.6	EER (%) vs m-independent hash functions on FVC2002(DB2)	50
4.1	SURF Fingerprint Feature Detection	55
4.2	FAR and FRR versus threshold - FVC2002 database	59
4.3	Accuracy plots for the proposed technique on FVC2002 database	59
4.4	Comparison of EER for the proposed methods on FVC2002 database	60
5.1	Convolutional autoencoder model [1]	76
5.2	Fingerprint Convolutional Autoencoder Architecture	77
5.3	The proposed method's block diagram	78
5.4	Training and validation loss of convolution autoencoder	80
5.5	ROC plots for the proposed technique on different datasets—Equal Error Rate (EER%): 0.1306 - FVC2002 DB1	80
5.6	ROC plots for the proposed technique on different datasets—Equal Error Rate (EER%): 0.0861 - FVC2002 DB2	81
5.7	ROC plot and Genuine-impostor distributions for the proposed technique on FVC2002 dataset	82

List of Tables

1.1	Possible solutions of different attacks on biometric authentication system	5
2.1	Dataset Summary	14
3.1	EER (%) vs k on FVC2002(DB1) with hashing functions m=600	47
3.2	EER (%) vs m on FVC2002(DB1)	49
3.3	EER (%) vs m on FVC2002(DB2)	49
3.4	Equal error rate (EER) of different cancelable biometrics	50
4.1	Comparison of Cancelable biometric methods for protecting fingerprint templates	54
5.1	Winner-take-all hashing Hashing Example with three input vectors x_1 , x_2 , x_3 , window size K and one permutation θ . x_1 and x_2 are unrelated and result in different output codes, each element in x_3 has been perturbed by 1, which changes the ranking of the items but keeps the maximum of the first K elements the same, yielding the same code once more.	79
5.2	Specification of the experimental datasets	81
5.3	Performance Comparison	82

CHAPTER - 1

Introduction

The fundamentals of fingerprint authentication system and biometric template protection are covered in this chapter. Further, the problem statement of the research is defined. The major objectives and the contributions of the research study are further described.

1.1 Overview of fingerprint authentication system

The IT security paradigm has evolved from secret-based to biometric identity-based. Biometric identification has become gradually more popular in recent years for handheld devices. Privacy-preserving is a key concern when biometrics is used in authentication systems in the present world today. Nowadays the declaration of biometric traits has been imposed not only by the government but by many private entities also. There are no proper mechanisms and assurance that biometric traits will be kept safe by such entities. The encryption of biometric traits to avoid privacy attacks is a giant problem. Hence, state-of-the-art safety and security technological solutions must be devised to prevent the loss and misuse of such biometric traits.

1.1.1 Biometric authentication system

In classical authentication systems, either users need to remember a password (knowledge-based identification system) or have to carry ID proof (token-based identification system). Over the last decades, biometric authentication systems have emerged as an alternative to classical authentication systems where your body is your password (e.g. fingerprint, face, or voice). The prime advantage of biometric traits is that they can never be lost or forgotten. On the other hand, if any of the biometric traits get compromised then the user will not be able to change it like a password. In the real world, while biometric authentication is

Introduction

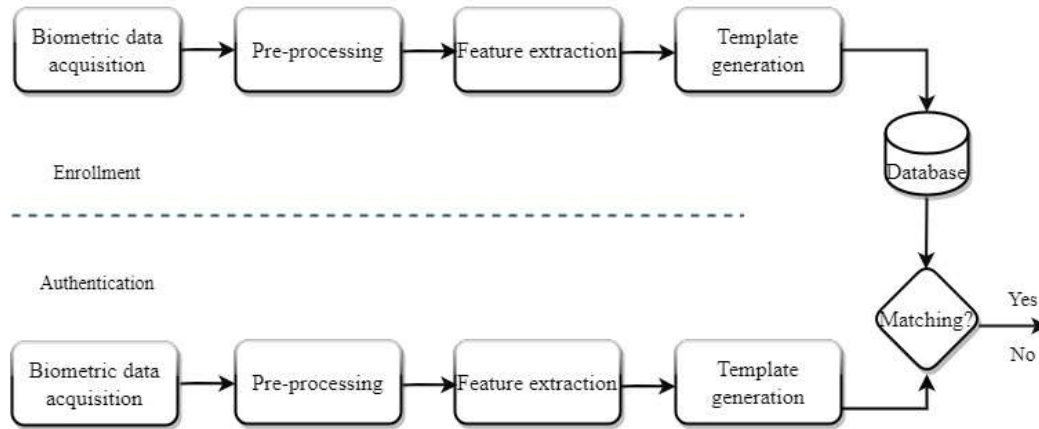


FIGURE 1.1 Privacy Preserving Biometric Authentication System

becoming gradually more popular, the privacy and security risks related to their usage are raising several concerns[2].

Biometric authentication systems use a person's voice, gait, fingerprints, face, iris, or other physical or behavioural characteristics to identify them. The compromise of any of the biometric traits of an individual may cause permanent identity theft that cannot be recovered. Hence, the biometric templates are derived from the biometric traits of an individual, which contain the person's obscure information [3]. If the biometric template is tainted, the same biometric traits can be used to construct a new multiple template. The two stages of the authentication procedure are the enrollment phase and the identification phase [4]. During the enrollment phase, biometric traits are extracted from individuals and stored in databases as biometric templates. During the identification step, biometric samples are retrieved from people and compared to those in the database [5]. If a match is found, the person is recognised as legitimate and is allowed to access the services. If no match is found, the person is considered illegitimate and is not permitted to use the services [6].

1.1.1.1 Privacy-preserving biometric authentication

Biometric authentication systems have become more popular nowadays because of mobile and other handheld devices since they eliminate the need for a password or PIN to remember. The usage of the internet and other handheld smart devices promotes the theft of users' biometric traits, which frequently results in a loss of privacy. If an intruder hacks biometric traits, there is no way to change the biometric traits of any person because they are permanently attached to the person. The biometric traits are not replaceable like passwords; hence, the key research area is privacy preservation. To stop such biometric traits from being stolen

1.1 Overview of fingerprint authentication system

or used improperly, secure technology solutions must be developed. Protecting biometric template data is essential for preventing the loss of user privacy and identification. An effective and efficient approach that focuses on the security and privacy issues of biometric traits is required.

The prime threat associated with biometric authentication is identity theft. Any attack that recovers the biometric template may have a serious impact since users can not change their biometric traits. Hence biometric templates must be protected to thwart any leakage as the biometric traits are extremely susceptible to change. In privacy-preserving biometric authentication systems, the biometric data is stored in a secure form which transforms the data into a distorted version and also matches the trait in the transformed domain at the time of recognition.

A number of assaults can be made against the biometric systems. The stored template attack is the most damaging to the biometric systems [7]. The sample biometrics of a person captured during the enrollment process are stored in the form of biometric templates. In the authentication process, biometric templates are crucial. Unlike passwords, templates cannot be cancelled or issued again after being compromised. The identity of the person is lost when his biometrics are compromised. Therefore, providing security and revocability to biometric templates are two prime issues [8] as indicated in figure 1.1, a privacy preserving biometric authentication system is necessary to address these challenges. Attacks against biometric systems are classified as zero effect attacks and adversary attacks. The Zero Effect attack results from a coincidental resemblance between templates from several sources. The adversary attack is due to an imposter who masquerades as a legitimate user [9]. Even though biometric systems provide convenience and security, they are subjected to various types of threats identified a number of potential attacks against a biometric system.

1.1.1.2 Vulnerabilities and possible solutions of biometric authentication systems

The extensive use of biometric templates begs the question of the security of these applications. A system could be hacked by a fraudster or impersonator, who might also steal biometric information. A template is undoubtedly more difficult to read and misuse than conventional passwords and tokens because it is a series of zeros and ones in a mathematical file. Biometric templates are digital representations of captured biometrics like fingerprints, iris, faces, etc. The biometric matcher doesn't make use of the original images. The similarity score, which is a vector representing the likelihood that two biometric templates match, is what the template matcher generates. Concerning templates, there are a few elements that could be compromised, like template databases, which are vulnerable to theft. Designing

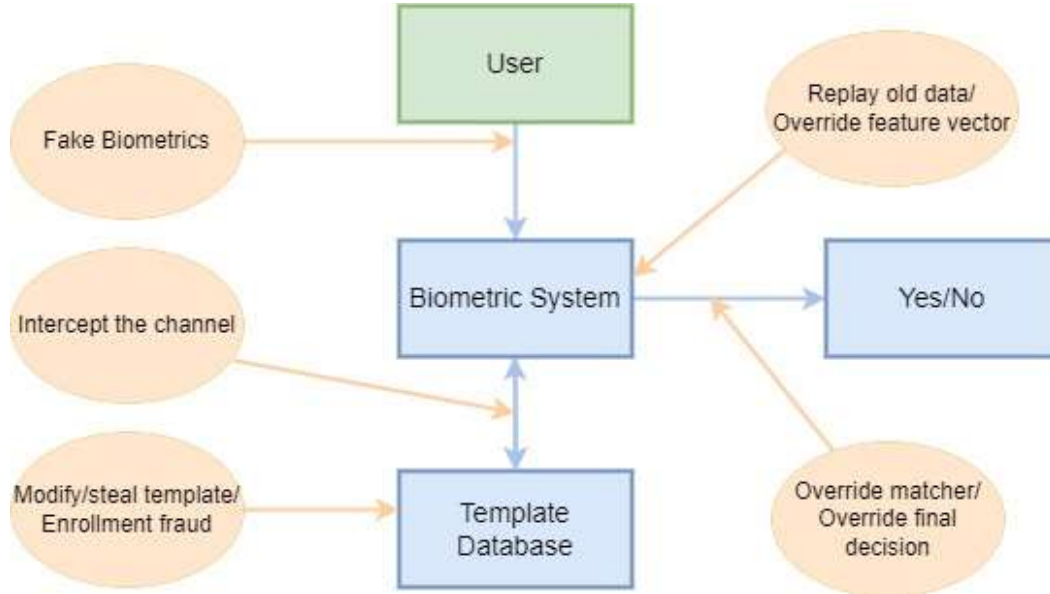


FIGURE 1.2 Biometric system vulnerabilities and underlying causes

a biometric protection system is a significant challenge since it must be able to manage intrauser variations in the collected biometric identifiers [10]. The following four characteristics are appropriate for a strong biometric template protection system that can manage intrauser variability: Diversity, Revocability, Security, and Performance.

A biometric system is additionally susceptible to a variety of system attacks that take advantage of the system's insecure infrastructure, such as a replay attack, insider attacks or administrative loopholes, denial-of-service attacks, altering the template database, or overruling a system choice at several stages, such as feature extraction, matching, or ultimate decision [11]. The biometric-based authentication system's architectural diagram, highlighting its main weaknesses and their underlying causes, as shown in figure 1.2.

There are many different ways to defend against attacks on biometric authentication systems. Our primary focus in this paper is on the safety of the template database. We must come up with a protection against modifying the database template. Cancelable biometrics and biometric cryptosystems, which offer security against alteration of the database template, are two such options that can be used. Soft biometrics, multimodal biometric systems, and liveness detection are some potential countermeasures against sensor attacks. Steganography, watermarking techniques, and challenge-response systems are possible remedies for replay attacks [2]. The remedy for overriding final decisions may be based on soft biometrics as shown in table 1.1.

1.1 Overview of fingerprint authentication system

TABLE 1.1 Possible solutions of different attacks on biometric authentication system

Attacks	Solutions
Attack on the sensor	Liveness detection, multi-modal biometric systems, soft biometrics
Replay attack	Steganographic and watermarking techniques, challenge-response systems
Attack on the database	Cancelable biometrics/feature transformation, biometric cryptosystem
Attack on the channel between the matcher and database	Steganographic and watermarking techniques, challenge-response systems
Overriding final decision	Soft biometrics

A biometric system is the most authentic way to provide security but still there are many loopholes in the system which needs to be entertained. Intruders can attack at different points of the biometric system like try to steal the data, provide fake biometrics, replay old data, modify template database or override the decision of the system at different levels as feature extractor level, matching level or final decision.

There are numerous possible solutions of different attacks on biometrics authentication systems. In this paper, our main concern is the security of the template database. We need to find a solution against modification of the database template. Two such possible solutions can be cancelable biometrics and biometric cryptosystem which provides security against database template modification[12].

The possible solutions of attack on the sensor can be liveness detection, multi-modal biometric systems and soft biometrics. The replay attack solutions can be steganography, watermarking techniques and challenge-response systems [8]. The attacks on the database can cope up with the solutions like Cancelable biometrics/feature transformation and biometric cryptosystem. The possible solutions of attack on the channel between the matcher and database are steganography, watermarking techniques and challenge-response systems. The solution of overriding final decisions can be soft biometrics [13]

1.1.1.3 Biometric template protection

To secure biometric templates from attacks by enemies, many protective methods are used. The many types of Biometric Template Protection techniques are depicted as shown in figure 1.3. Biometric cryptosystem [6] and cancelable biometrics [14] approach are the two primary

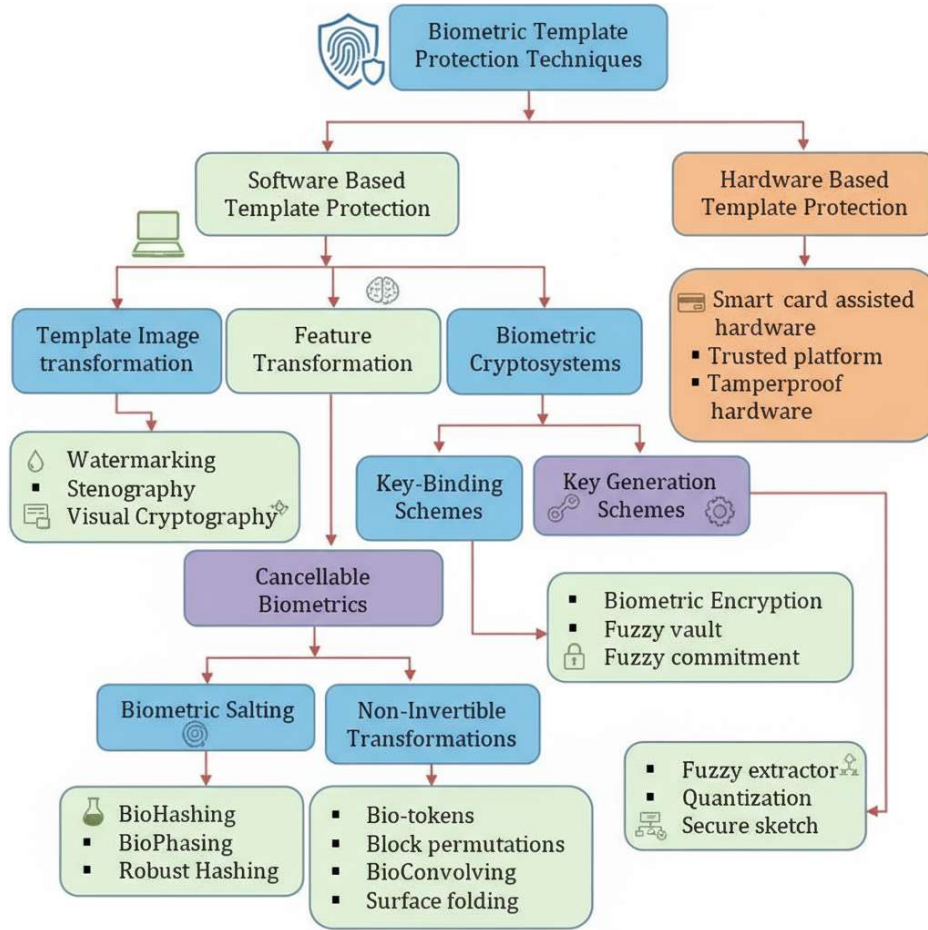


FIGURE 1.3 List of template protection schemes in the biometric system

categories into which biometric template protection methods fall. A transformation function is used in the cancelable biometrics approach to transform the acquired biometric template, and only the altered version is saved in the database. Typically, a randomly generated key or password is used to determine the transformation function's parameters. Helper data is saved in the biometric cryptosystem's template protection scheme. To extract a cryptographic key from the query biometric template, helper information is needed. After that, indirect matching is carried out by confirming the accuracy of the produced cryptographic key.

Depending on how the transformation function is configured, the cancelable biometrics technique is further categorized into two: salting and non-invertible transform. In the salting approach, if the intruder may get access to the key and salting template then he can easily get back the original biometrics from the transformation function. However, as the name implies, a non-invertible transformation cannot be reversed. Even if the key is known, it is very challenging to invert a changed template to the original template because it is a one-way

1.1 Overview of fingerprint authentication system

function. Following the method used to collect the auxiliary data, biometric cryptosystems are further divided into key binding and key generation. In a key-binding system, the biometric template is bonded to a key to extract the helper information. It is not easy to recover the key or the original biometric trait using the helper data. In a key generation biometric cryptosystem, the helper data and query biometric features are combined to create the key. A hybrid template protection scheme employs one or more template protection strategies [15].

In order to enhance security in biometric facial recognition systems, the paper proposes a novel cancelable FaceHashing technique that combines cryptographic template encryption with non-invertible transformations. Preprocessing the input image to extract the relevant facial region is the first step in the multi-step process. After feature extraction, SIFT descriptors from the face region undergo advanced optimisation techniques like spatial pyramid matching and sparse representation. After feature computation, a non-invertible transformation creates protected feature vectors. These cancelable features are then further protected by RSA-based encryption and decryption. This dual protection strategy ensures that, even in the case of a breach, the original biometric data cannot be recovered from stored templates, in compliance with the privacy requirements of biometric systems. Performance results demonstrated that the technology maintains high recognition accuracy while significantly improving the security of stored biometric templates when compared to previous methods. Both the cancelable and encrypted versions of the features showed resilience against various attacks and template breach scenarios. The paper gives a thorough explanation of the findings. According to performance comparisons, the proposed system outperformed cutting-edge methods in terms of template protection and recognition reliability[16].

A primary technique for authenticating users is that of biometrics. However, it has many challenges, particularly those related to security, as discussed in [2]. The biometric template that is saved in the database should be safeguarded through the use of biometric template data protection techniques. The literature now provides two categories of biometric template security measures: protection methods based on transformation (cancelable biometrics) and biometric cryptosystems. Biometric cryptosystem [17] provides biometric template security based on biometric features and cryptography, whereas transformation-based techniques like cancelable biometrics use non-invertible transformation and salting. Cancelable biometrics refers to the intentional and consistently used distortion of biometric characteristics to safeguard private user information. A thorough review of various frameworks for the recognition and protection of biometric templates existing in the literature is presented here [18].

Introduction

It is possible to state that a secure fingerprint authentication method is necessary without sacrificing the system's authentication functionality. There are four main characteristics to comply with, and they are security, performance, revocability, and diversity [12]. In addition, the suggested technique's four key qualities are compared with the benefits and drawbacks of many other techniques now in use. The incentives contain possible advantages that should propel the application of the proposed method. Two major approaches, the feature transformation approach, and the biometric cryptosystem-based approach, are used to protect biometric templates [19]. Salting and non-invertible transformation-based approaches are further categories for feature transformation-based techniques. Key generation-based and key-binding-based biometric cryptosystem-based techniques are other subcategories. Based on these methods, several other methods have been suggested in the literature [20].

1.1.2 Applications

Because biometrics are more effective at differentiating people and providing personal security, they are used in a wide range of applications from a variety of industries. The major fields of applications are:

- With great potential for widespread use in a variety of civilian applications, biometrics is a rapidly developing technology that has been utilized extensively in forensics applications including criminal identification and prison security.
- The three categories into which these applications can be separated are commercial, government, and forensic.
- Applications of biometrics in the commercial sphere include electronic data security, e-commerce, internet access, ATMs, credit cards, physical access control, mobile phones personal digital assistants, medical records, etc.
- The government domain uses biometrics in applications such as driver's licenses, passport control, social security, border control, national ID cards, correctional facilities, etc.
- Biometrics are used in a variety of forensic settings, including Identification of corpses, criminal investigations, identification of terrorists, determination of parenthood, missing children, etc.

1.1.3 Challenges

The major challenges of biometrics security are described below and need to be solved.

- Design a transformation approach for cancelable biometrics such that the templates are easy to revoke, difficult to invert, and do not degrade performance.
- Designing a biometric template protection system that provides security without compromising accuracy is a challenging task.
- It is a complicated task to find an appropriate transformation function for cancelable biometrics because of the intra-class variability of biometric patterns.
- Assume that CT is a cancelable transform that converts biometric z to a cancelable biometric $CT(z)$, FM is a fingerprint matching technique, and DT is the decision threshold. The matcher uses two biometrics, z_1 and z_2 , to determine the matching or similarity score. $0 \leq FM(z_1, z_2) \leq 1$.

Intrauser variability: When z_1 and z_2 match, the probability of a false reject should not increase in the transformed domain.

$$FM(z_1, z_2) > DT \implies FM(CT(z_1), CT(z_2)) > DT \quad (1.1)$$

Interuser variability: When z_1 and z_2 do not match, the probability of a false accept should not increase in the transformed domain.

$$FM(z_1, z_2) \leq DT \implies FM(CT(z_1), CT(z_2)) \leq DT \quad (1.2)$$

Transformation function design: The biometric z 's transformed version $CT(z)$ should not be identical to the original biometric.

$$FM(CT(z), z) \leq DT \quad (1.3)$$

Cross-site matching: Multiple $CT_1(z)$ and $CT_2(z)$ templates derived from the same biometric z with different keys should not match.

$$FM(CT_1(z), CT_2(z)) \leq DT \quad (1.4)$$

No inverse transform: The inverse transform CT^{-1} should not exist such that the original biometric z should not be revocable from the modified one $CT(z)$.

1.2 Research problem and objectives

1.2.1 Problem statement

Designing a biometric template protection system that provides security without compromising accuracy is challenging. It is a complicated task to find an appropriate transformation function for cancelable biometrics because of the intra-class variability of biometric patterns. Assume that CT is a cancelable transform that converts biometric z to a cancelable biometric $CT(z)$. The biometric z 's transformed version $CT(z)$ should not be identical to the original biometric. The inverse transform CT^{-1} should not exist such that the original biometric z should not be revocable from the modified one $CT(z)$.

1.2.2 Objectives

The major objectives are defined as follows:

- To study and explore various existing privacy-preserving approaches and understand their limitations.
- Design a transformation approach for cancelable biometrics such that the templates are easy to revoke, difficult to invert, and do not degrade performance. (e.g. security without compromising accuracy)
- To achieve a good performance in terms accuracy of biometric systems.
- To discover highly discriminative features of the biometric traits using the learning-based approach, which helps to achieve better accuracy.
- Evaluating the performance of the proposed approaches by comparing them with existing approaches.

1.3 Contributions

The major contributions are:

- The thesis work proposes three different approaches that are implemented and compared with other state-of-the-art methods to evaluate the performance.

- The first proposed cancelable biometrics approach is based on a non-invertible transformation function using the concepts of discrete cosine transformation and uniformly random permutation-based index of max hashing with Hadamard transform.
- The second proposed cancelable biometrics approach is based on a speeded-up robust feature, fast fourier transform, and partial Hadamard transform with an index of max hashing.
- The third proposed cancelable biometrics approach is based on a learning-based approach using the concepts of autoencoder.

1.4 Outlines of thesis

The outlines of each chapter of the thesis are given below:

- **Chapter 1 : Introduction**

In this chapter, the basic of the fingerprint authentication system is elaborated. Then brief about the major applications and challenges of biometric template protection is given. Further, the problem statement of the research, followed by the major objective and contributions of the thesis, is described. At last, the organization of the thesis gives a brief about all the chapters.

- **Chapter 2: Background and literature review**

In this work, the dataset and evaluation metrics of biometrics are summarized in the literature. The different methods to deal with the protection of biometric templates are summarized. Cancelable biometrics are widely used among the various techniques and are the primary emphasis of this research, as elaborated in the subsequent section.

- **Chapter 3: Cancelable Biometrics Based Fingerprint Template Protection**

The idea and benefits of cancelable biometrics in protecting fingerprint templates are covered in this chapter. In order to protect user privacy and improve system security, it investigates techniques for creating revocable and non-invertible fingerprint representations. The design, application, and assessment of transformation strategies that enable safe template replacement without sacrificing recognition accuracy are prioritised.

- **Chapter 4: Speeded-up robust feature-based Cancelable Biometrics Based Fingerprint Template Protection**

A biometric template protection technique based on accelerated robust fingerprint recognition features is presented in this chapter. Its main goal is to create a cancelable biometric system that protects fingerprint templates using transformation methods while maintaining computational efficiency and matching accuracy. The suggested method's application and assessment show improved processing speed and resistance to inversion or reconstruction attacks.

