Repeated Line Tracking and Multiline Neighbouring Relation (RLMN) framework for finger vein template security

Final Report

(IIBF Scheme for Research Fellowship in Banking Technology 2021-22)

Submitted by

Dr. Sachin Sharma,

Mr. Dhruv Sharma

Software Factory Department,
Global Information Technology Centre (GITC),
SCO 70, 2nd Floor, Sector 5, Panchkula (Haryana)
June, 2023

Candidate's Declaration

We hereby Certify that the work which is being presented in this report entitled "Repeated Line Tracking and Multiline Neighbouring Relation (RLMN) framework for finger vein template security" in fulfilment of the requirements for the award of the Research Fellowship in Banking Technology: 2021-22 by Indian Institute of Banking and Finance (IIBF) in association with Institute for Development and Research in Banking Technology (IDRBT), is an authentic record of my own work carried out during a period of Oct, 2022 to Dec, 2022 under the mentorship of Dr. M.V.N.K Prasad, IDRBT (Established by Reserve Bank of India), Hyderabad, Telangana, India and Dr. Mridula Verma, IDRBT (Established by Reserve Bank of India), Hyderabad, Telangana, India.

The content of this report has not been presented by us for the award of any other degree of this or any other institute/university.

(Dr. Sachin Sharma) (Dhruv Sharma)

ACKNOWLEDGEMENT

We would like to begin by thanking Dr. MVNK Prasad (IDRBT Hyderabad), Dr. Mridula Verma (IDRBT Hyderabad) and Dr. Kratika Shrivastava (IIBF Mumbai). Their support, encourage and enthusiasm motivated our team to believe in ourself towards this research work. Their professional yet caring approach towards the people they work with and their passion for living the life to the fullest have truly inspired us.

We owe our thanks to Prof. Kamal Kumar, NIT Uttarakhand for his unconditional support and believe in us. Our special thanks go to Sh. Mukesh Ahuja (State Bank of India – GOC Chandigarh) and entire team of State Bank of India at GOC Chandigarh for encouraging our team to pursue research. We would like to express our deepest gratitude to Sh. Gagandeep Singh for their invaluable guidance, support, and mentorship throughout this project. Their expertise and encouragement have been instrumental in shaping the outcome of this research.

We are sincerely grateful to Dr. Mulagala Sandhya (National Institute of Technology, Warangal) for their unwavering support and assistance during the course of this project.

I would like to express my sincere gratitude to the following individuals and institutions for providing access to their valuable finger vein databases, which have been instrumental in conducting my research:

Finger Vein USM (FV-USM) Database by Dr. Bakhtiar Affendi Rosdi, School of Electrical and Electronic Engineering, USM; The University of Twente Finger Vascular Pattern (UTFVP) Database by The University of Twente, Enschede, The Netherlands; The Hong Kong Polytechnic University Finger Image Database by The Hong Kong Polytechnic University

Their generous contributions have significantly enriched the scope and findings of this study.

All above mentioned thanks are, however, just fraction of what is because of Almighty for blessing me a chance and the divine grace to successfully achieve this task.

Dr. Sachin Sharma and Dhruv Sharma

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

PII	Personal Identifiable Information
FV-USM	Finger Vein USM
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
MQA	multi-image quality assessments
DBD	discriminative binary descriptor
CNN	convolution-neural-network
MoC	Match-on-Card
BDD	Binary decision diagram
GAN	Generative adversarial network
ROI	region-of-interest
LBP	local binary pattern
UTFVP	University of Twente Finger Vascular Pattern
HKPU	Hong Kong Polytechnic University

Table of Contents

Abstract

Due to rapid digitization, the password management becomes a challenge. There are different passwords for different applications. Therefore, financial institutions are working on alternatives like biometric for user authentication. There is an increasing trend of using biometrics in Banking and financial industry. There are various security issues with biometrics. When password of a customer is compromised, it can be changed and systems security can be tightened to avoid future attacks. This is not the case with biometrics as biometrics of a person cannot change. Therefore, financial institutions must adopt state-of-the-art security practices to handle biometrics. There has been a tremendous rise in identity theft in recent years. Biometrics is an effective tool for seamless person authentication. The parameter characteristics can be anatomical or behavioural. Anatomical characteristics refer to iris, fingerprint, voice, face etc. Behavioural biometric parameters refer to movement, keystroke dynamics etc. The technological advancements have improved biometric handling in recent year. Hence, applications of biometrics have gained popularity and are frequently used in personal computers login, office access, airport access and other. The legacy authentication systems based on tokens or password are losing popularity as they can be lost or forgotten. The on-boarding of user for biometric system is called as enrolment. In enrolment process, the key parameters of a person are extracted from biometric data and stored as templates. At the time of user authentication, the parameters are extracted from the person and matched with the parameters in enrolled template using query technique. The comparison result decides for the success or rejection of a person for authentication.

The adoption of finger vein biometrics has introduced a revolutionary approach to identity verification, promising heightened security and accuracy. We have developed a unique method for feature extraction from finger vein images, which significantly enhances the discriminative power of the biometric data. However, the stakes are high when it comes to safeguarding the stored templates. A compromise of finger vein templates can result in severe repercussions for both organizations and individuals, transcending mere financial losses and extending to potential breaches of sensitive data and personal privacy.

In response to this challenge, we are applying a cutting-edge cancellability technique to secure the finger vein biometric template. By employing irreversible template transformation, our approach ensures that even if the stored template is compromised, it cannot be reverse-

engineered to obtain the original finger vein pattern. This added layer of security complements the uniqueness of finger vein patterns and makes them highly reliable for identification purposes while mitigating the risks associated with template exposure.

Given the immutable nature of biometric traits, once compromised, the damage to the system is irreversible. Consequently, it is imperative to institute robust and sophisticated template protection mechanisms that pre-emptively shield the biometric data from unauthorized access and potential breaches. Our research proposal seeks to address this critical concern by exploring advanced encryption techniques, biometric key generation, and secure template matching protocols to further fortify the security of finger vein templates throughout their lifecycle.

Moreover, the applicability of these techniques in the banking system is of paramount importance, considering the sensitive nature of financial transactions. By integrating our proposed security measures seamlessly into the banking infrastructure, we aim to bolster the trust of both institutions and customers in the reliability and inviolability of finger vein biometrics.

Ultimately, the successful implementation of these advanced security measures, combined with our novel feature extraction method, will not only protect the interests of organizations and individuals but also foster greater acceptance and widespread adoption of finger vein biometrics as a secure and privacy-conscious identity verification solution.

Key words: *Finger vein, Cancelable biometrics, Repeated Line Tracking (RLT), Multiline Neighbouring Relationship, Quantization, Biometric Template Protection (BTP)*

CHAPTER-1

INTRODUCTION

1.1. Origin of the proposal

Introduction to Biometrics

Biometrics are the human characteristics trait that are unique in nature and are helpful in identification. Biometrics refer to the biological traits of humans such as finger print, finger vein, iris, palm, voice, etc. There is a separate field of study related to biometrics in computer science. There is an ongoing demand of authentication based on the biometrics of the user which does not require a password or a string to remember and is always available with the user. With these solutions, companies are building products around the biometrics and are able to provide more secure authentication.

Advantages

Following are the major benefits of using the biomet4cis authentication in various authentication-based accesses:

1. **Security Enhancement** – Since biometric is such a trait that the user always carries with himself or herself, the act of these getting stolen is rarely possible. The cyber criminals find it very hard to duplicate the biometrics to gain access. This is much secure than the traditional password-based accesses which can be easily forgotten, lost or brute forced.

2. **Accurate authentication**– Biometrics are the most authentic way of providing the access to any system since the biometrics can be helpful to uniquely identify the individual. In billions of populations, biometrics are such miracles of nature which are unique in nature and which provide almost 100% accuracy.

3. **Flexibility and Convenience** – Biometrics provide better flexibility and ease of access as the users do not have to provide passwords again and again for multiple access. The

authentication is really fast and accurate and provides ease to the user. Typing the password again and again will be cumbersome.

4. **Scalability** – Biometrics offer such a scalable solution that it can be integrated with multiple products and can provide single access to all of them.

Disadvantages

With great technological revolution, also comes some disadvantages or challenges which are highlighted below:

1. **Storage Issues:** This is a major challenge to the scientist to provide the storage of finger or vein pattern for all the users and to provide encryption and secure access. Huge databases and encryption techniques are required to keep this data safe and provide quick access at the same time.