- **Chapter 5: Learning Based Fingerprint Template Protection**

This chapter explores learning-based fingerprint template protection strategies. It outlines the design principles, implementation details, and conceptual underpinnings of learning-based techniques meant to improve the security and privacy of biometric templates. To demonstrate the efficiency and versatility of learning-driven models in real-world biometric systems, a comparison with conventional protection schemes is also provided.

- **Chapter 6: Conclusion and future work**

The conclusion of the research work conducted is presented in this chapter. Along with that, some of the future enhancements of the proposed work are also highlighted, which can be helpful for the research community of biometric security.

CHAPTER - 2

Background and literature review

The following sections present an overview of the contextual information pertinent to the research investigation. It covers details of the datasets used for the experimentation. Another important aspect of the experiment is the evaluation matrix. The background also covers details of the evaluation matrix. Nowadays, biometric template protection approaches are employed for safe authentication. A brief survey of various biometric template protection methods for the security of biometric traits is discussed further.

The comprehensive literature review discussed in this chapter provides the domain knowledge of cancelable biometrics with the deep neural networks, its challenges, and the solutions proposed in the scientific literature.

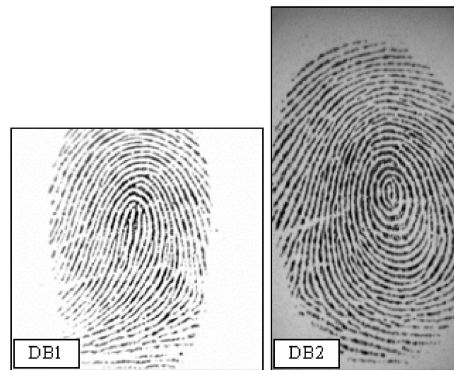


FIGURE 2.1 FVC2002 DB1 and FVC2002 DB2 Fingerprint Datasets

2.1 Background

2.1.1 Dataset

The experiment discussed in subsequent chapters is carried out on two publically available fingerprint datasets FVC2002 DB1 and DB2 as shown in figure 2.1 and specifications as per table 2.1.

Parameters	FVC2002 DB1	FVC2002 DB2
Total subjects	100	100
Samples per subject	8	8
Total number of fingerprint images	800	800
Quality of image	good to medium	good to medium
Resolution	500 dpi	569 dpi
Sensor type	optical Sensor	optical Sensor

TABLE 2.1 Dataset Summary

2.1.2 Evaluation Metrics

Biometric cryptosystem evaluation metrics assess the accuracy, security, and efficiency of the system. The primary evaluation metrics, arranged according to categories: Non-invertibility Evaluates the difficulty of using stored templates or assistance data to reverse-engineer the biometric data or key. Revocability: The ability to cancel and reissue biometric keys in the event that they are compromised. Unlinkability: Ensures that biometric templates cannot be connected to other databases or programs.

Statistical metrics like the Equal Error Rate (EER), False Accept Rate (FAR), and False Reject Rate (FRR) are used to quantify system accuracy in addition to these security parameters. Together, these metrics show how system robustness and user convenience are traded off.

False Acceptance Rate (FAR) / False Match Rate (FMR): This is the likelihood that the biometric system incorrectly matches the input to a template that should not be accepted (i.e., an imposter is accepted). The ratio of the number of false acceptances divided by the number of all imposter attempts.

False Rejection Rate (FRR) / False Non-Match Rate (FNMR): This is the likelihood that a valid user's biometric is incorrectly rejected. The ratio of the number of false rejections divided by the number of all genuine attempts.

Equal Error Rate (EER): It is the point of intersection of FRR and FAR values at particular threshold value. The lower the equal error rate value, the higher the accuracy of the biometric system.

Many genuine (valid users) and impostor (fraudulent attempts) samples are processed by the system. The system computes similarity scores (how closely samples match stored templates). By varying the threshold (the value above which a match is accepted), you can tabulate different rates: for instance, increasing the threshold decreases FAR but increases FRR, and vice versa. The threshold where FAR and FRR are closest or equal. The EER is identified graphically as the point where FAR and FRR are equal.

2.2 Literature review

This section thoroughly reviews relevant literature that provides insight into the topic. The first part covers various methods used for fingerprint biometric template protection. The subsequent section discusses different approaches to dealing with cancelable biometrics. Further, the different biometric cryptosystems methods proposed by the research community are discussed briefly. The next section addresses several strategies for hybrid biometric template protection.

2.2.1 Biometric Template Protection

A framework for protecting user privacy while securing biometric authentication on mobile platforms is presented in [21]. Strong biometric protection schemes that can defend off attacks like template leakage, replay attacks, and identity theft are essential, the paper notes, given the growing reliance on mobile devices for sensitive operations. The suggested framework is appropriate for resource-constrained mobile environments since it combines lightweight cryptographic protocols with biometric cryptosystems. To enable secure key binding without storing the raw biometric data, the authors suggest employing secure sketch mechanisms and fuzzy extractors to create stable cryptographic keys from noisy biometric inputs. The framework also allows for template revocability, which lets users reissue compromised templates. The approach is effective, protects privacy, and offers high authentication accuracy across a range of mobile biometric modalities, according to experimental results. The development of safe and intuitive biometric systems for mobile applications is greatly advanced by this work.

Background and literature review

For identity verification, biometric systems use behavioral or physiological characteristics (such as voice, face, iris, or fingerprints). However, because biometric traits cannot be altered if compromised, unlike passwords, the storage of biometric data raises special security and privacy issues. The paper describes vulnerabilities in various stages of biometric systems, including sensor input, feature extraction, template storage, and matching. It draws attention to possible attacks such as replay, template reconstruction, and spoofing. Because compromised templates can result in identity theft and a permanent loss of user trust, the authors contend that protecting biometric templates is essential. The paper examines a number of biometric template protection strategies to reduce these risks, such as cancelable biometrics, which allow modified biometric data to be revoked and reissued, and biometric cryptosystems, which bind a key with biometric data. The authors stress the importance of striking a balance between revocability, recognition performance, and template security. Additionally, they emphasize the significance of standardization and the assessment of protection schemes based on performance, diversity, and non-invertibility metrics. In the paper conclusion, a request for more research on reliable, approachable, and privacy-preserving biometric security systems is made [1].

The authors of *Security and Privacy in Biometrics* thoroughly analyze the theoretical underpinnings and real-world applications of fingerprint template protection schemes in [15]. They talk about the special difficulties that biometric data presents, like its permanence, non-revocability, and inter-user similarity, which leave it open to theft and abuse if not sufficiently safeguarded. By examining their fundamentals, benefits, drawbacks, and applicability for real-world systems, the authors divide protection strategies into two primary categories: feature transformation (cancelable biometrics) and biometric cryptosystems. The chapter highlights how crucial it is to meet the four fundamental requirements for fingerprint template protection: performance preservation, diversity, revocability, and non-invertibility. Based on these metrics, the authors assess a number of suggested schemes and talk about practical deployment factors like user acceptability, computational efficiency, and ease of integration. This work is an essential resource for researchers and developers working on safe and private biometric systems because it bridges the gap between theoretical security models and practical application constraints.

The authors of the paper [22] suggest a way to make revocable fingerprint templates that improve biometric systems' security and privacy. Applying a non-invertible transformation to the original fingerprint features—more especially, minutiae-based features—so that the resulting template cannot be linked to the original biometric data are the main idea. This guarantees that the original fingerprint cannot be recreated, even in the event that the template

is compromised. A user-specific key governs the transformation, enabling the creation of several revocable templates from a single biometric source. Template diversity and revocability are provided by the ability to issue a new template with a different key if one is compromised. The suggested scheme maintains high matching accuracy while providing strong resistance to common security threats like inversion, replay, and cross-database matching, according to the authors' validation of their method using fingerprint datasets. This work greatly aided the development of safe and privacy-conscious biometric systems

A comprehensive review of privacy-preserving biometric authentication systems is provided by [8], which highlights the challenges and risks that distinguish them from more traditional authentication methods. In the event that biometric data is compromised, the authors outline the serious concerns that biometric authentication systems face. These risks include identity theft, irrevocability (because biometrics cannot be updated like passwords), and the potential for user profiling and cross-database matching. The work highlights several key attack vectors, including biometric sample recovery, biometric reference recovery (especially through template or matching process attacks like center-search or hill-climbing), user traceability (allowing tracking across databases or attempts), and user distinguishability (cross-linking templates to actual identities). In order to minimise single points of failure, the authors describe distributed architectures and emphasise the importance of privacy-preserving techniques that encrypt data, restrict access, or use pseudonymization at each stage of authentication. Future research directions and tactics to counter these threats are covered in the study. Although they limit template reversibility, current template protection methods like biohashing and cancellable biometrics are vulnerable to some attacks. Secure multiparty computation (SMPC), homomorphic encryption, oblivious transmission, and garbled circuits are more robust cryptographic techniques that enable matching and decision-making on encrypted data without revealing the templates. However, these cryptographic systems often face problems with computational cost and error tolerance due to the inherent noise in biometric data. Other methods, such as the use of error correction codes, differential privacy, or Bloom filters to stop matching distances from leaking, are regarded as complementary strategies. The paper's conclusion highlights the importance of designing systems that balance privacy preservation, usability, and authentication performance and identifies the practicality and efficiency of cryptographic protocols as a major area for future research.

In the biometric recognition system, the privacy issues of the biometric trait are the main concern in both identification or verification process. In a database instead of storing the biometric traits in a plain format using the biometric template the traits can be stored in the distorted format so if the intruder will get the template he or she will not be able to crack or

recover the original biometric traits from the distorted template. The distortion can be applied by different methods of Biometric template protection. The biometric template protection schemes can be broadly classified in cancelable biometrics and biometric cryptosystems in order to mitigate the problem of stolen biometrics [15].

2.2.2 Objectives of Biometric Template Protection

The biometric template protection requires the following main objectives to be satisfied by any template.

- *Non-invertibility / Irreversibility*: The transformed template should be non invertible means the given transformed template the intruder cannot recover the original biometric template from it. It should not be feasible to reconstruct the original biometric M from the transformed template M' .
- *Diversity / Unlinkability*: To avoid cross-matching of the stored template in different applications, the identical template should not be used. Given two templates, t_1 and t_2 which are generated from the same biometric but with different methods, it should not be possible to identify that both the templates belong to the same biometric trait.
- *Reusability / Revocability*: The transformation should derive a number of protected templates from the same biometric input. So when the template is compromised it should be possible to straight forward to revoke and reissue the new template.
- *Performance*: The transformation must apply in such a way that it should not deteriorate the recognition performance. In other words, guarantee the privacy preservation without degrading the accuracy of the biometric authentication system.

2.2.3 Methodology of Biometric Template Protection

The extensive use of biometric templates raises the question of the security of these applications. A system could be hacked by a fraudster or impersonator, who might also steal biometric information. A template is undoubtedly more difficult to read and misuse than conventional passwords and tokens because it is a series of zeros and ones in a mathematical file.

A biometric template is a digital representation of captured biometrics like fingerprints, irises, faces, etc. The biometric matcher doesn't make use of the original images. The similarity score, which is a vector representing the likelihood that two biometric templates

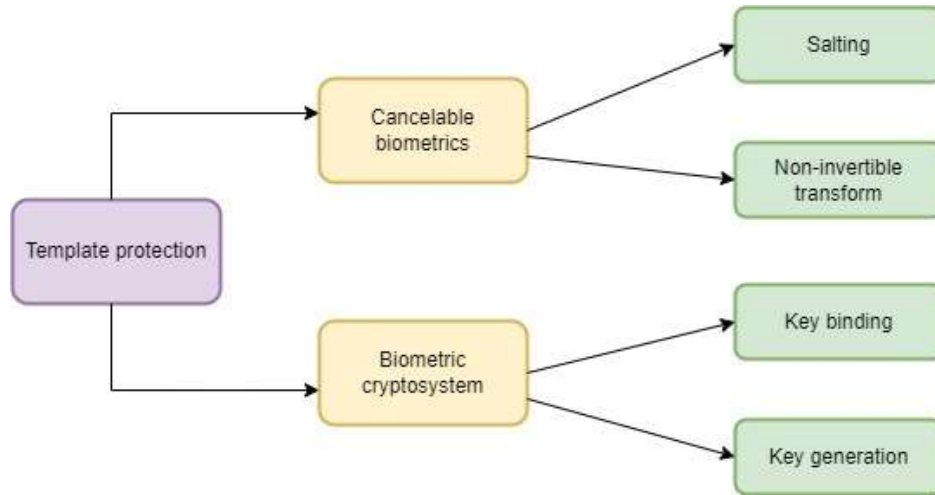


FIGURE 2.2 Biometric template protection schemes

match, is what the template matcher generates. With regard to templates, there are a few elements that could be compromised, like template databases, which are vulnerable to theft or hacking. Designing a biometric protection system is a significant challenge since it must be able to manage intrauser variations in the collected biometric identifiers [10]. The following four characteristics are appropriate for a strong biometric template protection system that can manage intrauser variability: diversity, revocability, security, and performance.

To protect biometric templates from attacks by enemies, many protective methods are used. The many types of biometric template protection techniques are depicted as shown in figure 2.2. The biometric cryptosystem approach [23] and cancelable biometrics approach [14] are the two primary categories into which biometric template protection methods fall. A transformation function is used in the cancelable biometrics approach to transform the acquired biometric template, and only the altered version is saved in the database. Typically, a randomly generated key or password is used to determine the transformation function's parameters. Helper data is saved in the biometric cryptosystem template protection scheme. In order to extract a cryptographic key from the query biometric template, helper information is needed. After that, indirect matching is carried out by confirming the accuracy of the produced cryptographic key.

Depending on how the transformation function is configured, the cancelable biometrics technique is further categorized into two types: salting and non-invertible transform. In the salting approach, if an intruder can gain access to the key and salting template, then he can easily retrieve the original biometrics from the transformation function. However, as the name implies, a non-invertible transformation cannot be reversed. Even if the key is known, it is

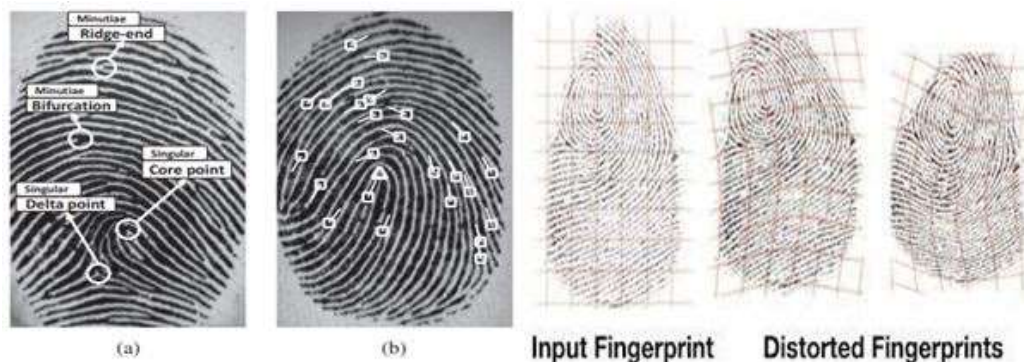


FIGURE 2.3 Fingerprint images (a) different fingerprint feature points (b) feature points and singular point (c) example of distorted fingerprints

very challenging to invert a changed template to the original template because it is a one-way function. By the method used to collect the auxiliary data, biometric cryptosystems are further divided into key binding and key generation. In a key-binding system, the biometric template is bonded to a key to extract the helper information. It is not easy to recover the key or the original biometric trait using the helper data. In a key generation biometric cryptosystem, helper data and query biometric features are combined to create the key. A hybrid template protection scheme employs one or more template protection strategies [15].

Figure 2.3 displays an illustration of a fingerprint biometric image with both singular and minutiae points highlighted on it. Ridge bifurcation and termination points are frequently used as minutiae points in fingerprint images [24]. A fingerprint's core point and delta point are also used as singular points; the area where the ridges are most curled is called the core point, and the delta point is the area where they form a delta shape.

2.2.3.1 Cancelable Biometrics

The authors present a novel method for creating secure and non-invertible cancelable fingerprint templates in [25]. The technique makes use of ridge feature transformation, which involves extracting and transforming the fingerprint's ridge orientation and frequency features using a collection of mathematical functions that are not reversible. This solves the crucial security problem of biometric irreversibility by guaranteeing that the original biometric data cannot be recovered from the modified template. The authors stress that their method provides non-invertibility, diversity, and strong revocability—three crucial characteristics for cancelable biometric systems. Tests conducted on common fingerprint databases demonstrate that the modified templates provide defense against a range of threats, including identity theft, cross-matching, and inversion, while maintaining the matching precision of the original

biometric system. In addition to supporting template re-issuance in the event of compromise, the suggested scheme is appropriate for safe biometric applications in practical settings.

The authors of the paper [10] suggest a way to create cancelable biometrics by protecting iris biometric templates through data hiding techniques. In order to securely store and transmit biometric templates while guaranteeing that the original biometric data is not directly exposed, the main concept is to embed the iris features into a cover image using reversible data hiding. This technique improves revocability and template security, which are essential components of workable biometric systems. In contrast to conventional, static biometric templates, the suggested scheme permits template revocation and reissue while maintaining recognition accuracy. The risk of template compromise can be mitigated by canceling the embedded templates and creating new ones using an alternative transformation. This approach is a feasible solution for secure iris recognition systems in privacy-sensitive applications, as demonstrated by the experimental results presented in the paper. It achieves a good trade-off between security, privacy, and authentication performance.

The problem of open-set face identification is addressed in [26], which was published in Pattern Recognition. In this method, the system must not only recognize known faces but also reject unknown faces that are not in the enrolled database. For large-scale face identification tasks, they suggest a novel Index-of-Max (IoM) Hashing technique that learns compact binary hash codes that maintain identity discrimination and enhance scalability. By concentrating on the index of the maximum response in a projected subspace, the IoM hashing technique converts facial features into secure and discriminative binary codes. This method ensures robustness against imposters while facilitating quick similarity searches and effective memory usage. The authors test their approach on benchmark face datasets and show that it outperforms open-set identification and conventional hashing techniques in terms of speed, accuracy, and unknown rejection. Significant improvements in face recognition security and performance are provided by the work, particularly for large-scale, practical deployment scenarios.

An inventive technique for creating cancelable fingerprint templates combining graph-based feature representation and Hamming embedding is presented in [5]. In order to capture the spatial distribution and relationships between features, the technique entails creating a graph from fingerprint minutiae. The graph is then converted into a fixed-length binary code, which acts as the safe, cancelable template, using a random projection-based Hamming embedding. The suggested method guarantees non-invertibility, which means that the stored template cannot be used to reconstruct the original biometric data. Additionally, it facilitates diversity and revocability by enabling the creation of multiple templates from a

Background and literature review

single fingerprint using various random seeds or keys. Using tests on common fingerprint databases, the authors verify the effectiveness and security of their methodology, showing that it provides robust defense against cross-matching and inversion attacks while retaining a high recognition accuracy. This work contributes a practical and theoretically sound solution for privacy-preserving biometric authentication.

In the paper [12], they suggest a way to create cancelable biometric templates using fingerprint data by applying non-invertible transforms to the original templates. The main idea is to change the fingerprint minutiae data with methods that are hard to reverse. This keeps the original biometric information safe. The authors present three specific transformation techniques: Cartesian, polar, and functional transformations. These methods change the spatial relationships of the minutiae points while keeping the important features needed for matching. In the Cartesian transformation, the fingerprint image is split into a grid. The positions of the minutiae are shuffled using a random rearrangement of the grid cells. This process ensures that the transformed data do not show the original structure. In the polar transformation, the minutiae are shown in polar coordinates related to a selected reference point. A non-reversible transformation is then applied to these coordinates, disrupting their geometric relationships. The functional transformation goes further by applying a mathematical function to the minutiae locations. This introduces a controlled distortion that is hard to reverse. Each transformation uses a user-specific key or transformation parameter. This allows for revocability by changing the key and diversity by using different keys for different applications. Each transformation can be revoked, meaning new versions can be made if a template is compromised. They are also diverse, allowing different applications to use different transformed templates for the same user. Experimental results show that transformed templates maintain high matching accuracy and provide strong resistance against inverse reconstruction and cross-matching attacks.

The authors present a secure method for protecting fingerprint templates using polar coordinate transformations [19]. They start by changing the raw fingerprint minutiae into a structured format. Next, they map these features from the Cartesian coordinate system to the polar domain, using a chosen reference point, usually the core or center of the fingerprint. This transformation creates a new representation of the fingerprint that is much harder to invert, keeping the original biometric data safe. After mapping to polar coordinates, they apply a quantization process, and then use a random projection with a user-specific key. This projection further obscures the transformed data, making it almost impossible to reconstruct the original minutiae or fingerprint image without the key. In addition to improving security, the authors highlight that their proposed method supports important

properties like revocability and diversity. Since the transformation and projection steps rely on a user-specific key, compromised templates can be easily reissued with a different key, ensuring template renewability. Additionally, using different keys across applications creates unique templates, which preserves unlinkability and stops cross-matching attacks. The experimental results in the paper show that the polar transformation method maintains high matching accuracy, similar to unprotected templates, while providing strong resistance to inversion attacks. The combination of polar coordinate transformation, quantization, and random projection offers a lightweight but strong solution for protecting biometric templates, making it suitable for real-world fingerprint authentication systems.

In the paper, the authors present a new method for creating cancelable biometric templates [27]. They use a technique called Index-of-Max (IoM) Hashing, which is a type of ranking-based Locality Sensitive Hashing (LSH). This method changes real-valued biometric feature vectors into discrete, non-invertible hash codes. These hash codes maintain similarity for matching but provide strong protection against inversion and linkage attacks. The IoM hashing works by projecting biometric feature vectors onto several random subspaces. In each subspace, it records the index of the maximum component. This index helps to create a compact hash code. Since only the ranking information (the position of the maximum value) is kept and not the actual feature values, the transformation is non-invertible by nature. The authors show that this IoM hashing framework meets important needs for cancelable biometrics: non-invertibility, revocability, and diversity. By using different random projection matrices, which serve as transformation keys, they can create multiple diverse templates from the same biometric data. This allows for template renewal and the generation of application-specific templates. The system achieves high matching performance under standard biometric evaluation protocols. It demonstrates robustness to changes within the same class while resisting attacks such as cross-matching and hill-climbing. Furthermore, the method is computationally efficient and works well in real-time because of its low complexity. Through thorough experiments on various biometric types, including fingerprint and face data, the authors confirm that IoM hashing offers a secure and precise framework for cancelable biometrics, balancing template protection with recognition accuracy.

The authors suggest a new alignment-free approach to protect fingerprint templates by using the k -nearest neighborhood structure (k -NNS) of minutiae points [17]. Unlike traditional methods that rely on aligning fingerprint images to a global reference, this technique emphasizes extracting local structural features from each minutia's k -nearest neighbors. These local structures capture the spatial relationships among minutiae in a way that remains unaffected by rotation and translation. This makes the method strong against

Background and literature review

fingerprint distortions and variations. Each local k-NNS is then encoded into a fixed-length representation, which serves as the foundation for a secure biometric template. The authors improve the security and non-invertibility of the template by applying a random projection to the k-NNS-based representation using a user-specific transformation key. This key controls the projection matrix, ensuring that the resulting templates are non-invertible, revocable, and diverse. Since the method does not depend on matching fingerprints to a global coordinate system, it is naturally alignment-free. This simplifies preprocessing and increases robustness against rotation, translation, and partial fingerprints. The use of random projection guarantees that even if a template is compromised, a new one can be created using a different key. Experimental results on standard fingerprint databases show that the method maintains high matching accuracy while significantly improving security and privacy. This makes it a promising solution for real-world biometric systems that need strong template protection without sacrificing recognition performance.

In the paper, the authors suggest a technique for creating cancelable and non-invertible biometric templates using Gaussian random projection [18]. The process starts with extracting fixed-length feature vectors from biometric data, such as fingerprints or iris scans. These vectors are then projected into a lower-dimensional space with a random Gaussian matrix. The projection matrix is created using a user-specific key, which makes the transformation unique and secure. The main idea is to keep the pairwise distances between data points the same. This helps maintain the ability to match while greatly reducing the chance of reconstructing the original biometric features from the transformed data. The projected feature vectors are then quantized and binarized. This process results in compact, non-invertible biometric templates that are highly secure and suitable for fast matching using Hamming distance. The non-invertibility arises from the nature of Gaussian random projections. Since the transformation matrix is random and the projection reduces dimensionality, it is mathematically impossible to reverse the transformation without the original matrix. The method also allows for revocability and diversity. If a template is compromised, a new one can be created by changing the random seed or projection matrix. Experimental evaluations show that the proposed method maintains high recognition accuracy while providing strong resistance to inversion attacks and cross-matching. This makes it an effective and practical solution for secure biometric authentication systems.

The authors introduce a new method for creating cancelable fingerprint templates using a partial Hadamard transform [28]. The main idea is to change fingerprint minutiae-based features into binary forms to improve storage efficiency and security while keeping matching accuracy. The method starts with extracting a fixed-length feature vector from the fingerprint

image and applying a Hadamard transform, a quick and orthogonal transformation. However, instead of using the entire Hadamard matrix, the authors only use a partial subset of its rows, which are randomly chosen based on a user-specific key. This partial projection reduces the data's dimensionality and adds randomness that ensures non-invertibility. The resulting real-valued vector is then turned into a binary template through quantization, creating a protected binary template. The proposed method ensures important features for cancelable biometrics: non-invertibility, revocability, and diversity. The partial Hadamard matrix is key-dependent and randomly generated; templates can be revoked and reissued by simply changing the key. This also allows for the creation of application-specific templates, which lowers the risk of cross-matching. The transformation process runs efficiently because the Hadamard transform is simple and works well for real-time biometric systems. Additionally, the binary output templates are compatible with fast and storage-efficient matching techniques like Hamming distance comparison. Experimental results on fingerprint datasets show that the method offers strong template security, high recognition performance, and resistance against inversion and linkage attacks. This makes it a practical choice for privacy-preserving biometric authentication systems.

In the paper "Cancelable Indexing Based on Low-Rank Approximation of Correlation-Invariant Random Filtering for Fast and Secure Biometric Identification" by T. Murakami et al. (2018), the authors present a new method for cancelable biometric indexing. This method improves both security and speed in large-scale biometric identification systems. The key to their approach is enhancing the well-known Correlation-Invariant Random Filtering (CIRF) scheme. This scheme allows biometric templates to be encrypted while still enabling matching in the encrypted domain. However, the traditional CIRF method requires a lot of computation. To solve this problem, the authors introduce a low-rank approximation technique. This technique significantly cuts down on the computation needed for CIRF without losing its security features. The low-rank structure helps project biometric data into a more compact form, which makes matching and indexing faster. The proposed system includes an indexing mechanism. In this mechanism, biometric templates are assigned to groups or clusters based on their low-rank features. This cancelable indexing structure allows for the revocation or reissuance of templates if they are compromised, while keeping them non-invertible and diverse. The random filtering process uses a user-specific key. This ensures that even if two users have similar biometric traits, their templates remain unlinkable across applications. Experimental evaluations on face and palmprint datasets show that the method achieves fast identification with high accuracy, even in large-scale settings. It also maintains strong resistance to inversion and correlation attacks. Overall, the approach strikes

Background and literature review

a practical balance between security, revocability, and speed. This makes it suitable for use in secure and scalable biometric identification systems.

In the paper, the authors present a new method for creating cancelable fingerprint templates using Minimum Spanning Trees [29]. They start by extracting minutiae points from the fingerprint and treating these points as nodes in a graph. They weigh the edges between nodes based on the Euclidean distances between the minutiae. Next, they construct the MST from this graph. It represents the essential structure of the fingerprint in a compact and connected way. This MST forms the basis for a topologically consistent but non-invertible representation of the fingerprint. It captures the key discriminatory features while hiding the raw minutiae data. To ensure cancelability and diversity, the authors introduce transformation techniques on the MST structure using user-specific keys. These transformations include random reordering, weight perturbation, and tree pruning or regeneration techniques. They change the structure in a non-reversible but consistent way, allowing for secure matching. The transformed MST-based templates are strong against rotation, translation, and partial prints because of their relational encoding. Additionally, since the transformations depend on the keys, compromised templates can be revoked and regenerated. This supports both revocability and unlinkability. Experimental evaluations show that the proposed method achieves high recognition performance and offers strong resistance against inversion and linkage attacks. This provides a viable and secure way to protect fingerprint templates in biometric systems.

An advanced cancelable biometric indexing scheme is proposed in the paper [30] to address issues with quick and secure identification systems, particularly for large biometric databases. Their strategy is based on Correlation-Invariant Random Filtering (CIRF), a template protection technique that uses random filtering in conjunction with the 2D number theoretic transform (NTT) to alter biometric images. Because it guarantees that altered biometric templates don't divulge details about the original feature, CIRF is renowned for its perfect secrecy. The high computational complexity of the matching phase, namely the 2D inverse NTT, makes standard biometric indexing techniques incompatible due to possible information leakage and makes traditional CIRF unfeasible for large-scale identification tasks. The authors present a novel cancelable indexing technique to address these issues, which maintains CIRF's security features while facilitating effective large-scale identification. Their solution includes a minimum spanning tree representation of low-rank matrices in the Fourier domain and employs a low-rank approximation of biometric images to speed up computation. By ensuring that the modified index does not reveal any information about the original biometric feature, this novel indexing technique successfully achieves perfect secrecy.

The suggested method dramatically lowers one-to-many matching time while preserving robust security and privacy guarantees for the templates and their corresponding indexes, according to extensive tests conducted on a finger-vein database that contains six finger images per subject from 505 individuals.

The technique presented by [31] focuses on creating cancelable fingerprint templates using bit-strings that are extracted from the fine details found in fingerprint photos. This method overcomes a significant obstacle in template generation by not requiring fingerprint pre-alignment, in contrast to many other biometric protection schemes. The main idea is to map minutiae points to a predefined three-dimensional array composed of tiny cells. If a cell contains minutiae, it is set to 1; if not, it is set to 0. Regardless of the fingerprint's initial orientation or position, a reference minutia is chosen, and subsequent minutiae are translated and rotated according to this reference, standardising their placement. A 1D bit-string is created by sequentially converting the resultant binary values. The order of the bit-string is permuted based on the type of reference minutia and a user-specific PIN to guarantee the cancelability and security of templates. This enables template regeneration or revocation as needed. By simply altering the reference details, new cancelable templates can be made, giving the scheme great flexibility and protection against template compromise. In comparison to earlier approaches, extensive tests on the FVC2004 database show improved recognition and revocability performance, successfully protecting user privacy while retaining system accuracy. For contemporary biometric applications, this approach works well because it strikes a balance between security, adaptability, and matching performance.

Based on the idea of Minimum Distance Graphs (MDG), [32] approach presents a reliable, alignment-free fingerprint hashing algorithm. This method uses orientation field analysis to identify the core point of a fingerprint and the crossing number technique to extract minutiae points. The MDG efficiently captures the distinct geometric arrangement of features in an invariant manner by taking into account vectors that represent the minimum distances from the fingerprint's core to each minutiae point. Because this representation does not require global pre-alignment, it is naturally resistant to rotations and translations. The system creates a hash value from each fingerprint's MDG structure in order to accomplish accurate and efficient matching. By comparing the minimum distance vectors of the query and template images, correspondence is established during identification. By calculating the number of similar vector pairs—which corresponds directly to the fingerprint's similarity score—the algorithm finds matches. Tests on common fingerprint databases show that this method provides dependable security and usefulness for biometric indexing systems by achieving

Background and literature review

robustness to common distortions and strong discrimination, as well as resilience to errors caused by spurious or missing minutiae.

The technique presented by [33] successfully tackles the registration problem in fingerprint template protection by introducing a novel framework to create cancelable fingerprint templates using pair-polar coordinates. Their scheme leverages the intrinsic relative relationships among minutiae, or specific points of interest in a fingerprint, in a structure that is intrinsically invariant to both rotation and translation, in contrast to traditional methods that mainly rely on precise alignment or detection of global features (such as singular points). The method ensures that even minor adjustments or shifts in fingerprint capture do not negatively impact the transformation or the authentication process, and it does away with the need for registration by mapping the minutiae into a pair-polar coordinate system. The original minutiae information from the stored templates cannot be recovered computationally because a many-to-one mapping is used to make the transformed templates non-invertible. To further obfuscate the spatial distribution of minutiae, a random translation parameter is added, strengthening the transformed template's defence against inversion attacks. The new scheme satisfies the basic requirements for biometric template protection, including non-invertibility, diversity, revocability, and strong security against correlation and inversion attacks, according to experimental results obtained on public fingerprint datasets like FVC2002DB1, FVC2002DB2, and FVC2002DB3. When compared to the original, unaltered templates, the results also showed only a slight decline in matching performance (as indicated by an equal error rate), underscoring the applicability of the suggested approach for actual biometric systems. The technique offers significant improvements for template security and privacy protection in large-scale biometric deployments by producing templates without requiring registration and guaranteeing non-linkability between various transformed versions.

2.2.3.2 Biometric Cryptosystem

The authors of the paper [34] present a novel biometric cryptosystem that uses fingerprint minutiae-based features to focus on key binding. The main concept is to safely bind fingerprint information to a cryptographic key, preventing the key from being retrieved until the right biometric input is provided. This solves the main privacy and security issues in biometric authentication systems by protecting the key and the biometric data at the same time. To manage intra-user variations in biometric inputs while maintaining the security of the original fingerprint template and cryptographic key, the suggested scheme makes use of a randomized look-up table and error correction codes (ECC). Strong non-invertibility, revocability, and defense against template inversion and cross-matching attacks are all accom-

plished by the technique. Experiments on benchmark fingerprint databases demonstrate that the system offers robustness and high verification accuracy without jeopardizing user privacy. In order to enable secure identity management, this work represents a major advancement in the integration of biometrics with cryptographic systems.

Rather than relying on conventional yes/no biometric matching, [35] present the idea of biometric encryption as a method for safely binding or creating cryptographic keys from biometric data. Their framework involves processing a biometric sample, like an iris or fingerprint scan, so that a secret key can be generated directly from the biometric template (called "key-generation") or linked to it (called "key-binding") without disclosing the original biometric data. The writers stress a number of fundamental design concepts, such as discrimination (to avoid false matches), security (to safeguard the key and stored data), privacy (to guarantee that the biometric cannot be recreated), and distortion tolerance (to manage inherent biometric variability). They go over methods that make secure key recovery easier, like fuzzy extractors, helper data schemes, and error-correcting codes. By doing this, biometric encryption transforms biometric systems from straightforward pattern-matching techniques into cryptographic frameworks in which a cryptographic key is generated for additional secure operations—like digital signatures or data encryption—when the proper biometric input is received. By enabling revocability (the ability to issue new keys in the event that they are compromised), unlinkability (the use of different keys for different applications), and privacy by design (the protection of raw biometric data), the method improves security and privacy. The authors summarise the latest findings in biometric cryptosystems research, emphasising the advantages and disadvantages of combining biometrics and cryptography. They point out that although tying biometrics to cryptographic keys can greatly increase system security, doing so also places limitations on biometric stability and input variability tolerance. They also note that leakage from helper data is still a possible vulnerability and that biometric entropy frequently restricts the possible key lengths. Thus, it is still difficult to strike a balance between biometric accuracy and key strength. The authors emphasise the necessity of careful system design to ensure robustness, revocability, and privacy protection, warning that many current biometric systems fall short of strict cryptographic standards in practice.

[36] present a novel cryptographic construct, A Fuzzy Commitment Scheme, which combines the ideas of conventional commitment schemes and error-correcting codes. The fuzzy commitment scheme is particularly well-suited for biometric and other noisy data sources because it is made to enable a commitment to be confirmed using an input that is roughly—rather than precisely—identical to the original. During the commitment phase,

Background and literature review

a random codeword c from an error-correcting code is selected, and an offset $\delta = x - c$ is computed based on the original biometric or noisy input x . The commitment is represented as the pair $(\delta, h(c))$, where $h(\cdot)$ is a cryptographic hash function. In the decommitment phase, a new input x' is accepted if $x' - \delta$ can be decoded to c and the hash $h(c)$ matches. Secure, noise-tolerant cryptographic commitments for biometric and related applications are made possible by this mechanism, which guarantees that the scheme can withstand inherent fluctuations in input data while preserving the standard security features of concealment and binding. Instead of concentrating on empirical performance metrics, the analysis mainly examines the fuzzy commitment scheme's theoretical underpinnings and security guarantees. They show that even if the verifying input differs slightly from the original, the scheme still achieves both concealment and binding properties under the right assumptions, namely the use of a secure one-way hash function and a well-chosen error-correcting code. Their findings demonstrate how well the fuzzy commitment model adapts traditional cryptographic commitments to account for input data uncertainty. The authors also go over the trade-offs and practical issues that come with implementation, such as how to balance security strength (which is impacted by code size and entropy) and noise tolerance (which is controlled by the code's decoding radius). They come to the conclusion that the fuzzy commitment scheme provides a strong theoretical basis for safe and privacy-preserving biometric authentication systems, despite admitting that choosing appropriate error-correcting codes for actual biometric variability can be difficult.

[23] presents a novel biometric cryptosystem that secures fingerprint templates by utilising the minutiae phase spectrum. In order to capture the spatial configuration of these points through their phase information, the technique entails extracting minute points from fingerprint images and converting them into a phase spectrum domain representation. By using the binarized phase spectrum (BiPS) method, common fingerprint variations like translations and rotations are given resilience. The system addresses the issues caused by noisy or distorted fingerprint inputs and provides improved security by combining biometric data protection with error tolerance when integrated within a fuzzy commitment framework. The effectiveness of the suggested cryptosystem is confirmed by experimental results, which show that it is more resilient and accurate at recognising objects than traditional minutiae-based techniques. Experiments on various fingerprint datasets demonstrate that the method can sustain high verification performance in spite of common fingerprint distortions. The system is positioned as a workable and dependable solution for secure fingerprint authentication in real-world biometric applications due to its strong template security and low false acceptance rates.

2.3 State of the Art: Biometric Template Security

A novel cryptographic framework called the "Fuzzy Vault Scheme," is intended to safely bind a secret to an unordered set while accepting input data errors [37]. The secret is encoded as a polynomial and then "locked" by linking it to a real set of points from biometric or other noisy data, along with a large number of random chaff points to mask the real data. An entity must provide a data set that sufficiently overlaps with the original in order to open the vault and retrieve the secret. The shortcomings of earlier cryptographic systems are addressed by this error-tolerant, order-invariant design, which permits secure authentication even when biometric inputs are noisy and vary in order. Through thorough theoretical analysis, the authors support the fuzzy vault's security and usefulness, showing that it is resilient to attackers and that its security depends on the computational difficulty of polynomial reconstruction problems. Its efficacy in addressing biometric variability, including noise, translation, and rotation, while preserving security assurances is demonstrated by empirical evaluations. By creating a strong mechanism for safe biometric key binding, the fuzzy vault scheme makes a substantial advancement for applications that need dependable cryptographic protection even in the face of imperfect input data.

[38] suggests a sophisticated method for fingerprint template security that improves the traditional fuzzy vault scheme by incorporating minutiae descriptors. These descriptors enhance the biometric representation by capturing the complex local ridge patterns surrounding each minutia, including orientation and frequency information. The technique greatly improves the vault's security by enclosing these intricate features in a fuzzy commitment framework, which makes it far more impervious to inversion or reconstruction attacks that could jeopardise conventional minutiae-only systems. Experiments show that adding minutiae descriptors strengthens security and increases the accuracy of the system's recognition. The method successfully lowers false acceptance rates while remaining resilient to biometric variations that are frequently seen in practical situations. Its practicality and effectiveness as a safe solution for fingerprint template protection in biometric authentication systems are demonstrated by this balance between improved security and trustworthy biometric verification.

2.3 State of the Art: Biometric Template Security

S. Wang et al. [28] had proposed a partial Hadamard transform approach to the design of cancelable fingerprint templates which contain binary biometric representations. In this system, an efficient partial Hadamard transform based non-invertible transformation method

Background and literature review

has been proposed to securely protect binary biometric representation in the design of cancelable biometrics.

The Hadamard transform is symmetric, orthogonal and non sinusoidal function (i.e. $H_n^{-1} = H_n^T = H_n$). It transforms from spatial domain to frequency domain. The H_n , unitary matrices consist of +1, -1 and the recursive transformations are computed using addition and multiplication only, with no multiplication being involved. The Hadamard matrix H_n is of dimension $2^n \times 2^n$. Where $*$ is the Kronecker product of two matrices. $H_n = H_1 * H_{n-1}$. For 2D image, The Hadamard transform Y of vector X is, $Y = H_n X H_n^T$.

A binary biometric representation in the data domain can be represented by a binary valued vector

$$t_d = [d(0), d(1), \dots, d(m-1)]^T, \text{ where } d(i) \in 0, 1 \quad (2.1)$$

The entries of the binary vector t_d are either 0 or 1. First DFT has been applied to the sparsely distributed binary biometric representations which make the resultant templates more complex because it renders a dense data representation in the transformed domain. The DFT operation can be performed using the powerful FFT algorithm on t_d to get t_D .

$$t_D = F t_d \quad (2.2)$$

where, $t_D = [D(0), D(1), \dots, D(m-1)]^T$.

After DFT, non-invertible partial Hadamard transform has been applied on t_D which makes complex resultant templates t_H from which the original vectors cannot be recovered. The length of the vector t_D is N and Suppose a random row vector of length r is denoted by $K = [k_1, k_2, \dots, k_r]$ where $r < N$ with $N = 2^n$. All entries of K are strictly positive integers with $K_i \neq K_j$. This random vector K has been used to construct the sub-matrix of H_n , denoted by H'_n , such that the i^{th} row of the H'_n is the k_i^{th} row of the H_n . For $i \in [1, \dots, r]$ and the size of H'_n is $r \times N$.

$$t_H = H'_n t_D \quad (2.3)$$

M. V. Prasad et al. [29] had proposed the method which generates the cancelable templates without requiring the pre-alignment of the fingerprint based on fingerprint minutiae representation. First, generate a minimum spanning tree for the fingerprint minutiae in a three-dimensional feature space which connects all the minutiae points then the two-dimensional feature space is generated based on the chain code representation from the generated MST. A bit string is then generated by mapping the chain code into the 2D array. Minutiae consists of (x, y, θ) , where (x, y) represents the minutiae coordinates and θ denotes the orientation of

2.3 State of the Art: Biometric Template Security

the minutiae. The set of minutiae is denoted by M .

$$M = \{M_i(x_i, y_i, \theta_i)\}_{i=1}^m \quad (2.4)$$

where m is the number of minutiae, (x_i, y_i) is the coordinates and θ_i is the orientation of the i^{th} minutiae. From this minutiae points a spanning tree which is a connected acyclic subgraph of the connected graph. MST of the $G = (V, E)$, such that the total weight or the total length of the edges is minimum. Considering the minutiae set M as vertices V . The prim's algorithm has been explored by finding $(m - 1)$ edges from the $m \in e_{ij}$ edges that form the MST, g' with a minimum total weight $m(m - 1)/2$.

$$g' = \{e_{i_r, j_r} : i_r < j_r; r = 1, 2, \dots, m - 1; i_r, j_r = 1, 2, \dots, m\} \quad (2.5)$$

Now the chain code CC is constructed from the generated MST by pairing up the length L of the edge e_{ij} and the orientation of the starting vertex of the edge θ . After selecting the initial vertex the tree is traversed by breadth-first search and produces the sequence of edges e_i where $i=1, 2, \dots, m-1$. For each edge e_i with two measurements, the weight of the edge (L_i) and the orientation (θ_i) of the minutiae v_i . Hence the chain of code C_i is the sequence of $(L_1, \theta_1)(L_2, \theta_2) \dots (L_{m-1}, \theta_{m-1})$.

$$C_i = (L_i, \theta_i); i = 1, 2, \dots, m - 1 \quad (2.6)$$

After chain code is generated then it has been mapped to the 2D array consisting of the small cells. After pairing the length and orientation of minutiae of MST, it can be determined which cell in the 2D array includes minutiae. A 1D bit string $\{h_k\}$ of length $d = M \times N$ is generated by sequentially visiting the cells by a raster scan of the above 2D array in which at most or less than $(m - 1)$ 1's and all others are 0's. If a cell in the 2D array has one or more than one minutiae then the cell is set to 1 otherwise they are set to 0. The complex-valued vector H is formed from the $\{h_k\}$ in the frequency domain by taking the discrete fourier transform(DFT). To add more security this complex valued vector H is multiplied by a random matrix key A in order to get the cancelable template $T = AH$.

B. Choudhury et al. [39] had proposed a novel method of non-invertible transformation function using the concepts of steganography which generates cancelable biometrics template. The combined approach of discrete cosine transformation (DCT) and Huffman coding had been used to get the non-invertible transformation in steganography. The steganography is the covered communication which hides the secret image through an unsuspecting cover image.

Background and literature review

In secret communication, the secret image is hidden by embedding in the least significant bits (LSB_s) of each pixel in the cover image.

The discrete cosine transformation (DCT) converts an image from the spatial domain to the frequency domain by subdividing the image into the 8×8 blocks and in each block, 64 DCT coefficients are generated. The Huffman encoded bit stream of the secret image is embedded in the (LSB_s) of the DCT coefficients of the cover image. The transformed template is generated after performing the inverse discrete cosine transformation (IDCT).

Z. Jin et al. [27] had proposed ranking based locality sensitive hashing for cancelable biometrics which uses index-of-max hashing. First LSH had been used to maximize the probability of a collision for similar biometric features. The locality sensitive hashing function $h : M \rightarrow S$ is an effective way of reducing dimensionality of the data by hashing the input items $M = (m, d)$ with a threshold $R > 0$, so that the similar items map to the same buckets $s \in S$ with the high probability of the collision. LSH is a probability distribution on a family H of hash functions h such that $P_{h \in H}[h(X) = h(Y)]$. The objects p and q can collide with probability at least $P1$, if $d(p, q) \leq R$, then $h(p) = h(q)$.

Index of max(IoM) hashing transforms the fixed length real-valued biometric feature vector into discrete index max ranked hashed code. It provides strong concealment to the biometric information such that it can not be inverted. The two variations of the IoM hashing had been proposed, namely Gaussian Random Projection based and Uniformly Random Permutation based hashing schemes.

The WTA hashing is a non-linear transformation that performs H random permutations on the input biometric vector with dimension d , $x \in R^d$. Then select the first k items of the permuted x and choose the largest element within the k items and also record the corresponding index values in bits. The previous steps are repeated m times, yielding in a hash code of length m .

The main thing about the uniformly random permutation(URP) based IoM hashing is the uniform random permutation that is inherited from the winner-takes-all(WTA) hashing and further strengthened by the Hadamard product operation. Suppose the biometric feature vector $x \in R^d$ and m independent hash functions $\{h_i(x) \in [1, k] | i = 1, \dots, m\}$ where each hash function consists of a p -order Hadamard product.

The overall URP based IoM hashing can be summarized as the following steps: For each hash function $h(x)$, permute the enrolled/query feature vector x randomly for m times. Generate a p -order Hadamard product vector by performing the element-wise multiplication on the p permuted vectors. For each $\bar{x}$, select the first k elements where $1 < k < d$. Find the

maximum entry value within window size k and record its index $t \in [1, k]$ as the URP based hashed code.

The two fingerprint vectors with high similarity give a high probability of collision in the rank domain when IoM hashing is used with ranking based LSH. On the opposite, the vectors far apart from each other result in a lower probability of hash collision. For example two hash codes, enrolled $t_{URP}^e = \{t_i^e | i = 1, \dots, m\}$ and query $t_{URP}^q = \{t_j^q | j = 1, \dots, m\}$ and $S(t_{URP}^e, t_{URP}^q)$ represents the probability of collision of the hashed codes i.e. $P[t_i^e = t_j^q] = S(t_{URP}^e, t_{URP}^q)$ for $i=1, \dots, m$. The high probability of collision implies high similarity of t_{URP}^e , t_{URP}^q and vice-versa.

2.3.1 Security Analysis of Biometric Template Transformation

The security of the generated template is depending on the information that has been used at the time of transformation. The security of template transformation is guaranteed by the following factors: Non-invertibility, Diversity, and Revocability.

Suppose biometric feature A is represented as an image which is a two-dimensional array with width (w) and height (h) pixels and the value of each pixel is an integer, i.e., $A \in Z^{wh}$. Let $a[x, y]$ represent the value of the pixel coordinates (x, y) , where $0 \leq x \leq w - 1$ and $0 \leq y \leq h - 1$. [20] To generate the cancelable biometric template $T \in T'$ from the biometric feature $A \in \beta$ using the random filter $K \in K'$, we can use the transformation function F as follows.

$$F : \beta \times K' \rightarrow T' \quad (A, K) \mapsto T = \mathfrak{Z}(A) \circ K \quad (2.7)$$

where $\beta, T \subseteq Z_p^{wh}$ and $K' = (Z_p^*)^{wh}$ (i.e. $Z_p^* = Z_p - \{0\}$)

Non-invertibility: The non-invertibility refers to the fact that it should be computationally infeasible to recover the original biometric data from the generated cancelable biometric template. Suppose secure cancelable biometric template T generated from the biometric feature set A . Using non-invertibility, it should be computationally hard to recover the original biometric features A from the generated secure cancelable biometric template T' . That means the process should be irreversible which gives guarantees that generated cancelable biometric template is secured without any loophole in the system [6].