2. **Scanner Compatibility:** It is also very important to understand that less technology exists in market which is open source for the other developers to build their products. Only a few patented technologies are working in monopoly and it is not always that all the scanner works perfectly with the users captured patterns. Compatibility issues remain a major challenge to upscale this technology.

3. **False positives:** Although the patterns of biometrics are unique in nature, there still are chances that biometrics can provide false positives and allow the wrong person to enter with your credentials and access your information.

Cancellable Biometrics

The concept of cancellable biometrics was necessary to avoid the situations of compromise of the patterns stored. Although it is very rare but still if the traits are lost, then the user is compromised forever. Therefore, a concept of cancellable biometric [24] was introduced to make a biometric template can be cancelled and be revoked like a password, as well as being unique to every application. The basic aim is to store a hashed version of cancellable biometrics which is linked with multiple modals so that a modal can be cancelled and reissued to the user in case of the compromise. The existing works in the technology involves the

distortion based on the no reversible matrix operations and Fourier transformations. The greater the size of the matrix the more difficult it is to form the original features for compromise.

Choosing Finger Vein for Research work

There are very few works in the industry on the finger vein and its cancellability [24]. Finger vein is emerging as the most promising technology due to its non-invasive nature and better security over finger print. The idea behind this is that the finger vein pattern is always unique. The finger prints can be forged and be compromised over time. This drawback is handled with finger vein authentication which is almost impossible to compromise because the pattern is hidden deep inside and can only be fetched from the authorised scanners.

We need to analyse the combination of finger vein and its cancellability and take forward the research and frameworks already developed in the biometric world. Since the finger vein is new and more secure than traditional biometrics, we need to analyse the already existing frameworks, strategies, and methodologies which have produced disruptive results in comparison to the finger vein.

1.2. Definition of the problem

There is a lot to explore in the field of finger vein biometrics. There is a need to explore its potential use as an alternative to the presently available authentication techniques. Finger vein data is PII (Personal Identifiable Information) and is very crucial for the organization. It is a big challenge to extract the biometric features out of the finger vein images and securely store them. In the event of any unforeseen security breach or compromise of stored data, what can be done? There is a need to explore the cancellable technique to apply it to finger vein biometrics.

CHAPTER-2

REVIEW OF LITERATURE

Recently, various proposals and studies have been published regarding finger vein, finger print and cancellable biometric. Few of them have been discussed below for reference of literature review.

In the context of telemedicine and real-time health monitoring systems, authors [1] have discussed the function of finger vein authentication systems. Wireless body area sensor networks must be developed for modern telemedicine. Protected health information is currently worth the most on the black market, and attackers and hackers are rapidly becoming aware of the potential of hacking telemedicine systems. Security is still a very difficult problem to address. One of the key areas for pervasive computing use is intelligent home settings. The two most crucial concerns in the remote monitoring and control of intelligent home environments for clients and servers in telemedicine architecture are security and privacy. A recently studied biometric method leverages the finger vein pattern for personal authentication. The paper identifies a few crucial areas for further research, such as finger vein biometric verification systems in telemedicine settings. An updated substructure of verification methods for sensor-based telemedicine architectures is what this study seeks to give. Studies that attempted to develop finger vein verification applications and software frameworks were investigated. Additionally, finger vein datasets from earlier investigations were highlighted. They discovered that some domains have gotten more study interest than others. These areas and functions give a clear picture of the gaps in terms of development and evaluation and reflect the sort of studies on finger vein biometric verification. Researchers have discussed the difficulties they encountered, and many have offered suggestions for overcoming these difficulties now and in the future. This encourages other researchers to identify possibilities and find answers by conducting additional study in this area.

To comprehensively analyze and develop a coherent taxonomy of the current research on finger vein biometric identification in medical systems, a review is undertaken [2]. In this study, papers containing the terms "biometrics," "finger veins," and "verification" in combination, as well as any of their variations, are analysed from various databases including Web of Science, ScienceDirect and IEEE Xplore. The final collection of papers on authentication models based

on finger vein biometrics are separated in systems with hardware components and with software components. Software development attempts are mentioned in the first category. The findings from the experiments, as well as the frameworks, algorithms, and techniques that work well, are provided. Additionally, the lessons learned from carrying out these investigations are explored. Hardware development attempts are detailed in the second category. This paper adds to the body of literature by offering a thorough analysis of workable solutions and knowledge gaps, enabling researchers and developers to advance the development of medical authentication system based on finger vein biometrics.

The authors suggested that the background data in images of finger veins be replaced by uniform grey data, and the effects on (i) achieved lossless compression performance and (ii) obtained recognition accuracy in case of lossy compression are assessed using 2 public datasets [3]. According to the findings, replacing the original background with a uniform one is unquestionably advantageous for lossless compression since, after smoothing out certain areas, replacement of the background improves recognition performance across all settings. According to this paper's experimental compression evaluations, it is advantageous to replace the original background of finger vein imagery with a uniform background of grey values. These effects are a result of sharp edges created when adding the uniform backdrop, which are compression artifacts at the border between finger tissue and background. More reliable outcomes are obtained by enhancing the boundary smoothness. They highlighted BPG's remarkable performance on uniform grey background data, which was undoubtedly made possible by the algorithm's superior intra-prediction.

Finger vein images are utilised to train the features of the CAE, which then uses the learnt feature codes to classify the finger veins. Experimental research employing the proposed technique and the FV USM and SDUMLA datasets has demonstrated that the proposed model performs better and operates more precisely and productively [4]. The FVUSM's EER increases from 0.16 to 0.12 percent. SDUMLA's EER increases from 6.28% to 0.21%. The FVUSM dataset results don't show much real improvement. However, there has been a major improvement in the SDUMLA database, and the EER result has been significantly reduced. The information contained in the photographs of the finger veins has been further reduced, which improves the practicality of the suggested method.

Compared to the current biometric technology, finger vein offers greater security and ease [5]. The performance of the equipment or its surroundings, however, may affect how accurate it is.

An algorithm has been suggested by the authors to enhance finger vein recognition systems. The maximum curvature method with MMCBNU 6000 was used in this paper to extract the Finger vein, and minutiae extraction was used to extract features. They use median filtering and picture dilation to lessen noise. Configure the filter bank to avoid cutting off the designated pulse when using the median filter. A block measuring 3 by 3 composes the filter bank. They eliminate the image noise and fill the finger slot by employing this technique. The MHD value improves as the Feature points decreases. Check the values with biometric authentication factors FAR, FRR, and EER. The FAR levels have improved. The EER of 3.21% is achieved, which shows the better performance than the existing vein recognition algorithms.

Another research employs an adaptive thresholding method and a binary robust invariant elementary feature from accelerated segment test feature points to propose a novel finger-vein recognition system [6]. Then, a second stage of verification is carried out using the suggested multi-image quality assessments (MQA). With the help of a strong feature and a rigorous MQA process, this recognition structure enables effective feature point matching. Because of this, the proposed method not only speeds up system computations, but also proves itself superior to earlier related studies. This paper proposes an enhanced biometric recognition system. A feature point-based approach, a POHE algorithm, and a MQA voting mechanism are all included in the now-proposed hierarchical verification system. The MQA voting method then offers a reliable identification as a second stage of verification. The optimal values for EER are, according to the experimental findings utilizing open-access databases, respectively 0.13%. The EER indices unmistakably demonstrate that the proposed strategy outperforms the cutting-edge systems. Liveness detection is a crucial spoofing defense for further development. It is necessary to confirm that the device can detect blood flow velocity using high frame rate, other light spectrum sensors.

Authors [7] have also suggested to solve the problem of unsatisfactory vein images. The suggested approach will fully utilize the labels before improving results. They contrast its performance with a number of well-known loss functions, including triplet loss and softmax loss. The MMCBNU 6000 and FV-USM datasets were used in the experiments, and the findings demonstrate that the proposed loss function not only minimizes error rates, is quicker to compute, but also prevents overfitting. Convolutional Neural Networks are noted for taking a long time to train. The length of the training phase increases with the number of layers in the network. Center loss was used in the model to obtain outstanding outcomes by maximizing the

distance between classes and minimizing the distance within classes. They also suggested an enhanced regularization to lessen the chance of overfitting. The effectiveness of the proper training tactics in identifying finger veins has been experimentally verified. According to experiments, the suggested method's accuracy in the MMCBNU 6000 and FV USM datasets can be as high as 99.05% and 97.95%, respectively, with equivalent error rates (EER) of 0.503% and 1.07%.

In order to recognize finger veins, the research suggests a brand-new feature learning technique termed the discriminative binary descriptor (DBD) [8]. By including our discriminative objective function and MDPDV into feature learning, it improves the performance of recognizing finger veins.

Deep learning is frequently employed in the field of biometrics, however in order to create a complex model that performs effectively, a lot of tagged image data is needed [9]. In terms of security and privacy, finger vein recognition outperforms traditional biometric techniques by a wide margin. However, finger vein-related datasets are scarce. This work offers a method for creating finger vein datasets using GAN as a solution to this issue.

Due to their high safety and stability qualities, finger vein features have drawn a lot of attention and are progressively finding use in a variety of areas. However, research has demonstrated that convolutional neural network-based finger vein recognition systems pose significant security issues [10]. Criminals may perform improper operations on the recognition system's database or results in order to gain access to some of the system's user information, which poses a serious security risk to the original vein data. In this research, they design a full finger vein recognition system with template protection as well as a finger vein picture encryption scheme based on the RSA algorithm. The goal of this system is to provide a finger vein feature recognition system that protects the user's finger vein template and improves the security of user biometric data. On 4 open data sets, they conduct a series of extensive tests. They intend to carry on their efforts in the following three areas in their next work. In order to increase the finger vein recognition system's representational capability and recognition performance, they will first try to employ the approach outlined in DARTS. Thirdly, they will think about safeguarding biometric templates and improving the system's defense against adversarial sample attacks.

The finger-vein is a perfect biometric feature for personal authentication because of its strength and individuality [11]. The two components of typical finger-vein authentication systems are feature extraction and feature matching. The inaccuracies in the infrared device's imaging of finger veins are brought on by changes in temperature, unreliable lighting, and deformed fingers. The retrieved characteristics are unsatisfactory and challenging to match since uncertainties lead to severe artefacts. They model the extracted characteristics as a Gaussian Mixture Model in an effort to solve the matching issue (GMM). Given two finger-vein feature maps, the proposed technique first models the inputs as GMM using the normal distribution transform, then uses gradient descent to minimize the distance between the two GMMs, and finally outputs the likelihood that the two feature maps are from the same individual. They test the performance increase using two different types of finger-vein features—finger-vein trajectory and finger-vein skeleton—to demonstrate its superiority over existing feature matching approaches. The proposed method is more precise than the traditional methods, according to experimental findings on the RATE dataset.

The premise is that verification systems arbitrarily reject low-quality pictures because they are led by the fundamental objective of evaluating the biometric quality, which is the minimizing of verification error [12]. Based on this assumption, the photographs are automatically divided into low-quality and high-quality categories. They then train a DNN to predict image quality using the obtained dataset. This study presented a unique method for predicting finger-vein picture quality through the learning of a deep feature representation.

To boost user-friendliness and lower the cost of system implementation, researchers take a finger and use all of its modalities, including fingerprint, finger-vein, and finger-knuckle [13]. The contactless fingerprint, finger vein, and finger knuckle images are all captured by just three cameras in the proposed system. They also provide a method to allow the machine to operate in identification mode. Experiments on well-known databases show that the recognition accuracy of our suggested approach is greatly increased. A low-cost, dependable imaging device that can capture contactless fingerprint, finger vein, and finger knuckle prints concurrently was also demonstrated. Only three cameras were included in the proposed system for picture capture. They could successfully merge 2D and 3D fingerprints, 2D and 3D finger veins, and 2D and 3D finger knuckle prints. The tests performed on well-known databases demonstrate that our system can handle the issue of finger rotation while improving recognition accuracy. They plan to enhance and optimize our system in subsequent work. Due of the

difficulty in reproducing, spoofing, and/or stealing the electrocardiogram (ECG), they will also add it as a biometric attribute.

Some authors [14] have studied the issue of recognition performance degradation caused by finger positional variation, misalignment, and shading from uneven illumination. Because different images are produced by different pixel values, they can be sensitive to noise. Additionally, the trained network's full layers cannot be used for computing the distance between feature vectors, hence this method is less accurate than one that uses different images. To address the challenges associated with noise and utilizing the entire network, this study proposes a method that uses composite finger-vein images as input to a deep, densely-connected convolutional network (DenseNet). The experiments were conducted using the Shandong University homologous multi-modal traits (SDUMLA-HMT) finger-vein database and The Hong Kong Polytechnic University finger image database (version 1). The results demonstrate that the proposed method outperforms existing techniques. To compensate for misalignment between enrolled and input images, a shift matching method was employed. Instead of using a difference image that is sensitive to noise, a 3-channel composite image was utilized as the input to the CNN. The study confirms that the recognition accuracy is higher when using the composite images compared to using different images. Furthermore, the composite image exhibits greater resilience against noise when tested with noisy images. Evaluation of different CNN models using two open databases revealed that the DenseNet-161 model, combined with the shift matching approach, achieved the highest recognition accuracy. According to the study's findings, a significant amount of misalignment and a lack of shading clarity were present in the majority of cases of mistaken rejection. In false acceptance cases, vein patterns were partially captured and there were issues of similarity in the pat- terns and shading. A desktop computer and an embedded system were used to test processing speed, confirming the adaptability of our method to different settings. The number of layers and transition layers in the DenseNet will be reduced in subsequent research in an effort to increase processing speed while retaining recognition accuracy. The deep CNN model and shift matching would also be used on palm- and hand-vein images in addition to finger- and palm-print images.

Following a critical comparative study of the emphasized methodologies, researchers present a few novel discoveries [15]. Comparative studies show that finger vein recognition techniques are accurate enough. This research offered a thorough analysis of traditional, machine learning-

and deep learning-based methods for identifying finger veins. The approaches for ROI extraction and picture enhancement in image preprocessing were examined. Additionally, four categories of traditional feature extraction techniques—vein-based, local binary-based, dimensionality-based, and minutiae-based techniques—were identified and described in depth. Both the distance-based matching approaches and the classifier-based matching methods were examples for the matching stage. They also contrasted established and recently created deep learning finger vein detection techniques. Deep learning algorithms outperformed conventional finger vein recognition methods, nonetheless, by a wide margin. Furthermore, to recognize spoof attacks, a high recognition spoof detection finger vein identification method is required. Additionally, the identification of finger veins benefits greatly from machine learning techniques. The integration of deep learning techniques into FVR has the potential to improve recognition performance generally. In conclusion, the authors hope that this study will serve as a valuable springboard for fresh ideas and a unifying foundation for several advantages in the field of finger vein authentication and identification.

The vein network calibration used in matching uses the venous backbone to compensate for finger displacements [16]. The suggested elastic matching method is used to compare two calibrated vein networks, and the degree of overlap between their respective vein backbones is then integrated to recompute the similarity. The efficiency of the suggested architecture has been confirmed by extensive tests on two open finger vein databases. In addition to proposing a useful framework for finger vein recognition, this article brought anatomical structure analysis to finger vein network extraction and matching.

Another research on CNN for better quality images has been discussed in another paper [17]. The main goal of the work is to produce a consistent reaction with correct performance while taking into account finger vein photos of different quality. The suggested approach is evaluated on a dataset that is thought to be publically accessible, and the published experiment results demonstrate that high identification accuracy may be attained using an efficient training and testing procedure. A convolution-neural-network (CNN) based technique is proposed in this paper that can train more quickly and identify finger veins regardless of image quality and environmental factors. The acquired findings from experimental research using a dataset that was thought to be publicly available demonstrate that the suggested method may achieve identification accuracy more than 95%, or rank-1. Large datasets can be used for more study, and using efficient training and testing techniques, accuracy can be increased.

In this study [18], the performance of vein minutiae recognition on three publicly available databases is assessed using two commercial and two freely available fingerprint comparison tools. The findings strongly suggest that minutiae-based comparison technology from fingerprint identification can be employed to identify finger veins and is capable of competing with and even outperforming traditional correlation-based techniques used in this sector. With this technique, vein recognition on MoC devices is made possible. This study demonstrates the viability of vein recognition for Match-on-Card (MoC) technology. In order to employ traditional minutiae-based fingerprint comparison tools for the recognition task, minutiae points are extracted from vein pictures and stored in a standard manner. This is an essential initial step for vein recognition for MoC systems to be seamlessly integrated. The utilization of two cutting-edge commercial and openly accessible minutiae-based fingerprint comparison software tools. The findings demonstrate that in terms of recognition performance, minutiae-based techniques can not only match but even surpass conventional correlation-based and CNN-based approaches.