Diversity: The cancelable template $T = F(A, K)$ is generated from the biometric feature $A \in \beta$ with transformation function F with the random filter $K \in K'$. Suppose the situation where two cancelable templates $T^1 = F(A, K1)$ and $T^2 = F(A, K2)$ generated from the same biometric feature a , can be enrolled in the two different databases. To prevent cross matching

Background and literature review

across the different databases, it is required that two cancelable biometric templates T^1 and T^2 do not have any correlation. Below theorem can prove the same.

According to the cryptosystem has perfect secrecy if any ciphertext $c \in C$ does not reveal any information about the plaintext $p \in P$. i.e. $Pr(p | c) = Pr(p)$ for any $p \in P$ and $c \in C$. Similarly it is proved that cancelable transformed template $T \in T'$ does not reveal any information about the biometric feature $A \in \beta$. i.e. $Pr(A | T) = Pr(A)$ for any $A \in \beta$ and $T \in T'$. (i.e. If $P(A | B) = P(A)$, then events A and B are said to be "independent": in such a case, knowledge about either event does not give information on the other).

Let us check the following decomposition

$$Pr(T^i) = \sum_{A \in \beta^*} Pr(T^i | A) Pr(A) \quad (i=1,2),$$

$$Pr(T^1, T^2) = \sum_{A \in \beta^*} Pr(T^1, T^2 | A) Pr(A) \quad (2.8)$$

Since for a fixed $A \in \beta^*$, there is one to one mapping from K^i to T^i . (i.e. $T^i = F(A, K^i)$)
 $Pr(T^i | A) = Pr(K^i | A)$

$$Pr(T^1, T^2 | A) = Pr(K^1, K^2 | A) \quad (2.9)$$

However, the occurrence of K^1, K^2 is independent of each other and of A, thereby
 $Pr(K^i | A) = Pr(K^i) = 1/|K'|$

$$Pr(K^1, K^2 | A) = Pr(K^1) Pr(K^2) = 1/|K'|^2 \quad (2.10)$$

Where $|K'|$ is the cardinality of K' . From Eqs.(2)-(4), we have

$$Pr(T^i) = \sum_{A \in \beta^*} Pr(1/|K'|) Pr(A)$$

$$Pr(T^i) = 1/|K'| \quad (2.11)$$

and

$$Pr(T^1, T^2) = \sum_{A \in \beta^*} Pr(1/|K'|^2) Pr(A)$$

$$Pr(T^1, T^2) = 1/|K'|^2 \quad (2.12)$$

From Eqs.(5) and (6),

$$Pr(T^1|T^2) = Pr(T^1, T^2)/Pr(T^2) = (1/|K'|^2)/1/|K'|$$

$$Pr(T^1|T^2) = Pr(1/|K'|) = Pr(T^1) \quad (2.13)$$

Revocability: Consider the cancelable biometric template is $T = F(A, K)$. Suppose the cancelable template T (or K) is compromised then we can revoke the new cancelable biometric template T' from the same biometric feature A as follows.

The user randomly choose the new random filter K' from K and calculate the differential filter,

$$\Delta K = K' \circ K^{-1} \quad (2.14)$$

and sent ΔK to the server. The server calculates the new cancelable template as follows,

$$T' = T \circ \Delta K = (\mathfrak{F}(A) \circ K) \circ (K' \circ K^{-1}) \quad T' = (\mathfrak{F}(A) \circ K')$$

$$T' = F(A, K') \quad (2.15)$$

Note that the ΔK does not reveal any information about the K , hence has no effect on security.

2.4 Summary

Cancelable biometrics is a field devoted to strengthening privacy and security by enabling biometric templates to be transformed or "canceled" upon enrollment so that they cannot be misused if compromised. A survey of cancelable biometrics finds that the investigation of techniques such as feature transformation, biometric encryption, and protection of the biometric template is quite wide. Among the key approaches taken to generating cancelable biometric templates are using cryptographic techniques, applying random transformations to biometric data, and using feature extraction methods that allow the biometric data to be changed while preserving its usability for authentication. The challenges are addressed—namely, guaranteeing cancelability without compromising the accuracy and usability of biometric systems and the risk of an attacker reverse engineering the transformation. Other works focus on hybrid methods combining different biometric modalities (e.g., fingerprint, face, iris) for enhanced cancelability, whereas others study specific attack vectors and countermeasures. Overall, the literature underlines the trade-offs between privacy protection and the performance of the systems, with a growing interest in practical implementations of cancelable biometrics in real-world applications.

CHAPTER - 3

Cancelable biometrics based fingerprint template protection using discrete cosine transform and index of max hashing

3.1 Introduction

In classical authentication systems, either users need to remember a password (knowledge based identification system) or have to carry ID proof (token-based identification system). Over the last decades, biometric authentication systems have emerged as an alternative to classical authentication systems where your body is your password (e.g. fingerprint, face or voice). The prime advantage of biometric traits is that it can never be lost or forgotten. On the other hand, if any of the biometric traits get compromised then the user will not be able to change it like a password. In the real world, while biometric authentication is becoming gradually more popular, the privacy and security risks related to their usage are raising several concerns.

The prime threat associated with biometric authentication is identity theft. Any attack that recovers the biometric template may have a serious impact since users can not change their biometric traits. Hence biometric templates must be protected in order to thwart any leakage as the biometric traits are extremely susceptible to change. In privacy preserving biometric authentication systems, the biometric data is stored in a secure form which transforms data in distorted version and it also matches the trait in the transformed domain at the time of recognition.[1]

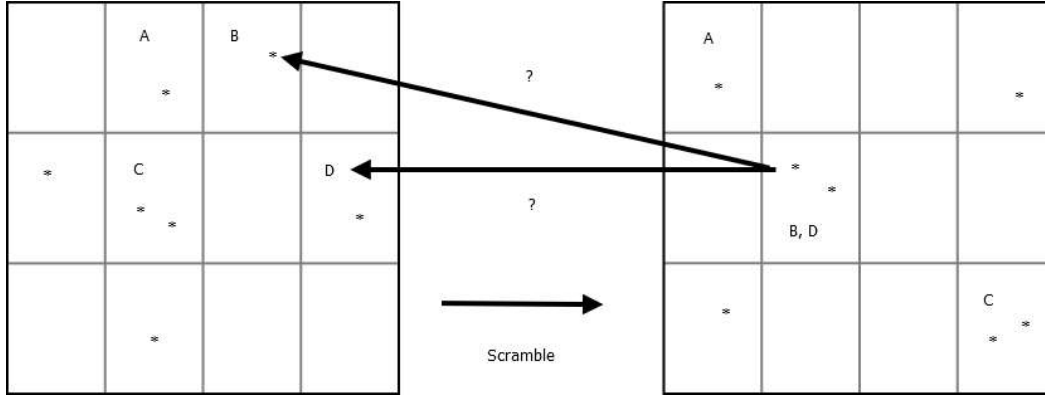


FIGURE 3.1 Distortion transform based on feature perturbation

3.2 Cancelable biometric template protection

Cancelable biometric is a template protection scheme in which the original biometric template is distorted repeatedly. The main advantage is that it can be canceled and revoked like a password once stolen, as well as being unique to every application. Even if the biometric template has been compromised, it is challenging for the intruders to reconstruct the original trait from the transformed one [40].

In the cancelable non-invertible transformation approach, the biometric template is secured by applying a one-way non-invertible transformation function that is easy to compute but hard to invert. Figure 3.1 shows a many-to-one function which is designed in such a way that will transform the raw biometric features into the transformed template which makes it computationally hard for the intruder to recover the original biometric template [jtepjoshi2018security].

3.2.1 Methods for Generating Cancelable Templates

- **Non-invertible Transformations:** Biohashing, random projections, permutation, and masking the original template with non-invertible functions are examples of irreversible mathematical changes that are applied to biometric feature sets. Because the change cannot be reversed, the original biometric cannot be readily recovered, enhancing revocability and privacy. With a focus on BioHashing, [41] talks about cancelable biometrics. According to the article, BioHash is a method that combines user-specific random integers with biometric data to produce modifiable and revocable biometric templates.

Cancelable biometrics based fingerprint template protection using discrete cosine transform and index of max hashing

- **Biometric Salting:** A random string or "salt" is combined with biometric traits prior to the creation of a template. Because of this, templates can be canceled and reprinted by simply changing the salt, ensuring that the same biometric data consistently creates unique templates. Token-based or password-based transformations, which generate salts using user input, are among the techniques. [42] presents a method for protecting biometric templates that uses a personal identification number to generate cancelable biometric templates. The technique creates a modified biometric template that can be revoked and altered by simply changing the PIN by combining biometric features with a user-selected PIN, ensuring security and privacy.
- **Feature Transformation with Key/Token:** Using a user-specific key or token, feature transformation techniques alter biometric features (e.g., by shifting, rotating, or mapping feature vectors). In the event that the key is compromised, template regeneration is possible because templates are hard to reverse-engineer without the key.
- **Biohashing:** Uses a mathematical hash function to combine biometric data with a random binary vector or user token. This procedure creates a distinct template that is very resistant to attacks that target the underlying biometric representation and can be revoked and changed. [43] recommends BioHashing, a state-of-the-art two-factor authentication method. This method combines user-specific fingerprint data with a tokenized pseudo-random integer using iterated inner products generated from wavelet and Fourier-Mellin transforms.
- **Block Permutation and Shuffling:** Separates the biometric feature set into blocks, which are then permuted or shuffled using a user-specific pattern or key. The final template is unique and can be made again by changing the permutation pattern.
- **Hybrid and Multi-biometric Techniques:** Certain methods use fused templates from various modalities (e.g., integrating iris and face patterns) or combine numerous methodologies, producing templates that can be revoked by altering transformation parameters or one or more modalities.

3.2.2 Preliminaries

For fingerprint identification systems, accurately detecting discriminative features like bifurcations and ridge endings—collectively referred to as minutiae—is essential. However, raw fingerprint images from optical or capacitive sensors often contain noise, uneven lighting,

3.2 Cancelable biometric template protection

ridge discontinuities, and background abnormalities. These degradations greatly reduce matching algorithms' dependability [44]. An effective pre-processing pipeline is essential to enhance ridge-valley structures and prepare the image for stable minutiae extraction. The following sections provide a research-focused explanation of each pre-processing step and the minutiae extraction technique. Fingerprint pre-processing, which ensures that the ridge-valley structure is accurately established before feature extraction, is an essential step in biometric recognition systems. Using contrast normalization, segmentation, orientation estimation, Gabor augmentation, binarization, and thinning, the image is transformed into a high-quality skeleton suitable for minutiae identification [45].

By modifying the fingerprint image to a predetermined mean and variance, normalization standardizes the intensity distribution. This process improves homogeneity throughout ridge and valley areas and lessens variances in illumination. This stage guarantees consistent performance of following filtering processes. The foreground and background are divided via segmentation. Incorporating background regions during enhancement or minutiae extraction frequently creates spurious features because they lack meaningful ridge patterns [46]. Block-wise variance thresholding, which divides the image into fixed-size blocks and assesses each block's variance, is a popular method. Compared to backdrop areas, ridge regions show noticeably greater variance. To conserve high-variance blocks and suppress the others, a binary mask is created. The mask can be improved with morphological operations. Ridge-valley contrast enhancement (e.g., Gabor filters, histogram equalization) is used in enhancement to highlight the ridge structure prior to transformation [47, 48].

3.2.2.1 Discrete cosine transform

By converting the fingerprint image from the spatial to the frequency domain and breaking it down into frequency components, the Discrete Cosine Transform (DCT) makes it possible to extract features that capture the texture and unique ridge patterns of fingerprints. Energy compaction, pixel data decorrelation, and effective representation of both local and global fingerprint features are the main benefits [49]. When fingerprints are subjected to DCT, statistical measures like standard deviations from grouped DCT coefficients are computed and used as reliable feature vectors for tasks involving matching and recognition. DCT-based features have been successfully combined with machine learning classifiers to improve performance, and they are useful for fingerprint identification with high accuracy and computational efficiency [50].

The pre-processed fingerprint image is divided into 8x8 blocks using DCT. To obtain the DCT coefficient matrix for every block, apply the 2D DCT to each block. Choose a

Cancelable biometrics based fingerprint template protection using discrete cosine transform and index of max hashing

subset of each block's DCT coefficients, usually the low-to-mid frequencies, as they are less susceptible to noise and contain the majority of the ridge structure. Using the chosen coefficients, one or more statistical features are calculated for every block. Create a fixed-length feature vector for the complete fingerprint image by concatenating these per-block feature values [51]. Frequently, the feature vector that is produced from all of the blocks has a set length. Indexing and matching are made easier by transform-domain features, which produce fixed-length vectors as opposed to minutiae sets, which vary in number per fingerprint.

3.2.2.2 Locality sensitive hashing

One effective method for locating approximate nearest neighbours in high-dimensional datasets is Locality Sensitive Hashing (LSH). LSH deliberately increases the likelihood that similar data points will hash to the same bucket, in contrast to conventional hashing techniques that seek to minimise collisions. This allows for the rapid identification of potential neighbours without the need for thorough comparisons. This method makes use of a family of hash functions that have the crucial characteristic of having a high likelihood of colliding in the same bucket if two points are close according to a selected similarity metric. On the other hand, the likelihood of such collisions is significantly lower at distant points. Formally, for two points a and b and a distance threshold r , the probability that a and b hash to the same value is high if their distance is below r , and low if above a scaled threshold cr ($c > 1$). Several hash functions and hash tables are frequently used in the implementation to improve accuracy; each hash table employs separately selected hash functions to boost recall while reducing false positives. Only the points in the buckets that match the hash values of the query are regarded as possible matches after it has been hashed similarly upon arrival. When compared to brute-force techniques, this drastically narrows the search space.

[52] provides a practical cancelable biometric framework that uses Locality Sensitive Hashing (LSH) to protect fingerprint templates without compromising recognition accuracy. The method first converts extracted fingerprint data into compact binary vectors before using Locality Sampled Codes (LSC), a randomized sampling technique that selects subsets of bit positions based on an LSH strategy. This makes it impossible for hackers to retrieve the original biometric information and generates a non-invertible, revocable template in which similar fingerprints correspond to similar sampling codes. [53] on non-invertible cancellable fingerprint templates offers a transformation-based method that preserves matching accuracy while converting raw fingerprint characteristics into protected, non-invertible templates using the concepts of Locality-Sensitive Hashing (LSH). In order to maximize inter-class separation

3.2 Cancelable biometric template protection

and guarantee intra-class similarity (real users map to comparable hash codes), the method collects minutiae-based feature vectors and projects them through an LSH-inspired hashing scheme. Because the change is one-way by design, even if the template is compromised, the original biometric cannot be recreated. [54] suggests two cancelable biometric template protection techniques based on Locality Sensitive Hashing (LSH), one optimized for the cosine similarity metric and the other for the Euclidean distance metric. The authors examine the behavior of several LSH families when applied to biometric feature vectors and demonstrate how carefully selected LSH functions can maintain matching accuracy while offering robust privacy through non-invertibility, revocability, and unlinkability. To assess recognition performance, collision behavior, and attack resistance, they do tests on common biometric datasets. Their findings show that LSH-based transformations are a workable alternative for large-scale biometric authentication systems since they can successfully change original biometric templates into safe, cancelable forms without significantly reducing matching accuracy.

3.2.2.3 Index of max hashing

Index of max hashing is a ranking-based variant of locality-sensitive hashing primarily used in biometric security and template protection. By determining the index of the maximum value from randomly projected vector components, it converts a real-valued biometric feature vector into a discrete code. This method is robust against changes in biometric data because it concentrates on the rank of features rather than their actual magnitude. These discrete index codes are created by applying random permutation and using externally generated random parameters. Strong non-invertibility guarantees provided by this discrete representation improve the concealment of biometric information by making it computationally difficult to reverse the hashed code back to the original biometric data. For accurate matching and alignment in biometric systems, it is robust to variations and scale-invariant. Because it supports cancelable biometrics, compromised templates can be removed and replaced without compromising the security and privacy of the original biometric data. Tests conducted on fingerprint databases show how well it works to preserve competitive accuracy while offering defence against a range of privacy and security threats. Additionally, its design guarantees unlinkability, which stops biometric templates from matching across applications.

The index of max hashing method offers a strong and novel approach based on the relative ranking of feature dimensions rather than their absolute magnitudes in the context of biometric template protection and secure hashing techniques. Its inherent resilience to noise and variation, which usually impact the scale but not the relative ordering of biometric

Cancelable biometrics based fingerprint template protection using discrete cosine transform and index of max hashing

data, comes from encoding the implicit order of features. This feature not only improves the generated hash codes' stability and dependability but also helps the method maintain security and privacy in biometric applications. In settings where data variability is a major problem, it thus presents a promising method for accomplishing reliable and privacy-preserving biometric authentication. [55] presents generalized Index of Max hashing, a novel cancelable biometric transformation created especially for unordered and variable-length fingerprint templates like the minutia cylinder-code. It can safely convert intricate minutiae structures into protected hash codes while maintaining discriminative matching capabilities, in contrast to the original index of max hashing, which is limited to fixed-length feature vectors. This makes it a practical and scalable approach for secure fingerprint template protection.

3.3 Methodology

The IT security paradigm evolves from secret-based to biometric identity-based. Biometric identification has become gradually more popular in recent years for handheld devices. Privacy-preserving is a key concern when biometrics is used in authentication systems in the present world today. Nowadays the declaration of biometric traits has been imposed not only by the government but by many private entities also. There are no proper mechanisms and assurance that biometric traits will be kept safe by such entities. The encryption of biometric traits to avoid privacy attacks is a giant problem. Hence, state-of-the-art safety and security technological solutions must be devised to prevent the loss and misuse of such biometric traits. In this paper, we have identified different cancelable biometrics methods with the possible attacks on the biometric traits and directions on possible countermeasures in order to design a secure and privacy-preserving biometric authentication system. We also proposed a highly secure method for cancelable biometrics using a non-invertible function based on Discrete Cosine Transformation and Index of max hashing. We tested and evaluated the proposed novel method on a standard dataset and achieved good results.

We have proposed a novel method for cancelable biometrics in this section. We have presented a non-invertible transformation function using the concept of index of max hashing. The combination of discrete cosine transformation (DCT) and uniformly random permutation based index of max hashing is a non-invertible transformation used in this method. The discrete cosine transformation converts an image from the spatial domain to the frequency domain by subdividing the image into 8×8 blocks. First discrete cosine transformation has been applied on the fingerprint image which makes the resultant templates more complex. After DCT, the uniformly random permutation based index of maxing has been applied in

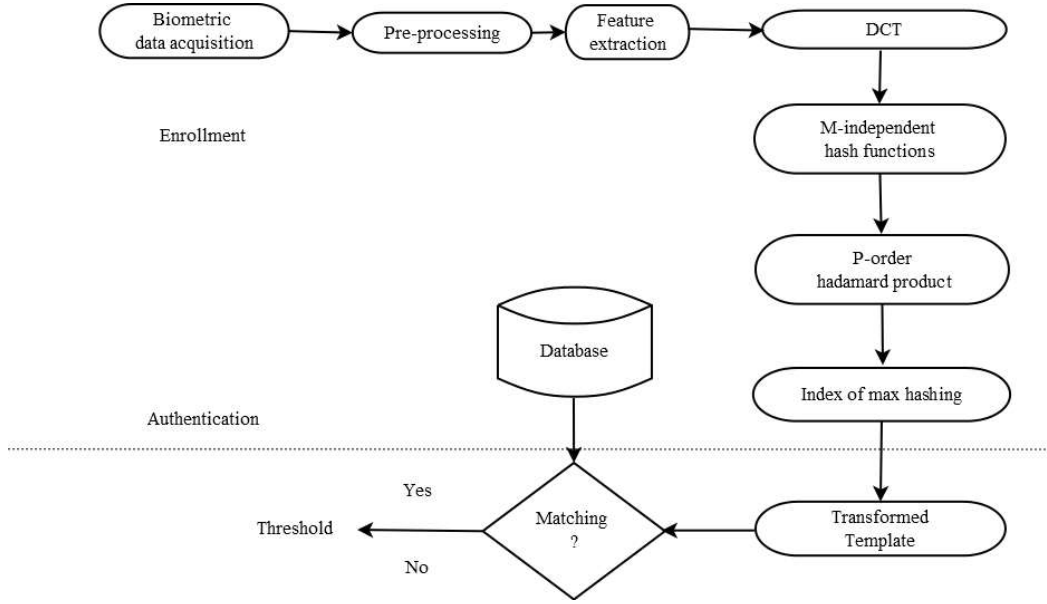


FIGURE 3.2 Diagram of the proposed cancelable biometrics scheme

order to get the transformed fingerprint template from which the original fingerprint cannot be recovered.

The two dimensional DCT transforms an image $f(i, j)$ into the frequency domain $F(u, v)$ by an equation given as,

$$F(u, v) = \alpha_u \alpha_v \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} f(i, j) \cos \left[\frac{\pi u(2i+1)}{2M} \right] \cos \left[\frac{\pi v(2j+1)}{2N} \right] \quad (3.1)$$

where $1 \leq u \leq M-1, 1 \leq v \leq N-1$

$$\alpha_u = \begin{cases} \frac{1}{\sqrt{M}}, u = 0 \\ \sqrt{\frac{2}{M}}, 1 \leq u \leq M-1 \end{cases}, \alpha_v = \begin{cases} \frac{1}{\sqrt{N}}, v = 0 \\ \sqrt{\frac{2}{N}}, 1 \leq v \leq N-1 \end{cases}$$

After applying DCT, the next step is uniformly random permutation based Index of max hashing. Index of max hashing is inherited from the locality of the sensitive hashing concept. The locality sensitive hashing property of index of max hashing gives guarantee of accuracy preservation after hashing. The Index of max hashing can strongly protect biometric data from being inverted. Figure 3.2 shows the block diagram of the proposed method.

The proposed algorithm for generating the cancelable fingerprint template can be summarized as the following steps:

Cancelable biometrics based fingerprint template protection using discrete cosine transform and index of max hashing

- Read the fingerprint image of size $M \times N$. Apply 2D DCT on fingerprint image and find the minimum value of the DCT coefficients and subtract the minimum value from all the DCT coefficients to convert the negative values into positive values.
- For each hash functions $h(x)$, permute the enrolled/query feature vector x randomly for m times, $\hat{x} = perm(x)$ in order to get the permutation set θ .

$$\{\theta_{(l,i)} | l = 1, \dots, q, i = 1, \dots, m\} \quad (3.2)$$

- Generate a p-order Hadamard product vector by performing the element-wise multiplication on the p permuted vectors. For $j = 1, \dots, k$ where k is the window size,

$$\bar{x}(j) = \Pi_{l=1}^p (\hat{x}_l(j)) \quad (3.3)$$

- For each $\bar{x}$, select the first k-elements where $1 < k < d$. Find the maximum entry value within window size k and record its index $t \in [1, k]$ as the hashed code. Repeat the previous steps with different permutations set $\{\theta_{(l,i)} | l = 1, \dots, q, i = 1, \dots, m\}$ and construct hashed code in order to generate the transformed template.

$$\bar{t} = \{t_i \in [1, k] | i = 1, \dots, m\} \quad (3.4)$$

The two fingerprint vectors with high similarity give a high probability of collision in the rank domain when index of max hashing is used with ranking based locality sensitive hashing. On the opposite, the vectors far apart from each other result in a lower probability of hash collision.

3.4 Experiment and analysis

We had tested an empirical study of different cancelable biometric approaches on two public fingerprint datasets FVC2002 DB1 and DB2. Each dataset consists of 100 users with 8 samples per user. There are 800 (100×8) fingerprint images in total in the dataset. The discrete cosine transformation has been applied on the fingerprint image then index of max hashing in order to get the transformed fingerprint template.