In this study [19], a CNN model was constructed using the pre-trained VGG-16 model, Adam optimization, and categorical cross-entropy loss function. Techniques such as image augmentation and dropout were employed to prevent overfitting. Various fusion techniques were explored to evaluate the impact of CNN model fusion on recognition performance, including feature and score level fusion. The effectiveness of the proposed method was empirically evaluated using the SDUMLA-HMT dataset. The study introduces a multimodal biometric model for user identification, combining iris, face, and finger vein features with two fusion algorithms. This research is the first known attempt to apply deep learning methods to a multimodal biometric model encompassing these three traits. Additionally, the study examines a multimodal identification biometric system incorporating the finger vein trait, which has not been extensively studied before. Three separate CNNs were utilized in the proposed model to identify each attribute.

They [20] gather a dataset of finger vein images in video format from 100 people over the course of four different exposure times to test the suggested methodology. The acquisition module was created using inexpensive sensors and was built to allow for unfettered hand movement, which greatly increased user comfort during enrolment and recognition. A database of on-the-fly hand acquisitions from 100 subjects has been compiled. Multiple cameras have been employed, each with a distinct exposure period to capture the hand's dynamic movement

over the sensors. The suggested method takes advantage of the temporal behavior of the moving hand over the sensors as well as the photos taken at various exposure durations. In both cases, deep learning techniques have been employed.

The major goal of the research [21] is to present a deep-learning technique for finger-vein recognition that can perform consistently and extremely well when dealing with photos of varying quality. The broad set of experiments that have been published demonstrate that the accuracy that can be achieved using the suggested approach can exceed identification rate of ninety five percent for each of the databases that have been taken into consideration. In this study, they put forth a CNN-based finger-vein identification system that can function effectively regardless of the surrounding environment. They have offered a comprehensive summary of the experimental tests performed on the four widely used and available databases. The collected findings demonstrate that our suggested CNN architecture can produce rank-1 identification accuracy values more than 95% for all four datasets. The current study is one of the first in-depth analyses of a finger-vein-based biometric identification system using more than two publicly available databases, and it aims to evaluate the performance of the suggested network under various conditions of image quality while requiring the least amount of human intervention. Additionally, it is evident that as more training photos are used, the suggested network's identification accuracy considerably improves.

Within a specified timeframe, authors [22] have explored the stability of finger veins (four years). To do this, a reliable database for stability was built, and all outside influences on finger-vein features—such as buying hardware, user behaviour, and ambient factors—were totally eliminated. They then proposed a steady-state model of finger-vein features, demonstrating that each particular finger has a stable steady state to which all of its finger-vein images would appropriately converge, regardless of time. On the basis of our 5-year/200,000-finger data set, experiments have been carried out. Additionally, findings from both real and fraudulent matches show that the model is solidly supported. This generic steady-state model offers a standard way to assess the stability of other kinds of biometric features. They suggest the first investigation into the stability of finger-vein features in this paper. Data preparation, steady-state model development, and model validation on a particular dataset comprise the bulk of our effort. We have created a useful dataset that spans the years 2010 and 2015 and contains finger-vein photos from young, healthy users between the ages of 16 and 25. For the stability investigation, they removed the significant irrelevant external impact elements (such as

illumination variation, posture changes, and some situational factors). They developed a steady-state model in this study with three key components: systematic stability, interval stability, and convergence stability. The results on the selected dataset provide strong support for their steady-state model and the notion that it proposes. The outcomes also demonstrated that finger-vein characteristics may be guaranteed to remain stable for at least four years. Additionally, some significant steady-state model characteristics (such as the model definition's converging speed parameters) offer a way to quantify the stability level of finger-vein or other types of biometric features.

To solve the problems of illumination variance and image misalignment, research has been done on multimodal biometric systems that can concurrently recognise fingerprints and finger veins [23]. However, because these techniques for identifying people rely on hand-crafted features, they have some limitations in terms of performance enhancement. In this study, deep convolutional neural network (CNN)-based multimodal finger-vein and finger shape biometrics were proposed. The following provides information on what they accomplished, their scientific contributions, the significance of their work, and the ways in which our results deviate from the state-of-the-art.

In another paper [24], a cancellable finger-vein based bio-cryptosystem has been presented by the authors, which can both authenticate users and encrypt private health information using a biometric cryptographic method. System security is further increased by the use of cancellable biometrics. The validity of the suggested scheme is demonstrated by the experimental findings and security analysis. Biometric authentication technologies have gained popularity as the primary method of identity authentication in the healthcare industry as a result of its benefits. In this study, the researchers propose a novel cancellable finger-vein biometric system integrated with a smart card, specifically designed for the healthcare industry. This technology offers both authentication and data encryption for sensitive healthcare information, which is a unique feature not found in existing healthcare biometric systems. Storing the biometric template and sensitive data on the smart card ensures that information remains secure during data exchange or template transformation, as the biometric data never leaves the card. The use of cancellable biometrics further enhances the system's security, providing an additional layer of protection.

Edge devices, such as smart cameras, are able to recognise and monitor people using artificial intelligence (AI) [25]. Edge biometrics is a key use of machine/deep learning as a driver behind

AI. Edge biometric systems that use machine learning or deep learning perform better than their traditional counterparts. Convolutional neural networks, for example, are invertible, according to studies, which means that adversaries can learn some knowledge about the initial inputs/templates. Because the biometric information contained in the original (raw) templates cannot be changed or reset, this information leakage is intolerable for biometric systems. Once compromised, they are irretrievably gone. Therefore, how to prevent original biometric templates from being attacked through inverting deep neural networks is a pressing but unsolved issue for deep learning based biometric recognition. To address the issue, another paper discuses a novel biometric template protection algorithm using the binary decision diagram (BDD) for deep learning-based finger-vein biometric systems. The suggested technique may produce a new, non-invertible version of the original finger-vein template, which is then stacked with an artificial neural network to create the BDD-ML-ELM, a finger-vein recognition system that protects privacy. Even if its converted version is flawed, the suggested BDD-ML-ELM ensures the security of the original finger-vein template. By simply altering the user-specific keys, the changed template can be revoked and replaced with a fresh copy if it becomes hacked. The size of the user-specific keys is reduced and thus less storage space is needed, which is advantageous for edge devices with restricted resources. This is accomplished by segmenting the lengthy binary-valued feature vector into short segments. The experimental findings demonstrate that the suggested BDD-ML-ELM achieves a good compromise between security and recognition precision. Our next work will look into ways to increase the recognition accuracy of edge biometric systems based on deep learning while enforcing template protection.

Authors [26] have tried to bring out constraints in the existing CNN based image enhancements technique. In this research, as the first attempt in this field, they present a unique method for finger vein extraction and verification called FV-GAN that is based on generative adversarial network (GAN). In this paper [26], they proposed a CycleGAN-based pattern extraction model called FV-GAN for finger vein verification. The FV-GAN framework was created to extract the vein patterns from photos of finger veins and estimate the likelihood that pixels in an image will be veins or background by learning a deep pattern representation. According to experimental findings, FV-GAN can reliably extract vein patterns and greatly enhance verification performance in terms of accuracy and EER, proving the value and effectiveness of adversarial training. To further enhance the effectiveness of finger vein verification, they intend to look into the following intriguing issues in the future.

Initially, a comprehensive examination of the finger vein imaging technique and the characteristics of the captured images is provided [27]. This analysis aims to demonstrate how the intensity distribution can be extracted as a soft biometric feature for recognition. Then, for intensity distribution feature extraction, three extraction algorithms for soft biometric trait and two methods for extracting background of finger vein are suggested. In order to address the dimension discrepancy, a hybrid matching technique is finally developed. In the past, the majority of finger vein recognition research has concentrated exclusively on the textural feature of the veins, paying little attention to the intensity distribution in the backdrop or even labelling it as noise. The idea of finger vein imaging is examined in this study, along with the image's properties, and a soft biometric trait extraction algorithm is suggested. First, ILS and GB are used to extract the background layer without the finger vein texture. Then, three soft biometric features are used to define the intensity distribution in the background layer.

The effectiveness of the system is negatively impacted by both of these issues. Generally speaking, current systems are more sensitive to finger positioning fluctuations, especially those brought on by pitch and roll motions [28]. Despite significant efforts to address it in recent years, this issue still presents a difficulty. The authors have proposed an entirely new system to address the aforementioned problems. This research introduces a full-view 3D finger vein verification system that overcomes the limitations of conventional systems. By utilizing three cameras positioned in an equilateral triangle, it captures comprehensive vein pattern information across the entire finger. This approach incorporates both 2D images and 3D geometric features, allowing for accurate reconstruction of the 3D finger vein structure. This innovative system represents the first instance of creating full-view 3D finger vein structures from three 2D photos. In order to verify 3D finger veins, they then devise a focused feature extraction and matching approach. Finally, they combine the finger's 3D geometric properties and texture features to further boost the system's performance. The outcomes of several studies conclusively show that the proposed 3D finger vein verification system not only outperforms conventional 2D finger vein verification systems in terms of verification performance but also has higher potential, especially.

The deformation tolerance of minutia-based finger vein recognition has been studied by authors, yet issues still exist: One minute detail is checked with every minute detail from every other image during matching, which takes time and can result in false pairings [29]. Two minutiae details are taken from some finger vein photos are small in amount. To tackle these

challenges, this study introduces a zone-based minutia matching strategy that merges traditional region-of-interest (ROI) based approach with minutia matching. To assure the quantity of the retrieved minutiae, they first extract minutiae from each block of segmented images. Second, a sensible neighbourhood zone's minutiae are chosen for matching, which to some part eliminates erroneous pairings and eliminates pointless matches. The suggested matching procedure is more reliable and parameter-free while performing minutia matching than conventional techniques. Numerous tests show that the suggested technique is reliable and effective.

The authors [30] partition the original finger vein images into structure and noise components, representing the levels of blurriness and the distribution of noise respectively, using total variation (TV) regularization first. Second, structure and noise data are encoded in the decomposed components using a block local binary pattern (LBP) descriptor. Finally, they employ a cascaded support vector machine (SVM) model for classification, which successfully identifies finger vein presentation attacks. They created a brand-new finger vein presentation attack database to gauge the effectiveness of our strategy. Our solution clearly outperforms state-of-the-art methods, according to extensive experimental results collected from two finger vein presentation assault databases and a palm vein presentation attack database. In this study, they put out a brand-new technique for treating finger vein PAD dubbed TV-LBP. We believe that this is the first time that the blurriness levels and noise distributions of authentic and fake photos have been considered as distinct properties. They discovered that they may extract discriminative features as PAD criteria as a result.

For the purpose of identifying finger veins, some writers have examined an adaptive-learning Gabor filter. In their approach, the authors [31] utilize a combination of Gabor filters and deep neural networks. They employ the Gabor filter to calculate the gradient of the filter's parameters based on the objective function, and then refine these parameters through back-propagation. By using this approach, they not only choose the most suitable and efficient parameters of Gabor filter to create the filter banks, but they also take into account how those parameters relate to one another. Finally, they conduct tests using four open datasets of finger veins. Experimental findings show that our method performs better than cutting-edge methods in classifying finger veins.

Conventional methods for extracting regions of interest (ROI) from finger veins often rely on techniques such as edge detection and sliding window identification of joint lines [32]. These

methods typically require the setting of a predetermined threshold, which involves adjusting multiple parameters. The derived results are not precise enough when there are significant variations in illumination or poor image quality. A defined operator pattern and a small number of extracted feature patterns are additional features of the current feature extraction method. As a result, a lot of useful feature information is lost. The efficiency of the innovation points of the multi-task model combined with several sub-tasks is demonstrated by the comparison with the single task model. Finally, it thoroughly assesses the applicability of the model in this work in comparison to the existing approaches on the EER index.

After study related literature in this field, we could identify the objectives of the research. The objectives are as:

1. Extraction of finger vein features using a Repeated Line Tracking algorithm.
2. Using a multiline neighbouring relation generation technique, apply cancelability to finger vein features.
3. Experimental setup using benchmark databases.
4. Results and analysis on parameters like accuracy, revocability and security analysis.

CHAPTER-3

FEATURES EXTRACTION AND CANCELABILITY

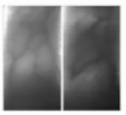
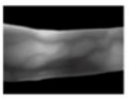
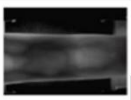
On analysis of related literature, we have identified Repeated Line Tracking algorithm for feature extraction from finger vein images.

Repeated Line Tracking Algorithm for Finger Vein Features Extraction

The minutiae detection algorithm used in this approach relies on ridge line following. Ridge line following involves identifying the local darkest position in the cross-sectional profiles. While this method works effectively when the ridge is clearly visible, it is not suitable for finger vein images due to their lack of clarity.

The Repeated Line Tracking algorithm described in [35] addresses the aforementioned issues. This method utilizes line tracking, starting from various positions, to identify local dark lines in the finger vein image. The tracking process involves moving pixel by pixel along the lines. In cases where a dark line is not detectable, a new tracking operation begins from another position. By repeatedly executing these local line tracking operations, all the dark lines in the image can be tracked. Ultimately, the overlapping loci of the lines provide the statistical pattern of the finger veins. The repeated tracking operations contribute to emphasizing the dark lines while minimizing the emphasis on noise, resulting in robust line extraction. Additionally, reducing the number of tracking operations and spatially reducing the pattern help reduce computational costs.

Some of the available databases (that can be utilized to apply RLT algorithm) are:

Database	No of images	No of Subject	Finger Number per Subject	Image Number per Finger	Image resolution	Format	Typical Image
THU-FVFDT1[13]	440	220	1	1	720x576pxl (raw)	.BMP	
UTFV[14]	1440	60	6 (Index, ring, middle, of both hands)	4	672x380pxl	8 bit gray scale .PNG	
MMCBNU_6000[15]	6000	100	6 (Index, ring, middle, of both hands)	10	480x640pxl	.BMP	
HKPU-FV[16]	6264	156	3 (Index, ring, middle of left hand)	12/6*	513x256pxl	.BMP	
SDMULA-HMT[17]	3816	106	6 (Index, ring, middle, of both hands)	6	320x240pxl	.BMP	

*For the second imaging session, there were only 105 subjects turned up, so each of fingers from these subjects has 6 images, but others each has 12 images

Figure 1. Finger vein databases available for public use [34]

Some of the available finger vein databases available for public use is displayed in Figure 1. We were able to gain access to three databases, namely the UTFV finger vein database, The Hong Kong Polytechnic University finger vein image database, and the Finger Vein USM (FV-USM) Database.

3.1 Features Extraction using RLT Algorithm (The University of Twente Finger Vascular Pattern (UTFVP) Database)

The steps used for experimental and result purpose are as:

a) Using an input image from database, grey value of every pixel is captured in text file.
b) Create histogram of the input image grey values with grey value on x-axis (0-256) and frequency of pixels grey values are on y-axis.
c) Apply repeated line tracking (RLT) algorithm on the input image.
d) Capture pixel values of every pixel after applying RLT on the image in text file.
e) Create histogram after applying RLT with grey value on x-axis (0-256) and frequency of pixels grey value on y-axis.
f) Binarization of the RLT image with a particular threshold. Values less than threshold are converted into 0 (Black) and values greater than threshold is converted into 255 (white).
g) The set of white pixels is considered as the finger vein features.

We have executed steps b to step g on every image of the database using different threshold. Initially, we have used threshold 150, 155, 160, 165 and 170.

On analysing output files of different threshold limits, it has been observed that the best results and binarized image is expected to get from threshold 151 and 155. The best results mean significant number of white pixels (features) and less noise in binarized image with clear view of the vein patterns.

Therefore, we have narrow down further and generated output for the UTVF database using threshold 151, 152, 153 and 154. By doing this, we have output results on complete UTVF database for threshold values 151, 152, 153, 154 and 155.

The source code is in C++ and is using opencv library.