The index-of-max cancelable biometric approach with discrete cosine transform has been used in an experiment where the fingerprint vector x with length 299 used as an input. For the matching protocol, 1st to 3rd samples of each user are used as training samples to generate

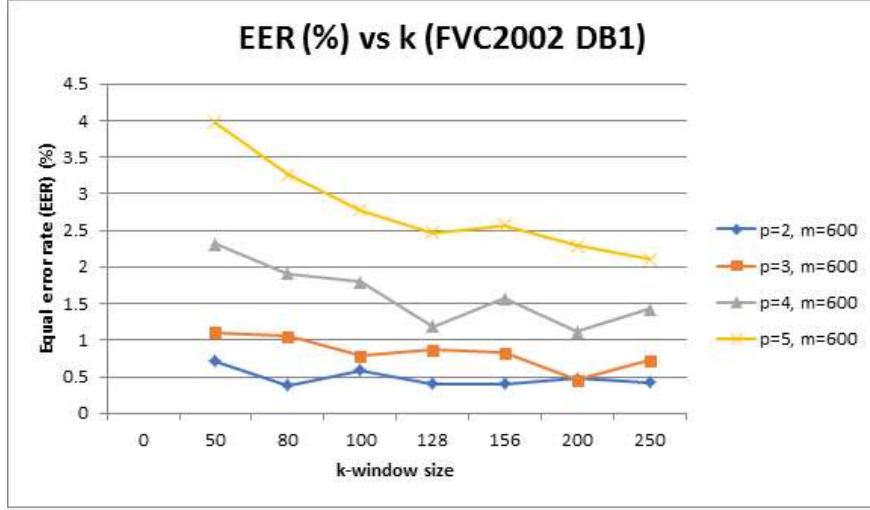


FIGURE 3.3 EER (%) vs k on FVC2002(DB1)

TABLE 3.1 EER (%) vs k on FVC2002(DB1) with hashing functions m=600

EER (%) vs k on FVC2002(DB1) with hashing functions m=600		
Window size k	Hadamard product p	EER (%)
50	[2,3,4,5]	[0.71, 1.10, 2.31, 3.97]
80	[2,3,4,5]	[0.38, 1.05, 1.91, 3.26]
100	[2,3,4,5]	[0.59, 0.79, 1.80, 2.77]
128	[2,3,4,5]	[0.40, 0.87, 1.19, 2.47]
156	[2,3,4,5]	[0.40, 0.83, 1.57, 2.57]
200	[2,3,4,5]	[0.48, 0.46, 1.11, 2.29]
250	[2,3,4,5]	[0.42, 0.72, 1.42, 2.10]

fingerprint vectors. The rest of the 4th to 8th samples of each user are used in this testing. There are 500 (100×5) in total. The experiment tested on the dataset yields 1000 genuine matching scores and 4950 imposter matching scores.

We have tested the effects of different parameters of index of max hashing with discrete cosine transform (DCT) like window size k, hadamard product order p, and the number of hashing function m. As shown in table 3.1, we have checked the performance in terms of EER with respect to the different window size k varied from 50, 80, 100, 128, 156, 200 and 250 by fixing m at 600 for the hadamard product order $p = [2, 3, 4, 5]$. Figure 3.3 and 3.4 show the EER drops gradually when larger k and p is applied. The small k implies fewer comparisons and thus less informative of max ranked features.

As shown in table 3.2 and 3.3, we have tested proposed discrete cosine transform method based on EER performance with respect to the effect of different independent hashing

Cancelable biometrics based fingerprint template protection using discrete cosine transform and index of max hashing

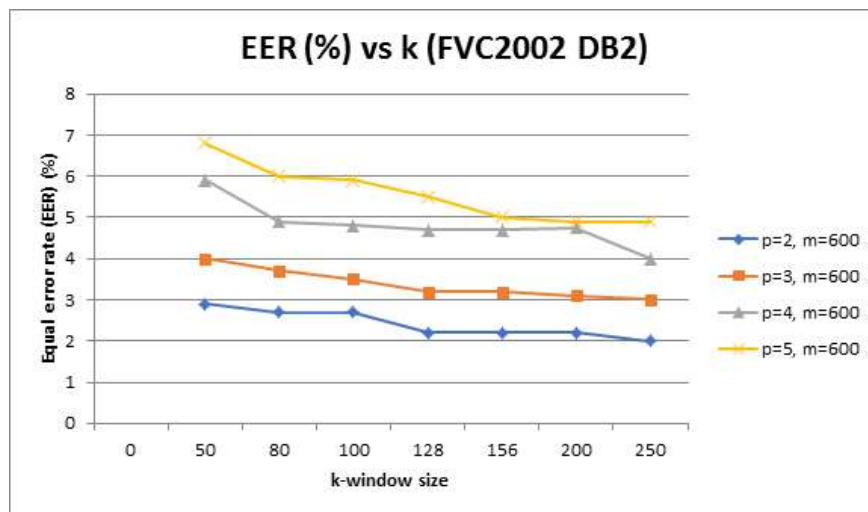


FIGURE 3.4 EER (%) vs k on FVC2002(DB2)

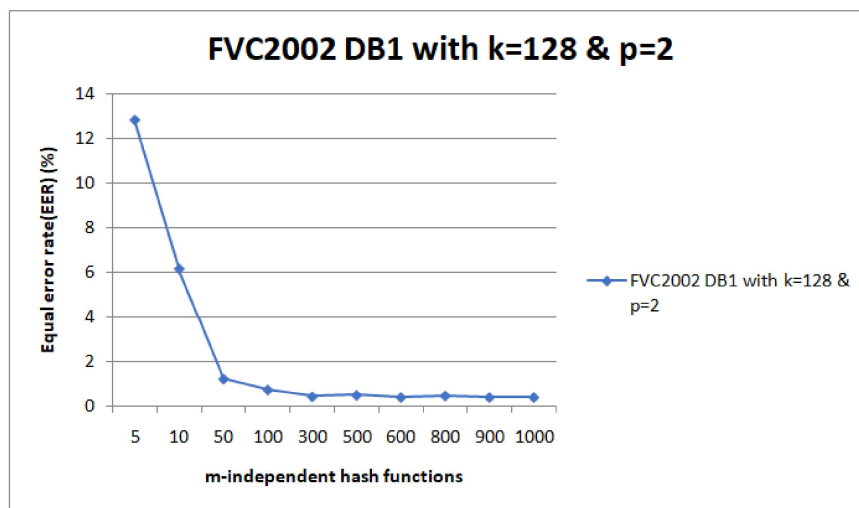


FIGURE 3.5 EER (%) vs m-independent hash functions on FVC2002(DB1)

TABLE 3.2 EER (%) vs m on FVC2002(DB1)

EER (%) vs m on FVC2002(DB1)	
Hash function m	EER (%)
5	12.87
10	6.18
50	1.23
100	0.74
300	0.43
500	0.50
600	0.40
800	0.47
900	0.40
1000	0.40

TABLE 3.3 EER (%) vs m on FVC2002(DB2)

EER (%) vs m on FVC2002(DB2)	
Hash function m	EER (%)
5	8.87
10	2.95
50	0.88
100	0.80
300	0.65
500	0.57
600	0.42
800	0.49
900	0.40
1000	0.40

functions m varied from 5, 10, 50, 100, 300, 500, 800 and 1000 while fixing $k=128$ and $p=2$. Figure 3.5 and 3.6 show the better EER can be attained with respect to the increment of m . The proposed method used DCT with uniformly random permutation based index of max hashing which gives good EER as compared to different cancelable biometrics methods. Table 3.4 shows the comparison of different methods of cancelable biometrics and the proposed method. From the table, we can see that the proposed method is performing better than some of the existing methods. Therefore, it can be one of the potential methods for generating transformed templates. We dedicate this section for analysis of the proposed biometric template protection method based on efficiency, robustness and non-invertibility.

Efficiency: To investigate the time efficiency of the proposed method, we record both average code generation and matching time on a machine with specifications, such as Intel

Cancelable biometrics based fingerprint template protection using discrete cosine transform and index of max hashing

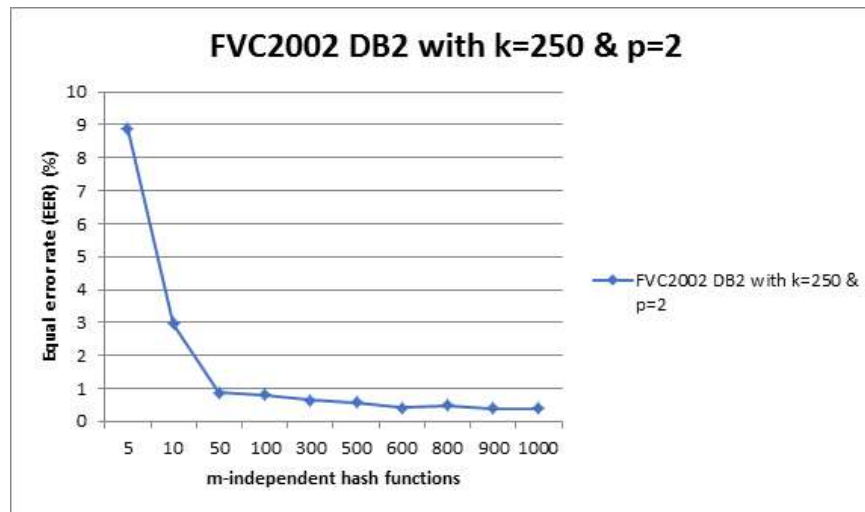


FIGURE 3.6 EER (%) vs m-independent hash functions on FVC2002(DB2)

TABLE 3.4 Equal error rate (EER) of different cancelable biometrics

Cancelable biometrics methods	Equal error rate(%)
B. Choudhury et al. [4]	1.2
S. Wang et al. [12]	1.15
M. V. Prasad et al. [19]	1.8
Z. Jin et al. [11]	0.43
Proposed method	0.39

CPU i7-7700HQ (2.8GHz) and 16GB RAM. MATLAB Ver. 2016a has been used without optimizing code. The computation time of the hash code generation is longer than that of the matching due to a large number of independent hash functions to be generated while matching takes much less time with the simple matcher. The proposed method of generating hash code at the enrollment stage with $k=125$ and $m=600$ on FVC2002 DB1 and DB2 gives average time 0.0685 and 0.0874 sec respectively. The proposed method of matching hash code at matching stage with $k=250$ and $m=600$ on FVC2002 DB1 and DB2 gives average time 1.8457×10^{-5} and 1.9323×10^{-5} sec respectively. Overall, the average matching time meets the expectation for an efficient matching requirement.

Non-invertibility: Non-invertibility enhances the security of the template space by employing a transformation process to reset the order or position of the feature set. It is computationally hard to reconstruct original features with resulting hash values due to one-way transformation characteristic of hashing function. In case hash values are compromised, users will be re-enrolled with a new hash function, hence both non-invertibility and reusability require-

ments are satisfied. Diversity can also be attained since different hash functions are used for old compromised hash values and new hash values. If both index of max hash codes and permutation set θ are revealed, the attack complexity could be significantly reduced. The p-order Hadamard product can largely increase the difficulty of such recovery. In the worst case, assume that the adversary learns the minimum and maximum values of the feature components of x . Let's take an example of FVC2002 DB1, the minimum and maximum values of the feature components are -0.2504 and 0.2132 respectively. Presume the adversary attempts to guess from -0.2504, -0.2503, -0.2502 and so on, until the maximum 0.2132. There are a total of 4636 possibilities. In our implementation, the precision is fixed at four decimal digits, the possibility of guessing a single feature component of x requires 4636 attempts (2^{12}). Thus, the entire 299 feature components require around $2^{12 \times 299} = 2^{3588}$ attempts in total. Obviously, this is computationally infeasible.

Robustness: In the proposed method, index of max hashing contributes strong concealment to the biometric traits. This empowers the notion of non-invertibility guarantee. The index of max hashing is a type of ranking based hashing method that relies on the relative ordering of feature dimensions so independent to the magnitude of the features. The proposed method transforms a real-valued feature vector into an index code such that the pairwise-order measure in the hashed codes are closely correlated with rank similarity measure.

3.5 Summary

Due to the non-revocable nature of the biometric traits, it cannot be replaced if once stolen by an adversary. Hence it would be better to find such a solution which gives security of biometric traits with high accuracy and makes templates as non-invertible and revocable as and when it requires. The main challenge is to design such a transformation approach for cancelable biometrics such that it provides high security with accuracy as it is a complicated task because of biometric intra-class variability. Another challenge is to cope up with record multiplicity attacks such that intruders cannot recover the original biometric template by interlinking the multiple templates from the different applications.

CHAPTER - 4

Cancelable biometrics for fingerprint template security based on speeded up robust feature, fast fourier transform and index of max hashing

4.1 Introduction

A person can be recognised or verified using biometric systems based on their physical or behavioural characteristics. Biometrics is well-defined as automated systems for recognising or verifying an individual based on his or her physiological or behavioural traits. The interesting notion of biometrics is that our body itself acts as a password. Individual identification is the act of associating a particular person with an identity. People are increasingly connected through electronic means in the age of information technology. Because of the prominence of privacy and security of information, automatic individual identification systems have become a very vital area in e-commerce, electronic banking, smart cards, etc [56]. There are two types of traditional automatic identification techniques that have been commonly used, i.e., knowledge-based and token-based. The token-based identification system uses some proof to prove personal identification. Persons are identified by representing that they are the owners of certain tokens, such as an Aadhar card, a PAN card, a passport, etc. The knowledge-based identification system uses something that you remember or know to prove your personal identification. Persons are identified by recalling the information or knowledge that only they are anticipated to know, such as a password, pin, etc [24].

The main benefits of traditional identification techniques are their simplicity and ease of integration with different systems. But these traditional identification techniques are not based on any inherent attributes of an individual. Hence, these different methods have a number of disadvantages. The token based authentication technique is prone to loss or theft

4.2 Cancelable fingerprint biometric template protection

of individual tokens, while the knowledge based authentication technique is prone to fraud of a password or pin. Hence, traditional approaches are unable to cope with the security requirements. In recent years, immense research has been carried out in the literature in order to address the different biometric authentication system issues like security, privacy, revocability, and unlinkability [57]. In the literature, the cancelable biometrics method is recommended as the most promising solution to these problems [58].

In this research, we identified various cancelable biometrics methods, as well as potential biometric trait attacks and countermeasures, in order to create a secure and privacy-preserving cancelable biometric system. The proposed transformation builds upon a speeded up robust feature, the index of maximum hashing, the hadamard product vector. We have used the most secure method of hashing like index of max hashing with the hadamard product. In comparison to previous approaches, the security analysis used in this research is more thorough. We highlight a key aspect of the suggested method, namely that it keeps the stochastic distance between feature vectors after transformation. The proposed method's security analysis is theoretically supported, further illustrated, and experimentally confirmed. The suggested template protection scheme's limit is to cope with record multiplicity attacks such that intruders cannot recover the original biometric template by interlinking the multiple templates from the different applications.

4.2 Cancelable fingerprint biometric template protection

Biometrics is a popular way to authenticate users. However, it has many challenges, particularly those related to security, as discussed in [59]. Techniques for protecting biometric template data are crucial for safeguarding the biometric template kept in the database. Available techniques in the literature for securing biometric templates can be categorised into two types: protection methods based on transformation (cancelable biometrics) and biometric cryptosystems. Biometric cryptosystem [7] provides biometric template security based on biometric features and cryptography, whereas transformation-based techniques like cancelable biometrics use non-invertible transformation and salting. Cancellable biometrics refers to the intentional and consistently used distortion of biometric characteristics to safeguard private user information. A thorough review of various frameworks for the recognition and protection of biometric templates existing in the literature are presented here [31].

A secure fingerprint authentication system can be considered essential without compromising the authentication performance of the system. There are four main characteristics to comply with, and they are security, performance, revocability, and diversity [29]. In addition,

Cancelable biometrics for fingerprint template security based on speeded up robust feature, fast fourier transform and index of max hashing

the suggested technique's four key qualities are compared with the benefits and drawbacks of many other techniques now in use. They provide strong motivation for the development of the proposed technique. Two major approaches, the feature transformation approach and the biometric cryptosystem-based approach, are used to protect biometric templates [60]. Salting and non-invertible transformation-based approaches are further categories for feature transformation-based techniques. Key generation-based and key-binding-based biometric cryptosystem-based techniques are other subcategories. On the basis of these methods, a number of other methods have been suggested in the literature [31].

Approach	Authors & Publication Year	Databases	EER (%)
Cartesian, polar, and surface folding transformations	Ratha et al.(2007)		
Hadamard transform	Wang and Hu (2013)	FVC2002 DB2	3%
Partial hadamard transform	Wang et al.(2017)	FVC2002 DB1	1%
		FVC2002 DB2	2%
		FVC2002 DB3	5.2%
		FVC2002 DB4	13.3%
Graph-based Hamming	Jin et al.(2014)	FVC2002 DB1	4.36%
		FVC2002 DB2	1.77%
Minimum spanning tree based	Prasad et al.(2014)	FVC2002 DB1	1.8%
		FVC2002 DB2	1.2%
Curtailed circular convolution	Wang and Hu (2014)	FVC2002 DB1	2%
		FVC2002 DB2	3%
		FVC2002 DB3	6.12%

TABLE 4.1 Comparison of Cancelable biometric methods for protecting fingerprint templates

4.2.1 Preliminaries

The speeded-up robust features, fast fourier transform, and index of max hashing are all briefly discussed in this section.

4.2.1.1 Speeded-up robust features

Feature selection is one of the most widely used techniques and involves choosing a subset of features from a given set that best capture the important data properties. It is an essential

4.2 Cancelable fingerprint biometric template protection

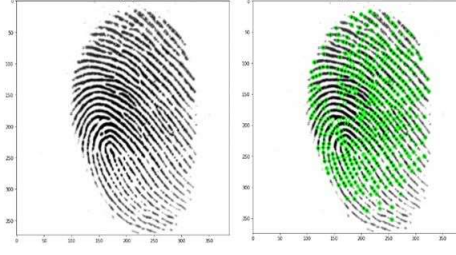


FIGURE 4.1 SURF Fingerprint Feature Detection

step used to reduce dimensionality, irrelevant data, and redundant data in order to improve performance. As shown in figure 4.1, speeded up robust features are a proprietary local feature extractor and classifier in computer vision. It is a speeded-up variant of SIFT, as it adds a lot of features to improve the speed at every step [61]. The rotated and blurred images can be easily handled using Speeded up robust features which is essential for improved authentication [62]. A straightforward estimate of a Hessian matrix is the basis of the speeded-up robust features method for locating interest points, as it is used because of its accuracy and quick computation times. It employs horizontal and vertical Haar-wavelet responses for feature description [63].

4.2.1.2 Fast Fourier Transform

In the transformed domain, the discrete Fourier transform ought to produce a dense data representation. The effective fast Fourier transform algorithms can be used to carry out the discrete Fourier transform operation. By factoring the discrete Fourier transform matrix into a product of sparse (mainly zero) elements, an fast Fourier transform quickly computes such transformations. Due to the unitary nature of the discrete Fourier transform matrix, take into account that the discrete Fourier transform is invertible. To ensure that the frequency samples of the feature vector are not sparsely distributed, the discrete Fourier transform is used to spread out the feature vector's spectrum [28].

The DFT matrix F is expressed as $F =$

$$\begin{bmatrix} 1 & 1 & 1 \dots & 1 \\ 1 & W & W^2 \dots & W^{N-1} \\ 1 & W^2 & W^4 \dots & W^{2(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & W^{N-1} & W^{2(N-1)} \dots & W^{(N-1)(N-1)} \end{bmatrix}$$

Cancelable biometrics for fingerprint template security based on speeded up robust feature, fast fourier transform and index of max hashing

with $W = e^{-j2\pi/N}$

The two dimensional Discrete Fourier Transform (DFT) transforms an image $f(i, j)$ into the frequency domain $F(u, v)$ by an equation given as

$$F(u, v) = \sum_{i=0}^{N-1} \sum_{j=0}^{M-1} f(i, j) e^{-2i\pi(\frac{ui}{N} + \frac{vj}{M})} \quad (4.1)$$

where $1 \leq u \leq N-1$, $1 \leq v \leq M-1$ and $f(i, j)$ is the pixel intensity value at (i, j) in the spatial domain image of size $N \times M$.

4.2.1.3 Index of Max Hashing

The index of maximum hashing was motivated by the locality-sensitive hashing used in the information retrieval field. Significant empirical and theoretical assurance of accuracy retention after hashing is provided by the index of maximum hashing. Its non-linear transformation from real-valued biometric data is explained by its pure maximum ranking and discrete index representation. Biometric data can be efficiently protected from inversion using the maximum hashing index [64]. A biometric feature vector is converted into a discrete max index of the hash code using the index of maximum hashing. Uniformly random permutation-based hashing algorithms are used to determine the index of maximum hashing.

4.3 Methodology

Biometric authentication methods have become more popular in recent years because they do not need a password or pin. These methods use features unique to individuals, making them hard for others to tamper with. Since biometric traits cannot be changed like passwords, protecting privacy is a vital area of research. We need to develop secure technology to stop biometric traits from being stolen or misused. In this work, we present a cancelable biometrics technique that offers a safe and reliable biometric authentication system. We had proposed a highly secure method for cancelable biometrics using a fast Fourier transform of an index of max hashing and Hadamard product vector after an accelerated robust feature approach for the extraction of picture features. The results of testing and evaluation of the proposed approach on standard datasets, FVC2002-DB1, and DB2, are fairly good.

The fingerprint template in this study is to be protected using the algorithm that has been proposed. Speeded up robust features were used to extract and select fingerprint features from the image, and they were then permuted to produce a robust, non-invertible template.

The proposed method of biometric template protection, namely the fast fourier transform and index of maximum hashing with hadamard product, has been demonstrated and compared in terms of EER. To achieve good accuracy with low computational complexity, we used the fast fourier transform based features for fingerprint matching. The proposed method reasonably gives a good recognition rate. The data domain has a vector B_v that can be used to describe a biometric representation. where, B_v is the feature vector with v dimensions. Because B_v contains sensitive biometric data, its security is critical. After extracting features with the speeded-up robust features, take N-point discrete Fourier transform of B_v . The fast fourier transform algorithms $B_V = FB_v$ can be used to carry out the discrete Fourier transform procedure. The unitary nature of the discrete fourier transform matrix allows the inversion of its operation. The fast fourier transform is used to spread out the spectrum's frequency samples so that they are not sparsely distributed.

The next step is to create a non-invertible transformation using index of max hashing with hadamard product vector that uses uniformly random permutation based hashing to safeguard B_V . If B_V secure, the feature vector B_v will also be safe. Let's create a row vector with length h and length N as the vector B_V , represented by the notation $H = [h_1, h_2, \dots, h_r]$, where $h < N$ with $N = 2^n$. Every entry in H is a strictly positive integer with the property that $h_i \neq h_j$. In cancelable biometrics, the vector K serves as a parameter key and is capable of being created at random. Using H , we create a submatrix of H_n called H'_n , where the i^{th} row of H'_n corresponds to the k_i^{th} row of H_n for $i \in [1, \dots, h]$. The transformation is non-invertible since it is a row-reduced submatrix of H_n and is always column rank deficient, in accordance with the characteristics of the hadamard matrix. The altered fingerprint template was created using the uniformly random permutation-based index of max hashing, from which the actual fingerprint could not be recreated. This phase involves creating random matrices g , adding them to the feature vector B to create z , and then recording the index of the highest value in c as the hashed code. The original biometric information is thus strongly concealed using index of max hashing, which converts features from the real value domain into the index domain.

In order to calculate a hash, we index the incoming data through the permutation array of the hash, therefore permuting the input vector $B_v = [x_1, x_2, \dots, x_k]$, yielding p permuted vectors, $p = \text{perm}(B)$. To create the h -order hadamard product vector z , element-wise multiply the p permuted vectors. Next, the y initial elements of the permuted vector Z are chosen for every section: $[x_1', x_2', \dots, x_y']$. When we compare these elements, the largest element's index is noted as c_i . To get the s hash section, this procedure is performed s times. A single hash c is created by concatenating these hash sections.

Cancelable biometrics for fingerprint template security based on speeded up robust feature, fast fourier transform and index of max hashing

The algorithm of biometric template security using proposed method is given below:

Biometric Template Security Algorithm

Input: Input: Fingerprint image of size $M \times N$, FVC2002

Output: Output: Hash Code $c = \{c_i \in [1, y] | i = 1, \dots, s\}$

Step 1: Read the fingerprint image. Extract fingerprint features using speeded-up robust features B_v .

Step 2: Apply the fast fourier transform to the v-dimensional fingerprint feature vector.

Step 3: Select and permute the strongest extracted features. Generate a permutation set θ for each hash function s based on g random permutation.

Step 4: Using s distinct hash functions $\{hash_i(X), i = 1, \dots, s\}$, randomly permute feature vector B for g times, yielding p permuted vectors, $p = \text{perm}(B)$

Step 5: To create the h -order Hadamard product vector z , element-wise multiply the p permuted vectors.

Set $z(j) = \prod_{l=1}^h (p(l))$

Step 6: Select the first y elements of the each z permuted vector.

Step 7: Initialize the i^{th} hash code $c_i = 0$.

Step 8: Within the y items, pick the largest elements.