Input Image and Image after applying Repeated Line Tracking (RLT) on UTVF database:

Input Finger Vein Image	Image after applying RLT on Input Image

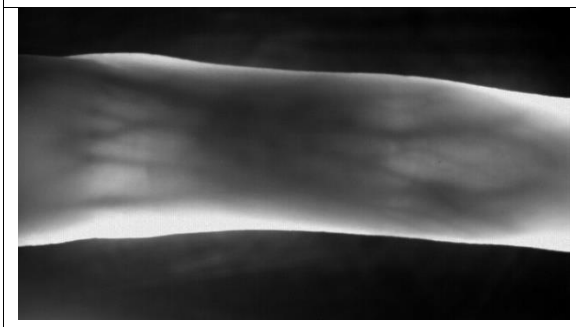
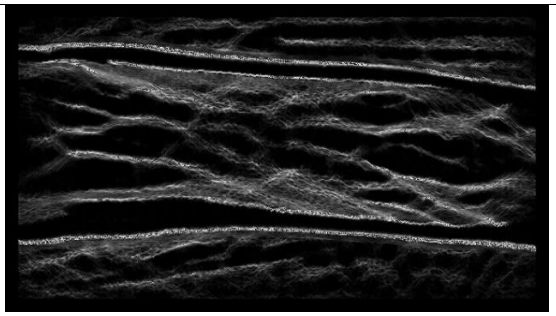

	

Figure 2. Input Image (UTVF Database)	**Figure 3.** Output Image after applying RLT on the input image (UTVF Database)

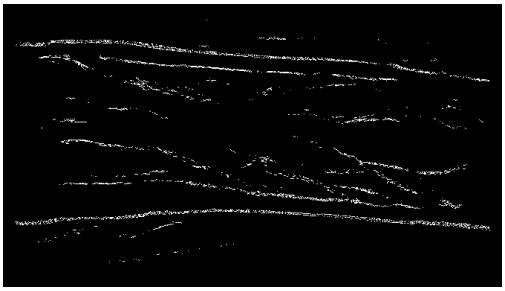


Figure 4: Binarized Image (UTVF Database)

Pixel Sr. No.	**Pixel Position**	**Grey Value**	**Pixel Sr. No.**	**Pixel Position**	**Grey Value**
1	(0,0)	7	…….	…….	…….

2	(1,0)	6	…….	…….	…….
3	(2,0)	7	…….	…….	…….
4	(3,0)	6	…….	…….	…….
5	(4,0)	8	…….	…….	…….
6	(5,0)	6	…….	…….	…….
7	(6,0)	9	255335	(646,379)	2
8	(7,0)	10	255336	(647,379)	1
9	(8,0)	8	255337	(648,379)	4
10	(9,0)	7	255338	(649,379)	3
11	(10,0)	9	255339	(650,379)	3
12	(11,0)	7	255340	(651,379)	3
13	(12,0)	10	255341	(652,379)	4
14	(13,0)	8	255342	(653,379)	2
15	(14,0)	9	255343	(654,379)	3
16	(15,0)	7	255344	(655,379)	3
17	(16,0)	11	255345	(656,379)	3
18	(17,0)	12	255346	(657,379)	4
19	(18,0)	11	255347	(658,379)	4
20	(19,0)	12	255348	(659,379)	2
21	(20,0)	14	255349	(660,379)	3
22	(21,0)	12	255350	(661,379)	4
23	(22,0)	13	255351	(662,379)	2
24	(23,0)	11	255352	(663,379)	1
25	(24,0)	14	255353	(664,379)	3
26	(25,0)	11	255354	(665,379)	3
27	(26,0)	15	255355	(666,379)	2
28	(27,0)	12	255356	(667,379)	1
29	(28,0)	12	255357	(668,379)	3
30	(29,0)	10	255358	(669,379)	0
31	(30,0)	12	255359	(670,379)	2
32	(31,0)	9	255360	(671,379)	0

Table 1: Raw Image Pixel Grey Values

Table 1 describe pixel intensity (grey value) of every pixel in the raw finger vein image from finger vein image database. Figure 2 is showing raw image from UTVF database and Figure 3 is showing image after applying Repeated Line Tracking (RLT) on the image.

Grey Value Histogram:

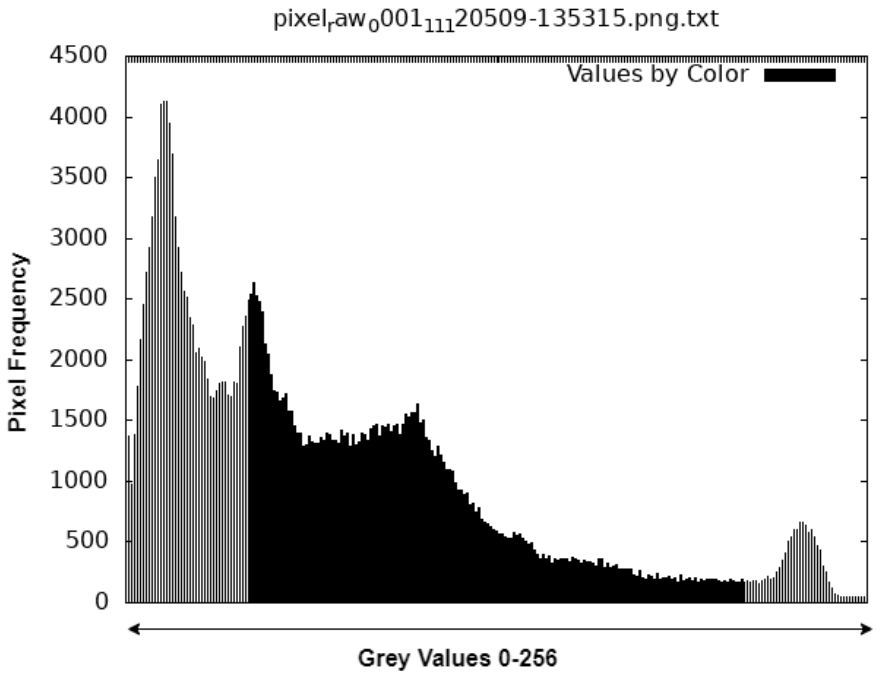


Figure 5. Histogram of the Input Image (from UTVF database)

Histogram of the input image is shown in Figure 5, which is showing grey values on x-axis and pixel frequency on y-axis.

Grey Value of some of pixels of RLT image (displayed in Figure 3 above):

Feature Coordinates	Grey Value after applying RLT	Original Grey Value	Feature Coordinates	Grey Value after applying RLT	Original Grey Value
(274,21)	177	18	(85,48)	251	15
(365,44)	167	19	(86,48)	194	19
(366,44)	173	19	(87,48)	214	17
(345,45)	171	25	(89,48)	209	18
(347,45)	181	22	(90,48)	158	19
(348,45)	167	23	(91,48)	200	16
(350,45)	173	24	(92,48)	216	21
(351,45)	196	21	(93,48)	232	17

(358,45)	165	23	(94,48)	189	22
(360,45)	211	21	(96,48)	211	21
(361,45)	229	19	(100,48)	209	21
(363,45)	165	18	(104,48)	248	18
(369,45)	218	16	(105,48)	248	21
(371,45)	226	16	(116,48)	174	24
(402,45)	162	13	(119,48)	162	20
(419,45)	169	13	(123,48)	252	21
(346,46)	179	27	(125,48)	197	25
(358,46)	198	21	(128,48)	202	24
(359,46)	218	19	(130,48)	215	22
(362,46)	191	20	(131,48)	163	20
(365,46)	168	20	(132,48)	162	23
(367,46)	254	16	(135,48)	230	21
(369,46)	160	17	(136,48)	211	22
(370,46)	241	18	(137,48)	180	20
(372,46)	241	20	(138,48)	251	26
(374,46)	185	19	(140,48)	220	24
(376,46)	199	18	(143,48)	232	20
(377,46)	202	16	(144,48)	196	25
(378,46)	193	17	(506,48)	167	8
(379,46)	197	15	(64,49)	167	17
(397,46)	156	15	(65,49)	165	16
(355,47)	158	21	(66,49)	172	18
(356,47)	201	23	(67,49)	169	16
(357,47)	222	20	(68,49)	160	16
(364,47)	174	22	(70,49)	167	16
(370,47)	174	18	(72,49)	207	15
(371,47)	235	17	(73,49)	182	13
(373,47)	218	16	(74,49)	211	18
(374,47)	163	18	(75,49)	204	16
(375,47)	172	15	(76,49)	209	17
(377,47)	182	17	(77,49)	240	16
(378,47)	194	18	(78,49)	240	16
(379,47)	205	15	(79,49)	211	16
(380,47)	202	16	(81,49)	190	14
(505,47)	173	9	(87,49)	194	17
(78,48)	172	17	(89,49)	225	17
(79,48)	192	15	(94,49)	196	23
(81,48)	173	15	(96,49)	183	21
(83,48)	188	17	(100,49)	236	22
(84,48)	177	15	(102,49)	232	21

Table 2: Grey Value of Some Pixels of RLT Image (UTVF database)