Step 9: Note the bits for the corresponding index values, c_i .

For $j = 1 \rightarrow y$

If $z(j) \geq z(c_i)$

then $c_i = j$;

Step 10: Repeat m times steps 4 to 8 in order to get a hash code of length s ,

$c = \{c_i \in [1, y] | i = 1, \dots, s\}$

4.4 Experiment and analysis

The proposed approaches' performance was examined in terms of False Accept Rate, False Reject Rate, and Equal Error Rate. A non-genuine user is accepted at a rate known as False Accept Rate, while a legitimate user is rejected at a rate known as False Reject Rate. Accuracy can be calculated as, $Accuracy = \max(100 - ((FAR_j + FRR_j)/2))$, where j is the particular threshold point and FAR_j and FRR_j are the values of FAR and FRR, respectively for the j^{th} threshold value.

More legitimate attempts will be classed as matches while less impostor attempts will be mistakenly labelled as matches as the score threshold rises. The ROC curves for the

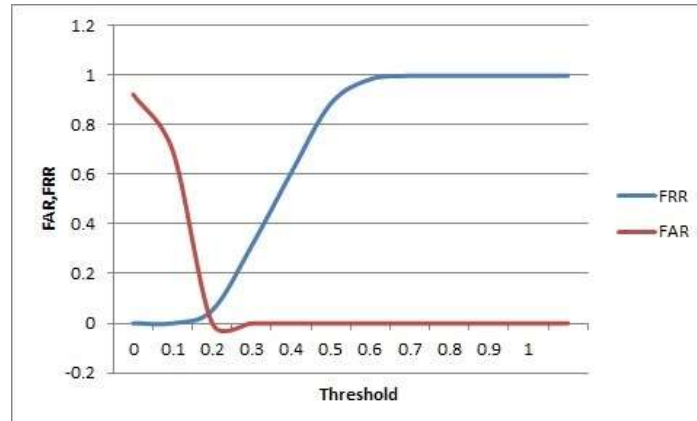


FIGURE 4.2 FAR and FRR versus threshold - FVC2002 database

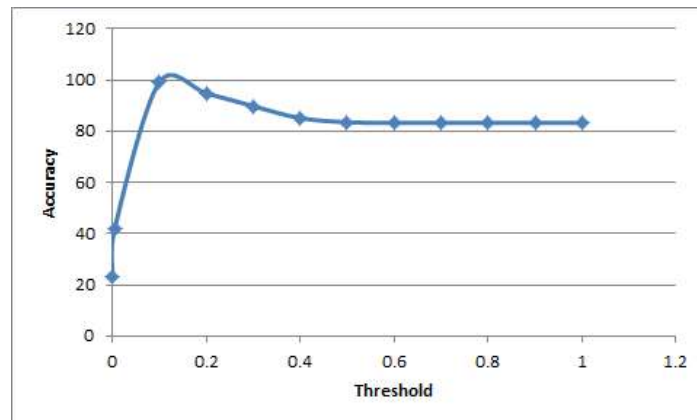


FIGURE 4.3 Accuracy plots for the proposed technique on FVC2002 database

Cancelable biometrics for fingerprint template security based on speeded up robust feature, fast fourier transform and index of max hashing

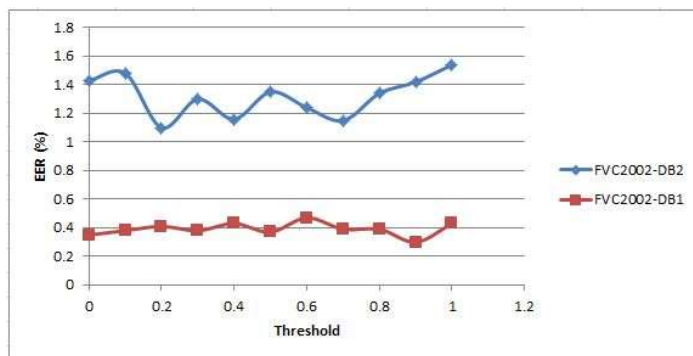


FIGURE 4.4 Comparison of EER for the proposed methods on FVC2002 database

FVC2002 dataset for various threshold settings in relation to the False Rejection Rate and False Acceptance Rate are shown in Figure 4.2. As the threshold/sensitivity increases, the FAR should decrease because the authentication system should be secure and doesn't allow unauthorized users. Increasing FRR indicates user convenience and decreasing FAR indicates a more secure system.

Figure 4.3 displays the suggested technique's accuracy for various threshold settings. The value of Total success rate / Accuracy decreases from higher to lower values as threshold increases. The proposed method of cancelable biometrics had been tested on the FVC2002-DB1 and DB2 datasets. To determine the average EER value, first obtain the EER values for the various authentication thresholds. The EERs for the various thresholds attained using the suggested strategy on the FVC2002-DB1 and DB2 datasets are shown in Figure 4.4. For the FVC2002-DB1 and DB2 datasets, the average EER is 0.40 and 1.31, respectively. It has been clearly seen that in general, the proposed method on the FVC2002-DB1 dataset has achieved smaller EERs (i.e., higher verification accuracy) than the FVC2002-DB2 dataset.

Non-invertibility: The biometric template's security is increased by its non-invertibility, which employs a transformation technique to reset the feature set's position or order. Reconstructing original features from hashed code is computationally challenging due to the hashing function's one-way transformation property. The needs of non-invertibility and reusability are satisfied by re-enrolling a user with a new hash function if their hash values are compromised. The different hash functions are used, increasing the variety, for both newly created hash values and previously compromised hash values.

4.5 Summary

We presented cancelable template generation using the index of maximum hashing, the fast fourier transform, the hadamard product, and speeded-up robust features-based feature extraction in this study. According to theoretical reason and actual evidence, the index of maximum hashed codes can substantially maintain accuracy performance as a rank correlation attribute. The proposed method is also shown to satisfy non-invertibility template protection criteria. Subject to correctly calibrated parameters, it is also very resistant to several important security and privacy attacks that are now in use. The paths for our future work will be to continue to push the suggested template protection scheme's limits. To look into further options, though, would be inspiring. In the future, we can put the proposed strategy to the test by combining encryption, watermarking, and steganography techniques for developing efficient cancelable biometric recognition systems. Another challenge is that we may think about extending it to multi-biometrics, where a different biometric modality could be utilized to construct the feature.

CHAPTER - 5

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

5.1 Introduction

The science of pattern recognition involves observation, The science of pattern recognition involves observation, recognition of patterns that are of interest, and accurate judgment about patterns. Pattern recognition is used by a biometric system to identify and categorize individuals by comparing them with saved templates. Biometric systems categorize and individually identify people based on physical traits or biological measurements using pattern recognition algorithms. Biometric identification is becoming more common in our daily lives. Even when twins are involved, physical traits are relatively unchanged and unique. Password systems for handheld devices, such as smartphones, tablets, and computers, as well as areas with restricted access, can be replaced with each person's distinctive biometric identity. Although biometric authentication is practical, privacy advocates worry that biometric security may jeopardize individual privacy. There must be some place to keep all that data, which feeds concerns about ongoing monitoring and data misuse. There is a possibility of a password database in which hackers might compromise security and grab unprotected data. However, there are distinctly different consequences. A password can be changed if it has been compromised. According to the contract, the biometric data is generally unchangeable. Individual trait security is, therefore, more important [1].

If a biometric system's design prioritizes performance over security and an unpredictable template space, it is to be assumed that the system will lack the randomness that is necessary for those two goals. As a result, creating a non-invertible function that meets both security

and accuracy requirements is quite difficult. The cancelable approach offers greater privacy because the actual biometrics of the user are never disclosed throughout the authentication procedure [31]. Cancelable biometrics are biometric signals that have been purposefully and repeatedly distorted using transforms that let users compare biometric templates in the transformed domain. Potential imposters must not be able to reverse such transformed biometric templates.

The distortion properties are altered if a cancelable feature is breached, and the identical biometric data is translated to a new template that is then used [25]. The actual template is not easy to reconstruct even if the key is known, but the non-invertible transform protection strategy offers stronger security than the salting approach. The non-invertible transform uses a one-way function to safeguard the biometric trait. The one-way function is simple to calculate but extremely challenging to reverse [26]. This method makes it computationally challenging for the attacker to restore the real biometric, even if he possesses the theft key and the altered template [24].

5.2 Learning based biometric template protection

Numerous academics have studied the security of the cancelable fingerprint approach. The principle of cancelable biometrics was introduced by [12]. To create several patterns from a fingerprint template, the authors took into consideration a wide range of non-invertible transforms, including Cartesian, polar, and functional transformations. The template makes use of the necessary minute details. The underlying, minute particulars create the fingerprint pattern. Original minutiae details are not kept in memory. Locations and orientations of minutiae are modified irreversibly. It is reasonable for the researchers to assume that a connectable, cancelable transform exists in the feature space. In addition to a cancelable fingerprint biometric template, the error correction-based key binding structure was provided by [34]. The research team used the VeriFinger 7 SDK to extract details from five public datasets while conducting their investigations. The approach may apply to different types of biometric features rather than just binary biometrics, as required in fuzzy commitment, allowing for the selection of a more potent matcher.

The majority of fingerprints are represented by minutiae, which are used to identify them [13]. In contrast to global features like a single point or ridge line shape, fingerprint minutiae offer enough individuality for precise matching. The minutiae representation is unorganized and varies in size due to the variability in the quantity of fake and missing real minutiae that occurred in different impressions of the same finger. The goal was to shorten the bit

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

string by switching from minutiae triplets to minutiae pairings [22]. As a result, the size of the template is decreased to 2^{18} and its effectiveness is improved by using a training procedure based on a majority vote. The suggested approach entails feature extraction from pairs of fingerprint minutiae, quantization, histogram binning, binarization, and ultimately, the production of binary bit strings.

By taking into account the aggregate wall distance, the average minutiae coordinate within a cuboid, and the standard deviation of the minutiae coordinates, this is considered a robust collection of characteristics [6]. Numerous additional features are extracted from the minutiae inside each such cuboid once a large number of contiguous patches are randomly chosen in the minutiae space. Although the fingerprint image must be aligned with registration points before feature extraction, this method performs well with good accuracy. On low-quality images, however, it can be difficult to recognize registration points. A plan that depends on the dense infinite-to-one mapping (DITOM) technique was put up by [65]. From two minutiae, it retrieves three invariant traits. After that, the retrieved features are binarized, hashed, and quantized. The next step is to use the DFT to create a complex-valued vector from the resulting bit string. To construct the final template, this complex vector is then merged with a random matrix. The intended transformation effectively implements an infinite-to-one mapping by describing the intersection of a number of hyperplanes.

[29] had proposed a method that generates the cancelable templates without requiring the pre-alignment of the fingerprint based on fingerprint minutiae representation. First, generate a minimum spanning tree for the fingerprint minutiae in a three-dimensional feature space, which connects all the minutiae points. Then, the two-dimensional feature space is generated based on the chain code representation from the generated MST. A bit string is then generated by mapping the chain code into the 2D array. Minutiae consists of (x, y, θ) , where (x, y) represents the minutiae coordinates and θ denotes the orientation of the minutiae. The set of minutiae is denoted by M .

$$M = \{M_i(x_i, y_i, \theta_i)\}_{i=1}^m \quad (5.1)$$

where m is the number of minutiae, (x_i, y_i) are the coordinates, and θ_i is the orientation of the i^{th} minutiae. From these minutiae points, a spanning tree is a connected acyclic subgraph of the connected graph. MST of the $G = (V, E)$, such that the total weight or the total length of the edges is minimum. Considering the minutiae set M as the vertices V . The prim's algorithm has been explored by finding $(m - 1)$ edges from the $m \in e_{ij}$ edges that form the MST, g' , with a minimum total weight $m(m - 1)/2$.

The chain code CC is constructed from the generated MST by pairing up the length L of the edge e_{ij} and the orientation of the starting vertex of the edge θ . After selecting the

5.2 Learning based biometric template protection

initial vertex, the tree is traversed by breadth-first search and produces the sequence of edges e_i where $i=1,2,...,m-1$. For each edge e_i with two measurements, the weight of the edge (L_i) and the orientation (θ_i) of the minutiae v_i . Hence the chain of code C_i is the sequence of $(L_1, \theta_1)(L_2, \theta_2) \dots (L_{m-1}, \theta_{m-1})$.

$$C_i = (L_i, \theta_i); i = 1, 2, \dots, m - 1 \quad (5.2)$$

[27] had proposed ranking-based locality-sensitive hashing for cancelable biometrics, which uses index-of-max hashing. First, LSH had been used to maximize the probability of a collision for similar biometric features. The locality sensitive hashing function $h : M \rightarrow S$ is an effective way of reducing the dimensionality of the data by hashing the input items $M = (m, d)$ with a threshold $R > 0$, so that the similar items map to the same buckets $s \in S$ with the high probability of collision. LSH is a probability distribution on a family H of hash functions h such that $P_{h \in H}[h(X) = h(Y)]$. The objects p and q can collide with probability at least P_1 . If $d(p, q) \leq R$, then $h(p) = h(q)$.

The index of max hashing transforms the fixed-length real-valued biometric feature vector into discrete index max-ranked hashed code. It provides strong concealment to the biometric information such that it cannot be inverted. The two variations of the index of max hashing that had been proposed were Gaussian random projection-based and uniformly random permutation-based hashing schemes. The winner-takes-all hashing is a non-linear transformation that performs H random permutations on the input biometric vector with dimension d , $x \in R^d$. Then select the first k items of the permuted x and choose the largest element within the k items, and also record the corresponding index values in bits. The previous steps are repeated m times, yielding a hash code of length m .

Biometric templates that are represented by real-valued vectors of a fixed length are subjected to the BioHashing algorithm in [43]. It creates binary templates that are either shorter or the same length as the original. The biometric template is created by transforming the fingerprint features into a real-valued vector of a predetermined length. The biometric template $T = (T_1, \dots, T_n)$ is converted into a binary template $B = (B_1, \dots, B_m)$ by the BioHashing algorithm. The BioHashing algorithm is distinctive because it employs a random seed of m bits and a one-way function. Every enrolled biometric feature generates a unique BioCode using a separate seed, which is crucial to remember. The scalar products with the orthonormal vectors guarantee the algorithm's performance, and revocability and diversity features are guaranteed by the random seed. Iterated mixing between the biometric feature and the user-specific pseudo-random number is the basis of BioPhasor, a type of cancelable

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

biometrics that was first introduced in [66]. The BioHashing algorithm is meant to be improved by the BioPhasor algorithm, which is a cancellable biometric technique that combines user-specific random numbers with biometric features to create a unique, compact binary code. It is designed to be revocable, meaning the biometric template can be reissued by replacing the token if it gets compromised.

Neural networks and sophisticated machine learning algorithms are used in machine and deep learning-based feature extraction techniques to automatically recognise and extract significant features from biometric data. A more thorough comprehension of the underlying structures is made possible by these techniques' ability to identify and model intricate patterns and representations in the data. As a result, when compared to conventional techniques, machine and deep learning-based approaches [67] frequently yield better performance and accuracy in feature extraction.

5.2.1 Machine/deep learning-based feature learning approaches

A promising approach to improving the functionality and dependability of cancellable biometric systems is feature learning based on machine and deep learning. Supervised and unsupervised learning are the two main types of machine and deep learning techniques used for feature learning in cancellable biometrics design. The use of labelled data is the primary difference between these methods; supervised learning makes use of labelled datasets to inform outcome prediction, while unsupervised learning does not.

5.2.1.1 Supervised machine/deep learning approaches

One machine or deep learning technique that stands out for its dependence on labelled datasets is supervised learning. These datasets are used to train, or "supervise," algorithms so they can accurately classify data or forecast results. A supervised learning model can assess its performance, gauge accuracy, and improve its predictive power over time by utilising labelled input–output pairs.

Neural networks—such as convolutional neural networks (CNNs) [68] and recurrent neural networks (RNNs) [69]—are among the most commonly used models in supervised machine and deep learning.

Convolutional neural network

The proposed system in the paper by [70] introduces a cancelable multi-biometric recognition framework leveraging deep learning, specifically convolutional neural networks (CNNs), to enhance template protection and recognition accuracy for biometric traits such as face and

5.2 Learning based biometric template protection

fingerprint data. To separately extract reliable and discriminative features from each biometric modality, the technique combines several CNN architectures. In order to improve security and privacy, these features are then changed using cancelable transformation techniques, which guarantee that the original biometric data cannot be reconstructed from the stored templates. Major concerns regarding irreversibility and renewability in biometric systems are addressed by the use of cancelable biometrics, which enable the renewal of templates in the event that they are compromised. When compared to conventional biometric solutions, the suggested system performs better in terms of resilience and recognition accuracy. Based on publicly accessible face and fingerprint datasets, the experimental results demonstrate that the multi-biometric approach, which combines transformed features from multiple modalities, performs better than single-biometric systems in terms of recognition rates and resilience to different attack scenarios. Furthermore, even after applying cancelable transformations, the system retains a high matching accuracy, suggesting that template protection measures have little effect on verification performance. All things considered, the study shows how well deep learning-based feature extraction and template transformation work to protect multi-biometric systems while maintaining robust identification capabilities.

In order to improve cancellable biometric authentication systems, [68] suggests a novel deep learning-based framework for face image retrieval. Strong facial features are extracted using deep neural networks, and these features are then mapped into compact, stable binary codes using hashing techniques. With template cancellability, this method protects user privacy and security while allowing the system to retrieve face images quickly. In order to preserve similarity relationships within the biometric data, the authors incorporate a deep hashing model that makes use of multiple loss functions. This lowers noise and increases the hash codes' dependability. To further secure the stored biometric templates, cryptographic hashing is also applied to these codes. Additionally, the framework presents an application-specific XOR string mechanism that makes it simple to revoke and regenerate biometric templates while maintaining the cancellability feature and biometric uniqueness. The suggested approach performs well on benchmark datasets for iris and face biometric data in terms of outcomes. Experiments demonstrate that the deep hashing-based framework outperforms traditional hashing techniques in terms of retrieval accuracy, especially when it comes to preserving high precision across a range of recall levels. In terms of mean average precision (mAP), retrieval precision, and robustness against variations like intra-class differences and expression changes, the method performs better than other state-of-the-art approaches. Key issues in cancellable biometrics, such as template security, revocability, and identification accuracy, are effectively addressed by combining deep learning

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

with cryptographic techniques. Overall, the study offers compelling proof that deep face image retrieval using the suggested framework improves security for cancellable biometric authentication systems while also having practical applicability.

Artificial neural networks with multiple layers, such as convolutional neural networks, are used to categorize images and discover patterns at the pixel level. Rather than learning a single global weight matrix between two layers, convolutional neural networks seek out a collection of neurons that are locally coupled. Convolutional neural networks aim to learn data-specific kernels rather than employ one of the predefined kernels. By making a single adjustment to a convolution kernel, filters make it simple to carry out complex operations. Applying a Gaussian blur kernel will smooth things out. By using the Canny kernel, you can see all edges. To obtain gradient features, apply the Gabor kernel.

A normal CNN typically includes convolutional layers, pooling layers, and fully connected layers, even though there are numerous distinct CNN architectures. The output feature map is produced by convolving a feature map from the preceding layer with several kernels at the convolutional layer before passing it to the activation function [71].

Convolutional layers can employ a variety of nonlinear activation functions, including sigmoid, rectified linear units (ReLUs), and hyperbolic tangent functions. This study selects the ReLU activation function by considering gradient disappearance and calculation cost. The pooling layer, which frequently follows the convolutional layer, is applied to make the feature map smaller, reducing the computational load. The maximum pooling method performs local maximums, whereas the average pooling method performs average operations on input features. An upsampling layer in the decoder is a straightforward layer with no weights that is used to expand the input's dimensions, compared to the pooling layer. A fully connected layer connects every neuron in both layers and, like a traditional multilayer neural network, turns the feature maps into a one-dimensional feature vector.

Linear discriminant analysis

A key dimensionality reduction method in machine learning that functions within a supervised learning framework is called linear discriminant analysis (LDA). In order to find a linear feature combination that best discriminates between two or more classes, it uses labelled data during the training phase. LDA projects the data onto a lower-dimensional space where class separability is maximised by optimising the ratio of between-class variance to within-class variance. By focussing on class-distinguishing features, this procedure not only makes data representation more efficient but also improves classification performance.

By combining Linear Discriminant Analysis (LDA) and random permutation, [72] present a novel method for creating cancelable biometric templates. To improve the security and

5.2 Learning based biometric template protection

privacy protection of the biometric data, the suggested method performs LDA-based feature extraction after applying a random permutation to the biometric feature vectors. By acting as a non-reversible transformation, this random permutation allays privacy concerns by making it difficult to retrieve the original biometric data from the stored templates. By applying LDA after permutation, the method also aims to maximise class separability in the transformed space and enhance the discriminative power of the features. This combination makes it easier to create cancelable templates that are non-linkable and revocable—two essential requirements for designing secure biometric templates.

According to the study's experimental findings, the random permutation-based LDA approach outperforms conventional cancelable biometric techniques in terms of recognition accuracy while offering robust security guarantees. The suggested approach retains dependable biometric recognition performance in spite of the applied transformations, according to tests conducted on common biometric datasets. Additionally, the technique ensures template unlinkability by demonstrating resilience against frequent attacks like template inversion and cross-matching. These findings demonstrate how well the suggested method balances template security and privacy with biometric recognition accuracy, making it a viable option for cancelable biometric systems in the real world.

Recurrent neural networks

By retaining information from prior time steps, recurrent neural networks (RNNs), which are neural architectures made up of one or more layers with recurrent connections, are able to process sequential data. These networks' innate ability to retain and use previous contextual information when evaluating current inputs makes them especially well-suited for learning patterns in time-series data, such as speech signals, video streams, and character sequences. A careful examination of the literature reveals that RNNs have not yet been applied to cancellable biometric systems, despite their considerable value in simulating sequential dependencies and their effective use in conventional (non-cancellable) biometric systems. However, RNNs' unique capacity to record temporal dynamics makes them attractive options for feature learning in future cancellable biometric applications. Given their proven efficacy in related domains, such as dynamic biometric traits in authentication and identity verification tasks, RNNs may provide useful solutions as cancellable biometrics research progresses.

An ECG identification system for personal authentication using deep recurrent neural networks based on Long Short-Term Memory (LSTM) is proposed in the study [69]. In order to capture the sequential patterns that are specific to each individual, the methodology focusses on utilising the temporal dependencies present in ECG signals by utilising LSTM architectures. To improve classification accuracy, preprocessing methods like R peak seg-

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

mentation are used on the ECG data. Their model balances same and different individual samples through a pairing strategy that employs the Adam optimiser for training and binary cross-entropy as the loss function. The system is robust for biometric authentication applications because of this preprocessing and LSTM modelling, which greatly enhances the system's capacity to distinguish between people based on their ECG patterns. The proposed LSTM-based approach outperforms other modern models like CNN-LSTM, LSTM, and Bi-LSTM, achieving average authentication accuracies of 92.1% and 95.3%, respectively, according to experimental results on benchmark datasets like ECG-ID and PTB. To guarantee the reliability of the results, the authors used five-fold cross-validation, noting a small degree of variability brought on by sample pairing randomness. The study demonstrates how their method is a state-of-the-art approach in ECG-based biometric authentication with promising practical applicability, handling imbalanced datasets and maintaining robust feature extraction through LSTM and CNN integration. These findings underscore the potential of LSTM networks in capturing distinctive temporal biometric features for secure personal identification, setting a benchmark for future research in ECG-based biometrics.

5.2.1.2 Unsupervised machine/deep learning approaches

In unsupervised learning, algorithms examine unlabelled datasets to find underlying patterns, structures, or relationships on their own without human oversight or predetermined labels. Without specific direction, these algorithms analyse unprocessed data to group, cluster, or transform information according to innate similarities and differences, allowing for the meaningful discovery of insights. Unsupervised techniques can uncover hidden features that are helpful for subsequent analysis or downstream tasks thanks to this self-directed learning process. Unsupervised learning works exclusively with input data, which makes it particularly useful for intricate tasks like clustering, dimensionality reduction, and anomaly detection. In contrast, supervised learning uses labelled input-output pairs to train predictive models. Although these algorithms are very good at revealing previously unidentified data features, they typically need to be interpreted by experts to confirm the found structures and guarantee their applicability to particular uses. As a result, by obtaining informative representations from sizable, unlabelled datasets, unsupervised learning is essential to exploratory data analysis and feature engineering.

Generative adversarial networks

A comprehensive and perceptive review of Generative Adversarial Networks (GANs), a subclass of deep learning frameworks created especially for generative modelling tasks, is provided in [73]. The basic process of GANs is the interaction of two neural networks: the

5.2 Learning based biometric template protection

discriminator, which separates generated and real data, and the generator, which combines data samples to mimic real data. The generator is forced to iteratively improve its output in order to produce data that is more and more similar to real-world examples through this adversarial training process, which is envisioned as a minimax game. The study thoroughly examines a number of noteworthy GAN variants, including conditional GANs, deep convolutional GANs (DCGANs), and Wasserstein GANs, explaining how these advancements address common issues like mode collapse and training instability to improve performance and wider applicability across a range of domains. significant progress made by GANs in producing diverse and high-fidelity data, particularly in the fields of data augmentation, video prediction, and image synthesis. The authors explain how, in contrast to more conventional generative techniques like Restricted Boltzmann Machines or Variational Autoencoders, the adversarial framework specifically allows GANs to model complex data distributions more successfully. Additionally covered in the paper are particular evaluation metrics that are appropriate for GANs, such as the Fréchet Inception Distance and the Inception Score, which quantitatively evaluate the variety and realism of generated samples. Unsupervised representation learning, semi-supervised classification, and domain adaptation are just a few of the many uses for GANs that have grown beyond their original application in image generation. Because of their adaptability, GANs are a prominent and expanding tool in modern machine learning research, with significant theoretical and practical implications.

Two novel multi-instance cancellable biometric schemes that make use of iris traits for improved privacy protection are presented in [74]. These methods ensure safe and reversible biometric authentication by using generative adversarial networks (GANs) to create cancellable biometric templates. The first scheme emphasises intra-class uniqueness while successfully differentiating weak inter-class variations by employing a ResNet101 backbone network to capture subtle, discriminative features from the pupil region. The second plan uses style transfer techniques to turn iris photos into new, editable templates that are simple to remove or modify, protecting biometric information from intrusion. Both techniques aim to create revocable and non-invertible biometrics without sacrificing recognition precision. These GAN-based cancellable biometric schemes' efficacy is confirmed by the experimental results, which show strong privacy preservation and high recognition accuracy. The generated cancellable templates demonstrate essential security features like non-invertibility and unlinkability, as well as resilience against possible attacks. The suggested methods' dependability and security are confirmed by the quantitative analyses, which show a high degree of similarity between the original and modified templates and low error rates in biometric recognition tasks. As a result, these schemes balance the dual goals of biometric

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

security and recognition performance in privacy-sensitive applications, providing workable solutions for actual iris biometric systems.

Principal component analysis

The paper [75] presents a new face recognition technique based on principal component analysis that uses a two-dimensional approach. Face images are projected into a specific "face space" made of eigenfaces—the principal components obtained from a representative set of training images—as part of the methodology. Each face can be represented as a linear combination of these basis images thanks to these eigenfaces, which capture the fundamental differences between various faces. While keeping the most discriminative features required for recognition, this transformation drastically lowers the dimensionality of the data. The system carries out effective and reliable face identification by comparing the eigenface coefficients of unknown faces to those of known people. This enables the dynamic addition of new faces without imposing a significant computational load. The authors' results show that their eigenface-based recognition system strikes a convincing balance between simplicity, speed, and accuracy. With reported recognition accuracies of around 85% on sample datasets, the method tracks and recognises faces robustly in limited environments while operating in near real-time. The technique's effectiveness is ascribed to its ability to depict faces holistically as opposed to depending solely on discrete features, thereby tolerating moderate variations in lighting and expression. Overall, the study demonstrates the eigenface technique as a computationally efficient and successful face recognition framework that combines mathematical rigour with physiological insight, significantly advancing the domains of cognitive neuroscience and computer vision.

[76] presents novel approaches to cancelable biometric recognition, namely Random Permutation Principal Component Analysis (RP-PCA) and Random Permutation Two-Dimensional Principal Component Analysis (RP-2DPCA). By creating revocable templates that secure user identity by incorporating a user-specific key, or PIN, these techniques aim to protect biometric data. The approaches transform biometric inputs via random permutations combined with PCA, creating irreversible and secure templates without the necessity for image registration. This leads to a simplified, computationally effective recognition procedure that can be used with datasets of faces, iris, and ears, among other biometric modalities. Their experimental results show that both RP-PCA and RP-2DPCA provide strong privacy protection while achieving recognition accuracy on par with or better than state-of-the-art techniques. Even when the biometric templates are purposefully obscured for security, the suggested random permutation framework successfully preserves the discriminative power of biometric features, enabling trustworthy identity verification. These strategies are demon-

5.2 Learning based biometric template protection

strated as workable solutions for realistic biometric systems where template revocability and user data security are critical, as the results validate the trade-off between system performance and template cancelability. By incorporating security considerations without sacrificing precision or effectiveness, this contribution advances the field of biometric recognition. A new approach for the representation and recognition of faces based on appearance is presented [77] and is called Two-Dimensional Principal Component Analysis (2DPCA). In contrast to conventional PCA, which necessitates converting two-dimensional image matrices into one-dimensional vectors, 2DPCA works directly with image matrices, maintaining the spatial relationships in the original data. With this method, eigenvectors are obtained to act as representative features by directly constructing an image covariance matrix from these matrices without vectorisation. Compared to traditional PCA, this matrix-based method improves efficiency while also streamlining the computational process. A nearest-neighbor classifier is then used to perform face recognition by calculating the Euclidean distances between the feature matrices taken from various face images. Extensive tests on three well-known face databases (ORL, AR, and Yale) show that 2DPCA consistently outperforms conventional PCA in terms of recognition accuracy. Furthermore, 2DPCA avoids the singularity issues commonly seen in PCA by working on a smaller covariance matrix, guaranteeing more stable and dependable computation. The method is suitable for real-world applications that require accuracy and efficiency in face recognition tasks because it not only improves accuracy but also drastically cuts down on computational time. These findings highlight 2DPCA's value as a successful and computationally beneficial method in the field of appearance-based face recognition.

K-means clustering

In order to effectively divide a dataset of M points in an N -dimensional space into K clusters while meeting the criterion of minimising the within-cluster sum of squares, [78] study presents an advanced k-means clustering algorithm. Their method uses a point relocation strategy, which differs from traditional iterative k-means approaches in that individual data points are moved from one cluster to another if doing so lowers the overall within-cluster variance. In order to reach a locally optimal clustering configuration, this iterative process assesses the possible improvement in the objective function upon moving each point and continues reassignments until no more reduction is possible. In multidimensional clustering contexts, the algorithm balances computational efficiency with robust convergence characteristics by starting with predefined cluster centres and making assignment decisions based on Euclidean distance metrics. Hartigan and Wong show that their algorithm outperforms earlier k-means approaches in terms of convergence speed and solution quality. According to

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

their empirical assessments, the relocation technique successfully finds cluster configurations with lower within-cluster sum of squares, demonstrating better optimisation results. The algorithm's computational benefits for large-scale clustering problems are further demonstrated by the fact that it takes fewer iterations to reach convergence. As a major addition to the toolkit for statistical cluster analysis, the authors highlight the method's practical applicability and robustness across a range of dataset sizes and dimensions. Thus, this work has contributed a computationally viable and methodologically sound approach to k-means clustering, which has been widely used in further studies and applications.

An advanced biometric template protection scheme created especially for palmprint recognition systems is introduced [79]. By using non-invertible transformations on palmprint features, this method successfully secures palmprint templates by combining cancelable biometrics with bio-cryptography. The method maintains recognition accuracy while guaranteeing the stored templates' revocability and unlinkability. By combining these strategies, it effectively protects biometric information against reconstruction and correlation attacks, greatly improving user security and privacy. Additionally, the system addresses important biometric security concerns by supporting template replacement in the event of compromise. According to the findings, the authors⁷ show that their suggested method improves security features like irreversibility and unlinkability while achieving a noteworthy recognition accuracy. The system's resistance to numerous known biometric template attacks is confirmed by thorough experimental assessments. Furthermore, the scheme demonstrates computational efficiency, confirming its appropriateness for realistic implementation in real-world situations. Overall, the results show that the suggested approach effectively strikes a balance between high recognition performance and strict security requirements, marking a significant advancement in the field of palmprint biometric systems.

Convolutional autoencoder

In order to detect sarcopenia from multi-frame ultrasound image slices, [80] present a novel framework that combines an autoencoder with a convolutional neural network (CNN). Through the extraction of salient features and the reduction of noise in each frame, the autoencoder component compresses the high-dimensional ultrasound data. The subsequent CNN classifier, which examines the compressed multi-frame data for precise sarcopenia classification, can process the data more quickly and effectively thanks to this dimensionality reduction. The framework demonstrates its usefulness in clinical ultrasound imaging contexts by leveraging the multi-frame nature of ultrasound data to achieve enhanced detection performance and noise resilience. The paper's results show that this autoencoder-CNN combination approach outperforms conventional detection techniques in terms of accuracy and robustness.

The framework makes the best use of multi-frame ultrasound data to improve sarcopenia classification by addressing noise filtering and dimensionality reduction simultaneously. The framework's efficacy has been empirically evaluated on patient ultrasound data, establishing it as a promising tool for ultrasound-based muscle health assessment and emphasising its potential contributions to clinical diagnostics and future medical image analysis research projects.

With an emphasis on facial recognition, the paper [81] presents a novel technique for creating cancelable biometric templates. Their approach utilizes a convolutional autoencoder to extract and encode salient facial features into a compact representation. A network called RandNet then processes this representation, adding randomised transformations to improve template security. By ensuring that reconstructing the original biometric information is computationally impossible even in the case of template compromise, this design greatly enhances user privacy and protects biometric systems from inversion attacks. According to the study's experimental results, the suggested framework effectively strikes a balance between preserving a high level of recognition accuracy and bolstering security. Experiments on well-known facial recognition datasets demonstrate that the convolutional autoencoder's integration with RandNet significantly improves security metrics like Diversity and Non-invertibility while maintaining strong verification performance. This method offers better accuracy and resilience than current cancelable biometric template generation techniques, highlighting its usefulness for improving privacy in biometric authentication systems.

5.3 Methodology

The convolutional autoencoder's operation is covered together with the theoretical underpinnings of the convolutional neural network in this part.

The performance of convolutional neural networks in the area of image categorization has been astounding. Deep learning models can produce predictions that are unstable and unreliable due to the noise and redundant data included in the high-dimensional input images. Unsupervised dimensionality reduction methods called convolutional autoencoders are capable of producing compressed image representations since they are made up of convolutional layers. It has been proven to provide robust and stable feature representations by filtering out noise and redundant data. The significant and most practical features have been extracted from the images using the convolutional autoencoder and represented in a latent space.

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

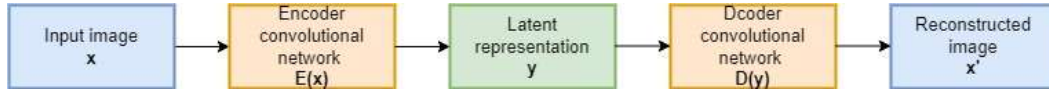


FIGURE 5.1 Convolutional autoencoder model [1]

As shown in figure 5.1, the encoder and decoder CNN models make up the convolutional autoencoder. The encoder's primary function is to convert the initial input image into a latent space with reduced dimensionality. Contrarily, the decoder is in charge of reassembling the compressed latent space and generating an image that is as similar to the original as possible. The loss function measures how much information is lost when comparing the compressed and uncompressed versions of the same data.

The initial input image x is denoted mathematically by $x = X^{M \times H \times W \times 3}$, where M is the number of samples and H and W are the number of pixels that correspond to each image X 's height and width. The encoded representation is denoted by $y = X^{M \times h \times w \times 3}$. Thus, for the compressed spatial 2D form [82]. The reconstruction uses decoding $x' = X^{M \times H \times W \times 3}$. The encoder produces $y = E(x)$, and the decoder produces $x' = D(y)$.

The usage of the internet and other handheld smart devices promotes the theft of users' biometric traits, which frequently results in a loss of privacy. Protecting biometric template data is essential to prevent loss of user privacy and identification. An effective and efficient approach is required that focuses on the security and privacy concerns associated with biometric traits. To cope with this issue, we propose a convolutional autoencoder and a winner-take-all hashing-based cancelable biometric template. For each image, the latent-space vector representation is computed, and the features are extracted using the convolutional autoencoder. The generated biometric feature vector is further enhanced with random noise to increase the discriminative power and enable the revocability of biometric templates. When computing similarity, winner-take-all hashing is used to determine the relevant features and effectively ignores the rest of the information. The performance of the suggested approach is evaluated using the fingerprint data sets FVC2002-DB1 and DB2. The results of the experiments and the security analysis support the effectiveness of the suggested approach.

The raw biometric data that traditional biometric systems store is susceptible to attacks, which can result in unauthorized access or identity theft. This risk is reduced by cancelable biometrics, which converts the original biometric data into non-reversible variants that permit replacement and revocation without compromising the original biometric data. A convolutional autoencoder is used to obtain features from the biometric image. The resultant feature vector is given some random noise, and then a winner-take-all hashing is applied to produce the cancelable template. The final cancelable template is obtained by median filtering.

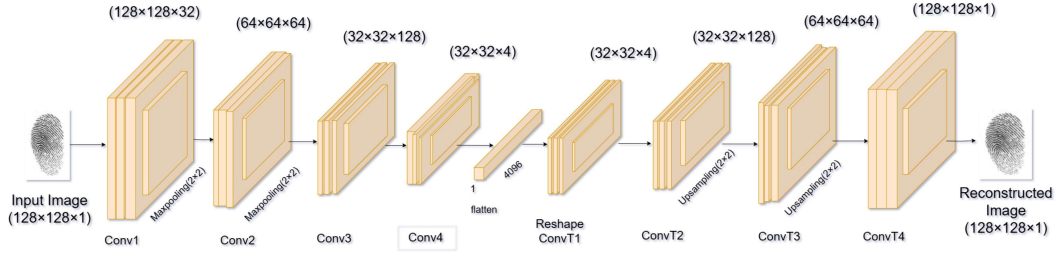


FIGURE 5.2 Fingerprint Convolutional Autoencoder Architecture

This approach leverages the feature extraction capabilities of convolutional autoencoders to create a latent space representation of biometric images that is then transformed into a cancelable template.

5.3.1 Architecture and training

Figure 5.2 depicts the architecture of the convolutional autoencoder. The convolutional autoencoder is constructed using Conv2D layers in the encoder and Conv2D transpose layers in the decoder to train a convolutional autoencoder using two CNNs. First, a convolutional layer-based encoder is employed to get the features from the source image before compressing it. With the help of transposed convolution layers, the second is a decoder that reconstructs the image from the features extracted. Python and TensorFlow are both used to implement this network. The fingerprint biometric image ($224 \times 224 \times 1$) is resized to $M \times N$ ($128 \times 128 \times 1$) as needed. After that, the image is normalized in the range of (0, 1) to create the input image, which is then prepared for input to the convolutional autoencoder. LeakyReLU and the batch normalization layer come after each block of convolution and transposed convolution. The $128 \times 128 \times 1$ input image is passed through a filter to produce a feature map in the convolution blocks. The 7×7 filter is present in each of the first convolution layers in the convolution blocks conv1, conv2, conv3, and conv4. The same is true for the transposed convolution blocks convT1, convT2, convT3, and convT4.

The FVC2002 DB1 and DB2 are used to train the network. For 300 epochs, the convolutional autoencoder is trained. The loss function used is mean squared error, and the optimizer is RMSprop with default values and a random seed value. Figure 5.4 displays the loss for the training and the validation.

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

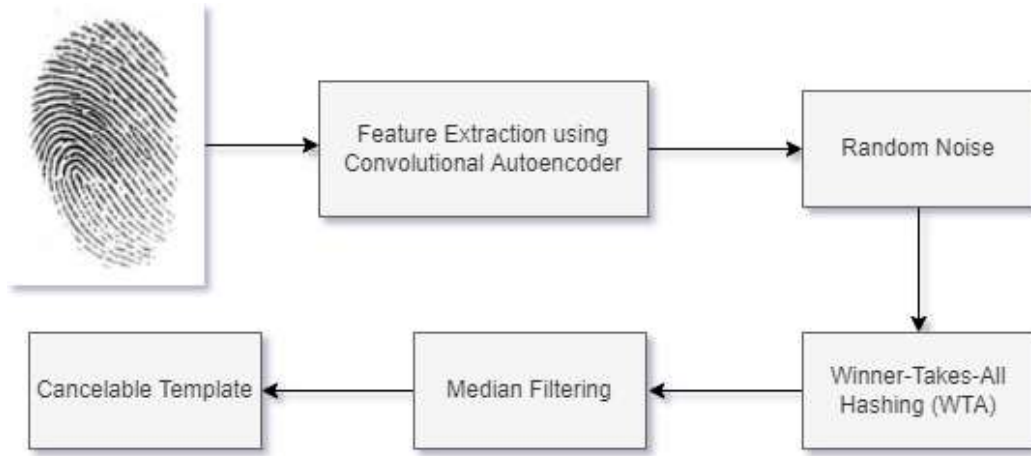


FIGURE 5.3 The proposed method's block diagram

5.3.2 Cancelable template generation

A convolutional autoencoder is used to obtain features of the biometric image of the source fingerprint, as illustrated in Figure 5.3. The resultant feature vector is given some random noise, and then a winner-take-all hashing is applied to produce the cancelable template. In winner-take-all hashing, a set of m random permutations θ is applied to the extracted feature vector, and then the first k features are selected, and the index of the highest k value is identified, as shown in the algorithm below. The final cancelable template is obtained by median filtering.

The winner-take-all hashing is a nonlinear transformation that bases its results on the implicit order of the input data rather than its absolute or numerical values. As a result, it demonstrates considerable resistance to numerical disturbance while giving a definite indicator of the fundamental resemblance of the examined items. Due to its success in facilitating quick similarity searches, Google uses the cutting-edge winner-takes-all hashing algorithm. Based on the number of permutations, the approach can produce a variety of sequences. After applying random permutations, it uses the rank of association measurements and logs the index of the biometric feature with the highest value, as shown in table 5.1.

Algorithm 1: Winner-take-all hashing algorithm

Require: vector X , A set of m Permutations θ , window size y

Ensure: Hash Code

- 1: Generate a permutation set θ for each hash function m based on g random permutation. θ_i in Θ .
 - 2: For each permutation θ_i in Θ ,
 - 3: (i) Permute elements of X according to θ_i to X'
 - 4: (ii) Initialize the i^{th} hash code $c_i = 0$.
 - 5: (iii) Set c_i to the index of the maximum value in $X'(1...y)$
 - 6: For $j = 1 \rightarrow y$
 - 7: If $z(j) \geq z(c_i)$ then $c_i = j$;
 - 8: $c = \{c_i \in [1, y] \mid i = 1, \dots, m\}$, each hash code in c of length m accepts a value between 0 and $y - 1$. $=0$
-

TABLE 5.1 Winner-take-all hashing Hashing Example with three input vectors x_1, x_2, x_3 , window size K and one permutation θ . x_1 and x_2 are unrelated and result in different output codes, each element in x_3 has been perturbed by 1, which changes the ranking of the items but keeps the maximum of the first K elements the same, yielding the same code once more.

Feature	Permuted Feature based on random permutation set $\theta =$ $\{4, 5, 1, 0, 3, 2\}$	Selected feature based on window size $K=4$	Winner- take-all Hashing Hwta(Fx)
$F_{X1} = \{1, 6, 4, 8, 7, 9\}$	$\theta(F_{X1}) = \{7, 9, 6, 1, 8, 4\}$	$F_{S1} = \{7, 9, 6, 1\}$	2
$F_{X2} = \{10, 3, 9, 2, 5, 4\}$	$\theta(F_{X2}) = \{9, 3, 2, 4, 10, 5\}$	$F_{S2} = \{9, 3, 2, 4\}$	1
$F_{X3} = \{2, 7, 4, 9, 8, 10\}$	$\theta(F_{X3}) = \{8, 10, 7, 2, 9, 4\}$	$F_{S3} = \{8, 10, 7, 2\}$	2

5.4 Experiment and analysis

The qualitative results of the proposed approach on various datasets are shown in this section. The suggested methodology is thoroughly compared with a number of state-of-the-art methods that are also offered. The FVC2002 DB1 and DB2 public fingerprint datasets were used for the experiments, as shown in Table 5.2. 100 users and 8 samples per user make up each dataset. Each dataset has 800 fingerprint images altogether. The false acceptance rate, false reject rate, genuine acceptance rate, and receiver operating characteristic curves are used to assess the accuracy performance.

Figure 5.4 illustrates the synchrony between the validation and training losses. It demonstrates that the model is not overfit. The validation loss is decreasing and not increasing. The

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

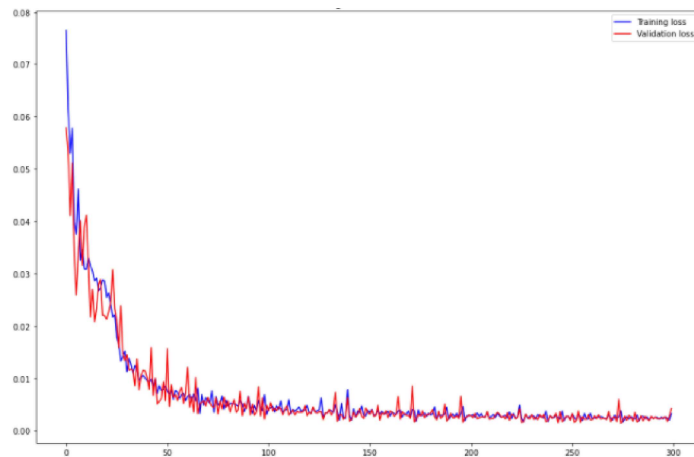


FIGURE 5.4 Training and validation loss of convolution autoencoder

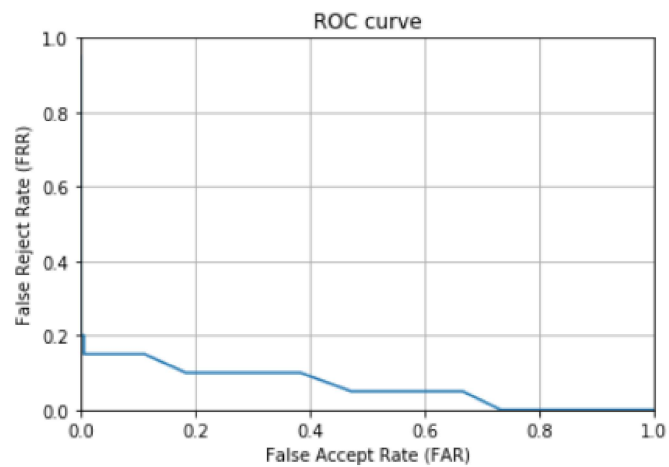
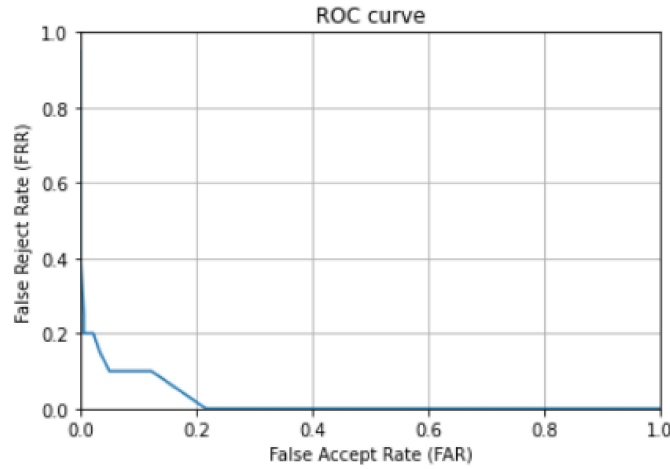


FIGURE 5.5 ROC plots for the proposed technique on different datasets—Equal Error Rate (EER%): 0.1306 - FVC2002 DB1

TABLE 5.2 Specification of the experimental datasets

Dataset Name	Modality	Users	Samples	Resolution	Sensor type	Quality
FVC2002 DB1	Fingerprint	100	8	500 dpi	Optical	Medium
FVC2002 DB2	Fingerprint	100	8	569 dpi	Optical	Medium

**FIGURE 5.6** ROC plots for the proposed technique on different datasets—Equal Error Rate (EER%): 0.0861 - FVC2002 DB2

equal error rates for the FVC2002 DB1 and DB2 datasets are 0.1306 and 0.0861 (EER%), respectively, as illustrated in Table 5.3. Figures 5.5 and 5.6 display the ROC plots for the suggested method on several datasets. In the normal verification scenario, each enrolled user must provide their unique keys during the verification process for any biometric recognition system. The genuine scores and the imposter scores are calculated by matching against the true class and by matching against all other enrolled classes apart from the true class, respectively. Figure 5.7 depicts the genuine-impostor distributions for the FVC2002 DB1 database. An obvious separability between the two distributions indicates that the experiment produced practically ideal results. The interesting finding in this situation was that our system's imposter scores consistently stayed close to zero, leading to incredibly low EER values.