Pixel wise frequency of grey value of raw image as shown in Figure 2:

Grey Values	Pixel Frequency	Grey Values	Pixel Frequency	Grey Values	Pixel Frequency
0	51259	86	576	172	87
1	23505	87	517	173	78
2	17083	88	523	174	85
3	11080	89	475	175	76
4	7179	90	492	176	77
5	5340	91	470	177	66
6	4340	92	467	178	76
7	3792	93	435	179	73
8	3392	94	406	180	61
9	3087	95	426	181	84
10	2949	96	403	182	66
11	2762	97	425	183	51
12	2654	98	378	184	65
13	2569	99	402	185	56
14	2454	100	342	186	50
15	2397	101	366	187	60
16	2265	102	362	188	63
17	2212	103	337	189	64
18	2126	104	326	190	68
19	2061	105	362	191	54
20	2058	106	359	192	51
21	1981	107	336	193	49
22	1874	108	308	194	69
23	1824	109	319	195	49
24	1830	110	291	196	46
25	1795	111	287	197	47
26	1718	112	277	198	44
27	1736	113	269	199	54
28	1622	114	253	200	50
29	1577	115	280	201	61
30	1600	116	251	202	78
31	1622	117	259	203	50
32	1599	118	253	204	44
33	1522	119	256	205	43
34	1517	120	210	206	52
35	1477	121	221	207	43
36	1427	122	225	208	39
37	1496	123	229	209	53
38	1438	124	233	210	46
39	1461	125	189	211	50

40	1336	126	213	212	43
41	1378	127	186	213	52
42	1298	128	224	214	37
43	1295	129	203	215	48
44	1297	130	188	216	59
45	1198	131	190	217	46
46	1208	132	177	218	47
47	1248	133	169	219	29
48	1215	134	173	220	48
49	1208	135	160	221	48
50	1219	136	159	222	37
51	1221	137	162	223	42
52	1164	138	165	224	28
53	1098	139	151	225	40
54	1091	140	132	226	44
55	1108	141	132	227	25
56	1019	142	126	228	32
57	1039	143	134	229	44
58	1086	144	144	230	27
59	976	145	143	231	39
60	976	146	111	232	36
61	989	147	121	233	26
62	1015	148	114	234	39
63	962	149	84	235	25
64	955	150	127	236	35
65	965	151	118	237	32
66	912	152	100	238	23
67	862	153	105	239	33
68	860	154	109	240	34
69	854	155	92	241	28
70	823	156	88	242	35
71	809	157	95	243	38
72	790	158	115	244	25
73	736	159	85	245	30
74	761	160	89	246	28
75	717	161	81	247	28
76	762	162	92	248	29
77	703	163	78	249	25
78	646	164	108	250	21
79	708	165	88	251	32
80	674	166	91	252	32
81	660	167	101	253	25
82	554	168	93	254	26
83	578	169	87	255	25

84	604	170	84		
85	547	171	71		

Table 3: Pixel wise frequency of grey value of raw image as shown in Figure 2 (UTVF database)

Table 3 is showing pixelwise frequency of grey value of raw image of UTVF database.

Histogram of image after applying Repeated Line Tracking (RLT) Algorithm (UTVF Database):

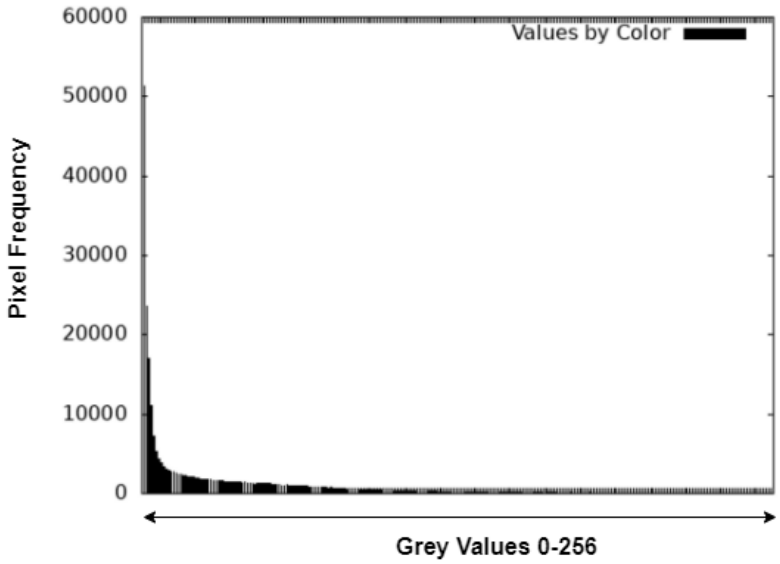


Figure 6. Histogram of image after applying RLT (UTVF Database)

Histogram showing in figure 6 describing grey values on x-axis and pixel frequency on y-axis. This histogram is based on the pixels and grey values described on Table 2.

3.1.1 Output Results using Threshold 151

Binarization of Image (Threshold 151)

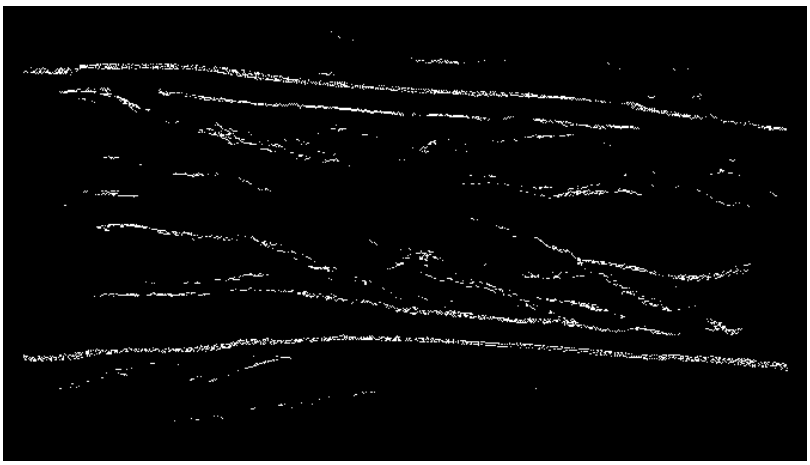


Figure 7: Binarized image after RLT (Threshold 151).

The binarization has been applied on the RLT image as shown in figure 3. The threshold value used for binarization is 151 for experimental purpose. This implies that pixel having grey value greater than 151 is converted into 255 and in other case, the pixel grey value (pixel intensity) is converted into 0. 0 grey value represents black background and 255 value represents white pixels which may be referred as the features of the image.

The resultant binarized image using threshold value of 151 is shown in Figure 7 above. The RLT image is having total pixels 255360, out of which white pixels comes out 5755 and 249605 pixels are black pixels. This means that using threshold value of 151 for binarization, the number of features of the RLT image comes out as 5755.

3.1.2 Output Results using Threshold 152:

Binarization of Image (Threshold 152)

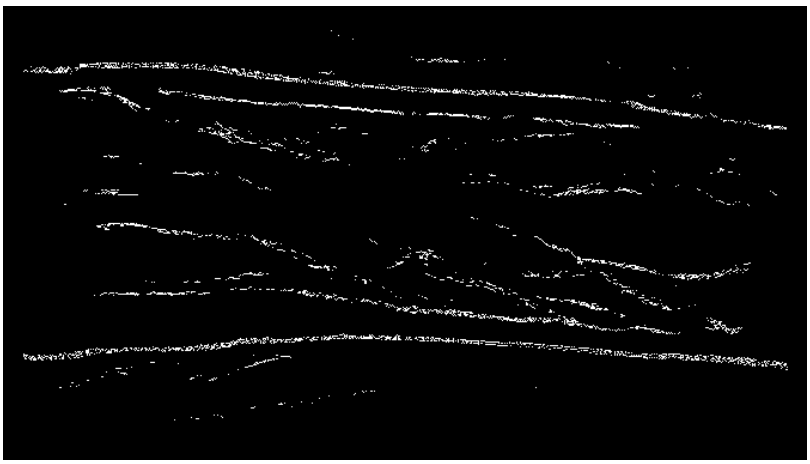


Figure 8: Binarized image after RLT (Threshold 152)

The binarization has been applied on the RLT image as shown in figure 3. The threshold value used for binarization is 152 for experimental purpose. This implies that pixel having grey value greater than 152 is converted into 255 and in other case, the pixel grey value (pixel intensity) is converted into 0. 0 grey value represents black background and 255 value represents white pixels which may be referred as the features of the image.