Every cancelable transformation must satisfy the requirement of non-invertibility because the security of the templates depends on it. Once a template has been created, the real fingerprint biometric image cannot be retrieved without the aid of a trained network with predetermined weights. A seed value has been used during the convolutional autoencoder training process. Even if another convolutional autoencoder is trained, it will not be able

Learning based fingerprint template protection using convolutional autoencoder and winner-take-all hashing

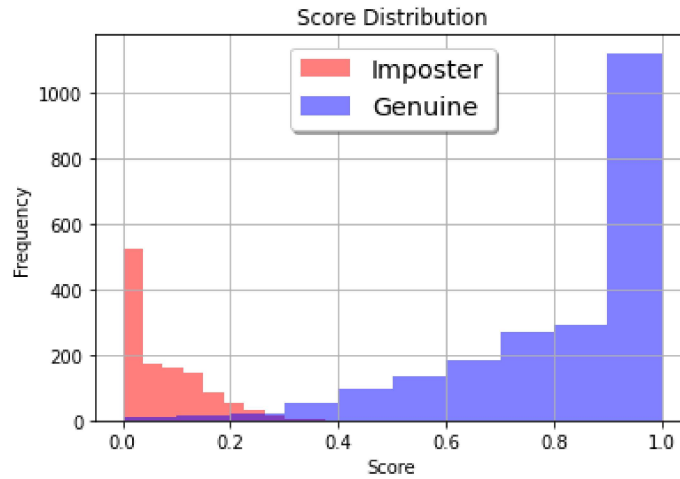


FIGURE 5.7 ROC plot and Genuine-impostor distributions for the proposed technique on FVC2002 dataset

TABLE 5.3 Performance Comparison

Methods	FVC2002-DB1 Dataset-EER(%)	FVC2002-DB2 Dataset-EER(%)
Random Projection-based [83]	4	3
Bloom-filter with fingerprint [84]	2.3	1.8
Huffman encoding and DCT based [39]	1.2	-
A partial hadamard transform [28]	1.15	2
Minimum spanning tree based [29]	1.8	-
Proposed Method with Convolutional Autoencoder and WTA hashing	0.1306	0.0861

to rebuild an exact image from the compromised templates using the same convolutional autoencoder without the seed value. The winner-take-all hashing permutes the extracted feature vectors of the convolutional autoencoder using random permutations, which makes the template non-invertible. The produced template has also undergone non-invertible median filtering. As a result, the templates produced by the proposed work are non-invertible.

Random noise is integrated into the framework to enhance the randomness of the generated template, introducing variability and making it difficult for attackers to reverse-engineer or misuse the original biometric data. The addition of random noise creates variability in the generated templates. Even if two templates are derived from the same biometric input, the

presence of noise ensures that they will not be identical, which provides non-linkability of the templates.

5.5 Summary

The biometric traits are irrevocable, so if they are stolen by an adversary, they cannot be recreated. Therefore, it would be preferable to create a method that provides high-precision biometric trait security and renders templates non-invertible and revocable as and when necessary. Convolutional autoencoding is used in the suggested method for feature extraction, and winner-take-all hashing with median filtering is used for the creation of cancellable biometric templates. The technique demonstrated effectiveness, non-invertibility, and privacy preservation. Despite the single modality approach, research offers a significant contribution to the understanding of cancelable biometrics. As a limitation, we further use the advantages of multi-modal systems, and the research could be expanded by integrating other modalities in future studies.

CHAPTER - 6

Conclusion and Future Work

6.1 Conclusion

The recent scientific literature is examined for understanding the problem of biometric template protection using deep learning models. The literature study identifies and summarizes the numerous ways to deal with the threat to biometric traits and its various possible solutions. Several different approaches with deep learning were studied to get a deeper understanding, and some fundamental methods were put into practice and contrasted.

This research proposed cancelable template generation using the discrete cosine transform, index of maximum hashing, the fast fourier transform, the hadamard product, and speeded-up robust features-based feature extraction in this study. According to theoretical reason and actual evidence, the index of maximum hashed codes can substantially maintain accuracy performance as a rank correlation attribute. The proposed method is also shown to satisfy non-invertibility template protection criteria. The results show that proposed methods outperform other state-of-the-art methods for the protection of biometric templates.

The proposed work uses the discriminative features of the autoencoder model for efficient feature extraction. The biometric traits are irrevocable, so if they are stolen by an adversary, they cannot be recreated. Therefore, it would be preferable to create a method that provides high-precision biometric trait security and renders templates non-invertible and revocable as and when necessary. Convolutional autoencoding is used in the suggested method for feature extraction, and winner-take-all hashing with median filtering is used for the creation of cancellable biometric templates. The technique demonstrated effectiveness, non-invertibility, and privacy preservation. Despite the single modality approach, research offers a significant contribution to the understanding of cancelable biometrics.

The proposed work is trained and tested on the two openly accessible datasets; FVC2002 DB1 and DB2. The results of all proposed approaches are compared with those of other methods available in the literature. Our proposed methods outperform the other state-of-the-art methods of the biometric template protection. This research would help the biometric community handle the privacy-preservation of biometric data.

This research contributes to the biometric research community by providing effective mechanisms to address privacy and security challenges associated with biometric traits. By introducing robust non-invertible and cancelable template protection techniques, the proposed approach enhances resistance to unauthorized reconstruction and misuse of biometric data, thereby supporting the development of secure and privacy-preserving biometric systems.

6.1.1 Future Work

This thesis presents cutting-edge approaches that advance state-of-the-art biometric template protection. The experiments revealed several potential enhancements indicating new areas for further investigation.

- Future research can enhance multi-modal systems by integrating additional biometric modalities, leading to more robust, secure, and versatile systems. The key challenge is effectively combining diverse biometrics to develop comprehensive and reliable feature sets for improved practical applications. Such advancements would enhance the versatility and security of biometric technology.
- Cancelable biometrics use non-invertible transformations on biometric data to allow template revocation and replacement if compromised, similar to resetting a password. The main challenge is designing transformations that ensure security and revocability while maintaining high recognition accuracy despite intra-class variability within biometric data from the same individual.
- The proposed strategy involves integrating encryption, watermarking, and steganography techniques to develop an efficient and secure cancelable biometric recognition system.
- Another challenge is addressing record multiplicity attacks, which occur when intruders attempt to reconstruct the original biometric template by correlating multiple templates across different applications. Effective countermeasures are required to prevent such cross-matching and ensure the security of biometric data.

References

- [1] Anil K Jain, Karthik Nandakumar, and Abhishek Nagar. Biometric template security. *EURASIP Journal on advances in signal processing*, 2008, 2008.
- [2] Anil K Jain, Karthik Nandakumar, and Arun Ross. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79: 80–105, 2016.
- [3] Gayatri U Bokade and Rajendra D Kanphade. A novel approach for secured multimodal biometric authentication based on data fusion technique. *International Journal of Computational Vision and Robotics*, 11(2):214–243, 2021.
- [4] Anand Handa, Rashi Agarwal, and Narendra Kohli. Incremental approach for multi-modal face expression recognition system using deep neural networks. *International journal of computational vision and robotics*, 11(1):1–20, 2021.
- [5] Zhe Jin, Meng-Hui Lim, Andrew Beng Jin Teoh, and Bok-Min Goi. A non-invertible randomized graph-based hamming embedding for generating cancelable fingerprint template. *Pattern Recognition Letters*, 42, 2014.
- [6] Abhishek Nagar, Karthik Nandakumar, and Anil K Jain. Biometric template transformation: a security analysis. In *Media Forensics and Security II*, volume 7541. International Society for Optics and Photonics, 2010.
- [7] Mahesh Joshi, Bodhisatwa Mazumdar, and Somnath Dey. Security vulnerabilities against fingerprint biometric system. *arXiv preprint arXiv:1805.07116*, 2018.
- [8] Elena Pagnin and Aikaterini Mitrokotsa. Privacy-preserving biometric authentication: challenges and directions. *Security and Communication Networks*, 2017, 2017.
- [9] Karthik Nandakumar and Anil K Jain. Multibiometric template security using fuzzy vault. In *2008 IEEE Second International Conference on Biometrics: Theory, Applications and Systems*, pages 1–6. IEEE, 2008.
- [10] B. Choudhury, P. Then, V. Raman, B. Issac, and M. K. Haldar. Cancelable iris biometrics based on data hiding schemes. *2016 IEEE Student Conference on Research and Development (SCOREd)*, pages 1–6, 2016.
- [11] Ayesha S. Shaikh and Vibha D. Patel. Significance of the transition to biometric template protection: Explore the future. *International Journal of Image and Graphics*, 21(02):2150025, 2021. doi: 10.1142/S021946782150025X.

- [12] Nalini K Ratha, Sharat Chikkerur, Jonathan H Connell, and Ruud M Bolle. Generating cancelable fingerprint templates. *IEEE Transactions on pattern analysis and machine intelligence*, 29, 2007.
- [13] Davide Maltoni, Dario Maio, Anil K Jain, and Salil Prabhakar. *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.
- [14] Christian Rathgeb, Frank Breiting, Christoph Busch, and Harald Baier. On application of bloom filters to iris biometrics. *IET Biometrics*, 2014.
- [15] Anil K Jain, Karthik Nandakumar, and Abhishek Nagar. Fingerprint template protection: From theory to practice. In *Security and privacy in Biometrics*. Springer, 2013.
- [16] Alamgir Sardar, Saiyed Umer, Chiara Pero, Michele Nappi, et al. A novel cancelable facehashing technique based on non-invertible transformation with encryption and decryption template. *IEEE Access*, 8(105263105277), 2020.
- [17] Mulagala Sandhya and Munaga VNK Prasad. k-nearest neighborhood structure (k-nns) based alignment-free method for fingerprint template protection. In *Biometrics (ICB), 2015 International Conference on*. IEEE, 2015.
- [18] Harkeerat Kaur and Pritee Khanna. Gaussian random projection based non-invertible cancelable biometric templates. *Procedia Computer Science*, 54, 2015.
- [19] Limei Guo, Yun Mao, and Ying Guo. Non-invertible fingerprint template protection with polar transformations. In *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*. IEEE, 2016.
- [20] Kenta Takahashi and Shinji Hirata. Cancelable biometrics with provable security and its application to fingerprint verification. *IEICE Transactions*, 94-A:233–244, 2011.
- [21] Wencheng Yang, Jiankun Hu, Song Wang, and Qianhong Wu. Biometrics based privacy-preserving authentication and mobile template protection. *Wireless Communications and Mobile Computing*, 2018, 2018.
- [22] Zhe Jin, Andrew Teoh, Thian Song Ong, and Tee Connie. A revocable fingerprint template for security and privacy preserving. *TIIS*, 4:1327–1342, 12 2010. doi: 10.3837/tiis.2010.12.020.
- [23] Karthik Nandakumar. A fingerprint cryptosystem based on minutiae phase spectrum. In *2010 IEEE International Workshop on Information Forensics and Security*, pages 1–6. IEEE, 2010.
- [24] Zhe Jin, Andrew Beng Jin Teoh, Thian Song Ong, and Connie Tee. Fingerprint template protection with minutiae-based bit-string for security and privacy preserving. *Expert systems with applications*, 39, 2012.
- [25] Rudresh Dwivedi and Somnath Dey. A non-invertible cancelable fingerprint template generation based on ridge feature transformation. *arXiv preprint arXiv:1805.10853*, 2018.

References

- [26] Xingbo Dong, Soohyung Kim, Zhe Jin, Jung Yeon Hwang, Sangrae Cho, and Andrew Beng Jin Teoh. Open-set face identification with index-of-max hashing by learning. *Pattern Recognition*, 103:107277, 2020.
- [27] Zhe Jin, Jung Yeon Hwang, Yen-Lung Lai, Soohyung Kim, and Andrew Beng Jin Teoh. Ranking-based locality sensitive hashing-enabled cancelable biometrics: Index-of-max hashing. *IEEE Transactions on Information Forensics and Security*, 13(2):393–407, 2017.
- [28] Song Wang, Guang Deng, and Jiankun Hu. A partial hadamard transform approach to the design of cancelable fingerprint templates containing binary biometric representations. *Pattern Recognition*, 61, 2017.
- [29] Munaga VNK Prasad, P Swathi, C Raghavendra Rao, and BL Deekshatulu. Minimum spanning tree (mst) based techniques for generation of cancelable fingerprint templates. *International Journal of Pattern Recognition and Artificial Intelligence*, 28(06):1456013, 2014.
- [30] Takao Murakami, Tetsushi Ohki, Yosuke Kaga, Masakazu Fujio, and Kenta Takahashi. Cancelable indexing based on low-rank approximation of correlation-invariant random filtering for fast and secure biometric identification. *Pattern Recognition Letters*, 2018.
- [31] Chulhan Lee and Jaihie Kim. Cancelable fingerprint templates using minutiae-based bit-strings. *Journal of network and computer applications*, 33, 2010.
- [32] Priyanka Das, Kannan Karthik, and Boul Chandra Garai. A robust alignment-free fingerprint hashing algorithm based on minimum distance graphs. *Pattern Recognition*, 45, 2012.
- [33] Tohari Ahmad, Jiankun Hu, and Song Wang. Pair-polar coordinate-based cancelable fingerprint templates. *Pattern Recognition*, 44, 2011.
- [34] Zhe Jin, Andrew Beng Jin Teoh, Bok-Min Goi, and Yong-Haur Tay. Biometric cryptosystems: a new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognition*, 56:50–62, 2016.
- [35] Ann Cavoukian and Alex Stoianov. Biometric encryption. In *Encyclopedia of cryptography and security*, pages 90–98. Springer, 2011.
- [36] Ari Juels and Martin Wattenberg. A fuzzy commitment scheme. In *Proceedings of the 6th ACM conference on Computer and communications security*, pages 28–36, 1999.
- [37] A Juels and M Sudan. A fuzzy vault scheme. in proc. ieee int. In *Symp. Inf. Theory, Switzerland*, volume 408, 2002.
- [38] Abhishek Nagar, Karthik Nandakumar, and Anil K Jain. Securing fingerprint template: Fuzzy vault with minutiae descriptors. In *2008 19th International conference on pattern recognition*, pages 1–4. IEEE, 2008.
- [39] Bismita Choudhury, Patrick Then, Biju Issac, Valliappan Raman, and Manas Kumar Haldar. A survey on biometrics and cancelable biometrics systems. *International Journal of Image and Graphics*, 18, 2018.

- [40] Anil K Jain and Karthik Nandakumar. Biometric authentication: System security and user privacy. *IEEE Computer*, 45, 2012.
- [41] Andrew BJ Teoh, Yip Wai Kuan, and Sangyoun Lee. Cancellable biometrics and annotations on biohash. *Pattern recognition*, 41(6):2034–2044, 2008.
- [42] Patrick Lacharme and Aude Plateaux. Pin-based cancelable biometrics. *International Journal of Automated Identification Technology (IJAiT)*, 3(2):75–79, 2011.
- [43] Andrew Teoh Beng Jin, David Ngo Chek Ling, and Alwyn Goh. Biohashing: two factor authentication featuring fingerprint data and tokenised random number. *Pattern recognition*, 37(11):2245–2255, 2004.
- [44] Lovelesh Khard, Raju Baraskar, and Uday Chaurasia. Survey on fingerprint recognition system using image preprocessing and de-noising. *International Journal of Computer Applications*, 155(4), 2016.
- [45] Lin Hong, Yifei Wan, and Anil Jain. Fingerprint image enhancement: algorithm and performance evaluation. *IEEE transactions on pattern analysis and machine intelligence*, 20(8):777–789, 1998.
- [46] P Pakutharivu and MV Srinath. A comprehensive survey on fingerprint recognition systems. *Indian Journal of Science and Technology*, 8(35):1, 2015.
- [47] Miao-li Wen, Yan Liang, Quan Pan, and Hong-cai Zhang. A gabor filter based fingerprint enhancement algorithm in wavelet domain. In *IEEE International Symposium on Communications and Information Technology, 2005. ISCIT 2005.*, volume 2, pages 1468–1471. IEEE, 2005.
- [48] Haroon Shams, Tariqullah Jan, Amjad Ali Khalil, Naveed Ahmad, Abid Munir, and Ruhul Amin Khalil. Fingerprint image enhancement using multiple filters. *PeerJ Computer Science*, 9:e1183, 2023.
- [49] Vishal M Patel, Nalini K Ratha, and Rama Chellappa. Cancelable biometrics: A review. *IEEE signal processing magazine*, 32(5):54–65, 2015.
- [50] Abeer D Algarni, Ghada El Banby, Sahar Ismail, Walid El-Shafai, Fathi E Abd El-Samie, and Naglaa F. Soliman. Discrete transforms and matrix rotation based cancelable face and fingerprint recognition for biometric security applications. *Entropy*, 22(12): 1361, 2020.
- [51] Fatma G Hashad, O Zahran, S El-Rabaie, Ibrahim F Elashry, Ghada Elbanby, Moawad I Dessouky, and Fathi E Abd El-Samie. Cancelable fingerprint recognition based on encrypted convolution kernel in different domains. *Menoufia Journal of Electronic Engineering Research*, 29(2):133–142, 2020.
- [52] Debanjan Sadhya, Zahid Akhtar, and Dipankar Dasgupta. A locality sensitive hashing based approach for generating cancelable fingerprints templates. In *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–9. IEEE, 2019.

References

- [53] Amit Kumar Trivedi, Dalton Meitei Thounaojam, and Shyamosree Pal. Non-invertible cancellable fingerprint template for fingerprint biometric. *Computers & Security*, 90: 101690, 2020.
- [54] Yubing Jiang, Peisong Shen, Li Zeng, Xiaojie Zhu, Di Jiang, and Chi Chen. Cancelable biometric schemes for euclidean metric and cosine metric. *Cybersecurity*, 6(1):4, 2023.
- [55] Xing-Bo Dong, Zhe Jin, and KokSheik Wong. A generalized approach for cancellable template and its realization for minutia cylinder-code. In *2018 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, pages 908–915. IEEE, 2018.
- [56] Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng, and Craig Valli. A fingerprint and finger-vein based cancelable multi-biometric system. *Pattern Recognition*, 78: 242–251, 2018.
- [57] Sanghoon Lee and Ik Rae Jeong. On the unlinkability of fingerprint shell. *Security and Communication Networks*, 2020, 2020.
- [58] Karthik Nandakumar and Anil K Jain. Biometric template protection: Bridging the performance gap between theory and practice. *IEEE Signal Processing Magazine*, 32, 2015.
- [59] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14, 2004.
- [60] Rudresh Dwivedi and Somnath Dey. Score-level fusion for cancelable multi-biometric verification. *Pattern Recognition Letters*, 2018.
- [61] Subrahmanyam Murala, RP Maheshwari, and R Balasubramanian. A relevance feedback-based learner for image retrieval using sift descriptors. *International Journal of Computational Vision and Robotics*, 2(2):99–114, 2011.
- [62] H Kavitha and MV Sudhamani. Experimental analysis of sift and surf features for multi-object image retrieval. *International Journal of Computational Vision and Robotics*, 7(3):344–356, 2017.
- [63] Umma Hany and Lutfu Akter. Speeded-up robust feature extraction and matching for fingerprint recognition. In *2015 International Conference on Electrical Engineering and Information Communication Technology (ICEEICT)*, pages 1–7. IEEE, 2015.
- [64] Takao Murakami, Tetsushi Ohki, Yosuke Kaga, Masakazu Fujio, and Kenta Takahashi. Cancelable indexing based on low-rank approximation of correlation-invariant random filtering for fast and secure biometric identification. *Pattern Recognition Letters*, 126: 11–20, 2019.
- [65] Song Wang and Jiankun Hu. Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (ditom) approach. *Pattern recognition*, 45(12): 4129–4137, 2012.

- [66] ABJ Teoh and DCL Ngo. Cancellable biometrics realization through biophasoring. In *Proceedings of 9th IEEE international conference on control, automation, robotics and vision (ICARCV'06)*, 2006.
- [67] Ian Goodfellow. Deep learning, 2016.
- [68] Young Kyun Jang and Nam Ik Cho. Deep face image retrieval for cancelable biometric authentication. In *2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, pages 1–8. IEEE, 2019.
- [69] Beom-Hun Kim and Jae-Young Pyun. Ecg identification for personal authentication using lstm-based deep recurrent neural networks. *Sensors*, 20(11):3069, 2020.
- [70] Essam Abdellatef, Nabil A Ismail, Salah Eldin SE Abd Elrahman, Khalid N Ismail, Mohamed Rihan, and Fathi E Abd El-Samie. Cancelable multi-biometric recognition system based on deep learning. *The Visual Computer*, 36(6):1097–1109, 2020.
- [71] Mohammadreza Kaji, Jamshid Parvizian, and Hans Wernher van de Venn. Constructing a reliable health indicator for bearings using convolutional autoencoder and continuous wavelet transform. *Applied Sciences*, 10(24):8948, 2020.
- [72] P Punithavathi and S Geetha. Random permutation-based linear discriminant analysis for cancelable biometric recognition. In *Advances in Computing and Network Communications: Proceedings of CoCoNet 2020, Volume 1*, pages 593–603. Springer, 2021.
- [73] Antonia Creswell, Tom White, Vincent Dumoulin, Kai Arulkumaran, Biswa Sengupta, and Anil A Bharath. Generative adversarial networks: An overview. *IEEE signal processing magazine*, 35(1):53–65, 2018.
- [74] Mayada Tarek, Eslam Hamouda, and Abdelaziz Said Abohamama. Multi-instance cancellable biometrics schemes based on generative adversarial network. *Applied Intelligence*, 52(1):501–513, 2022.
- [75] Vytautas Perlibakas. Distance measures for pca-based face recognition. *Pattern recognition letters*, 25(6):711–724, 2004.
- [76] Nitin Kumar, Surendra Singh, and Abhimanyu Kumar. Random permutation principal component analysis for cancelable biometric recognition. *Applied Intelligence*, 48(9): 2824–2836, 2018.
- [77] Jian Yang, David Zhang, Alejandro F Frangi, and Jing-yu Yang. Two-dimensional pca: a new approach to appearance-based face representation and recognition. *IEEE transactions on pattern analysis and machine intelligence*, 26(1):131–137, 2004.
- [78] John A Hartigan and Manchek A Wong. Algorithm as 136: A k-means clustering algorithm. *Journal of the royal statistical society. series c (applied statistics)*, 28(1): 100–108, 1979.
- [79] Alamgir Sardar, Saiyed Umer, Ranjeet Kumar Rout, and Muhammad Khurram Khan. A secure and efficient biometric template protection scheme for palmprint recognition system. *IEEE Transactions on Artificial Intelligence*, 4(5):1051–1063, 2022.

References

- [80] Emmanuel Pintelas, Ioannis E Livieris, Nikolaos Barotsis, George Panayiotakis, and Panagiotis Pintelas. An autoencoder convolutional neural network framework for sarcopenia detection based on multi-frame ultrasound image slices. In *IFIP International Conference on Artificial Intelligence Applications and Innovations*, pages 209–219. Springer, 2021.
- [81] Pankaj Bamoriya, Gourav Siddhad, Pritee Khanna, and Aparajita Ojha. Cancelable template generation using convolutional autoencoder and randnet. In *International Conference on Computer Vision and Image Processing*, pages 363–374. Springer, 2021.
- [82] Emmanuel Pintelas, Ioannis E Livieris, and Panagiotis E Pintelas. A convolutional autoencoder topology for classification in high-dimensional noisy image datasets. *Sensors*, 21(22):7731, 2021.
- [83] Song Wang and Jiankun Hu. A blind system identification approach to cancelable fingerprint templates. *Pattern Recognition*, 54:14–22, 2016.
- [84] Narishige Abe, Shigefumi Yamada, and Takashi Shinzaki. Irreversible fingerprint template using minutiae relation code with bloom filter. In *2015 IEEE 7th international conference on biometrics theory, applications and systems (BTAS)*, pages 1–7. IEEE, 2015.

List of Publication

Published:

- Journal:"Significance of the Transition to Biometric Template Protection: Explore the Future", International Journal of Image and Graphics, Vol. 21, No. 2, 2021 (Scopus/ESCI)
- Journal:"Fingerprint Template Protection: Cancelable Biometrics", International Journal of Computational Vision and Robotic, Vol. 16, No. 4, 2026 (Scopus)
- Journal:"Privacy Preserving Fingerprint Authentication Based On Cancelable Biometrics", Multimedia Tools and Applications, Vol. 85, No. 457, 2026, Springer (SCI/Scopus/EBSCO)