The resultant binarized image using threshold value of 152 is shown in Figure 8 above. The RLT image is having total pixels 255360, out of which white pixels comes out 5655 and 249705 pixels are black pixels. This means that using threshold

value of 152 for binarization, the number of features of the RLT image comes out as 5655.

3.1.3 Output Results using Threshold 153:

Binarization of Image (Threshold 153)

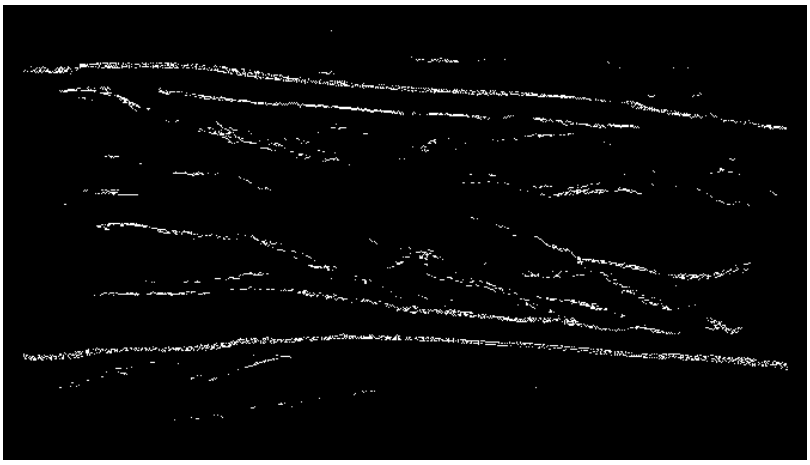


Figure 9: Binarized image after RLT (Threshold 153)

The binarization has been applied on the RLT image as shown in figure 3. The threshold value used for binarization is 153 for experimental purpose. This implies that pixel having grey value greater than 153 is converted into 255 and in other case, the pixel grey value (pixel intensity) is converted into 0. 0 grey value represents black background and 255 value represents white pixels which may be referred as the features of the image.

The resultant binarized image using threshold value of 153 is shown in Figure 9 above. The RLT image is having total pixels 255360, out of which white pixels comes out 5550 and 249810 pixels are black pixels. This means that using threshold value of 153 for binarization, the number of features of the RLT image comes out as 5550.

3.1.4 Output Results using Threshold 154:

Binarization of Image (Threshold 154)

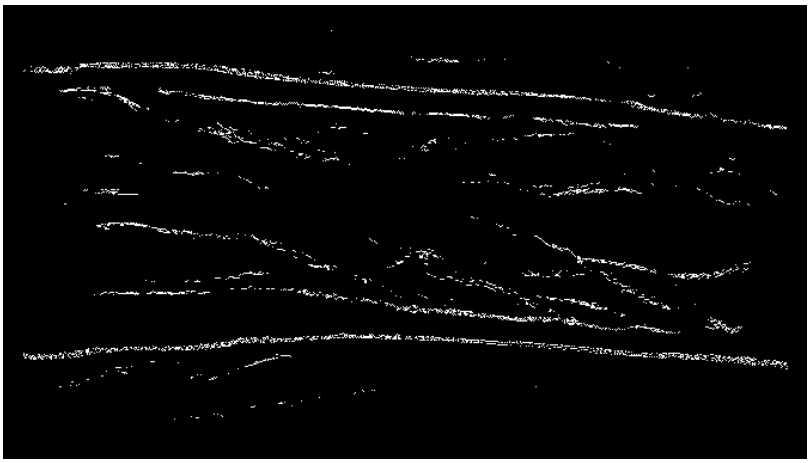


Figure 10: Binarized image after RLT (Threshold 154)

The binarization has been applied on the RLT image as shown in figure 3. The threshold value used for binarization is 154 for experimental purpose. This implies that pixel having grey value greater than 154 is converted into 255 and in other case, the pixel grey value (pixel intensity) is converted into 0. 0 grey value represents black background and 255 value represents white pixels which may be referred as the features of the image.

The resultant binarized image using threshold value of 154 is shown in Figure 10 above. The RLT image is having total pixels 255360, out of which white pixels comes out 5441 and 249919 pixels are black pixels. This means that using threshold value of 154 for binarization, the number of features of the RLT image comes out as 5441.

3.1.5 Output Results using Threshold 155

Binarization of Image (Threshold 155)

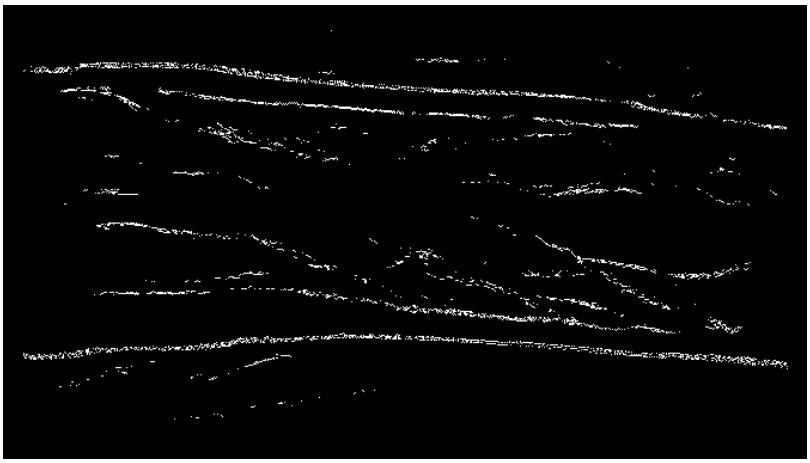


Figure 11: Binarized image after RLT (Threshold 155)

The binarization has been applied on the RLT image as shown in figure 3. The threshold value used for binarization is 155 for experimental purpose. This implies that pixel having grey value greater than 155 is converted into 255 and in other case, the pixel grey value (pixel intensity) is converted into 0. 0 grey value represents black background and 255 value represents white pixels which may be referred as the features of the image.

The resultant binarized image using threshold value of 155 is shown in Figure 11 above. The RLT image is having total pixels 255360, out of which white pixels comes out 5349 and 250011 pixels are black pixels. This means that using threshold value of 155 for binarization, the number of features of the RLT image comes out as 5349. Bar chart of binarized image having threshold value of 155 is shown in figure 12 for UTVF database.

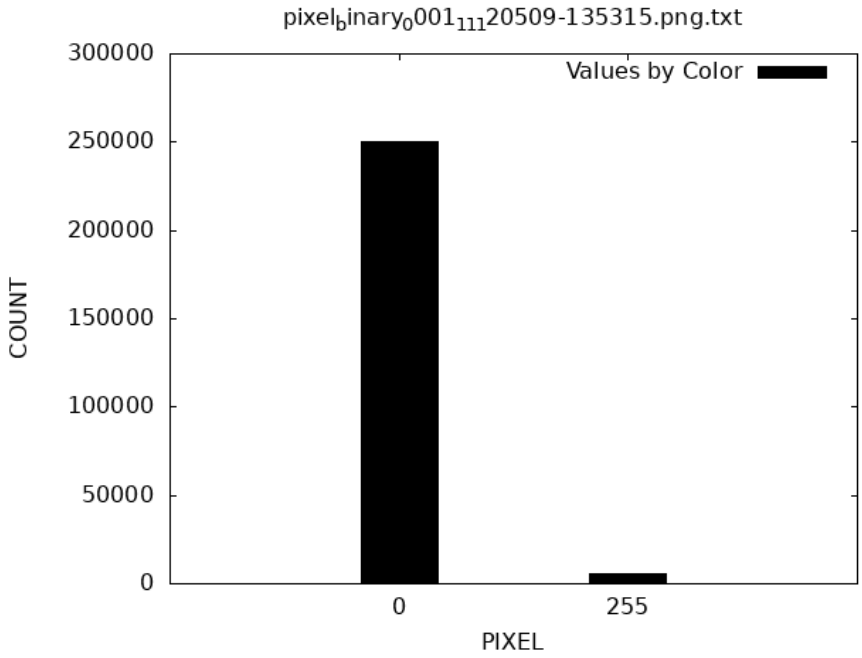


Figure 12: Bar Chart of Binarized Image (Using Threshold 155) – UTVF Database

3.2 Features Extraction using RLT Algorithm (The Hong Kong Polytechnic University Finger Image Database)

Input Image and Image after applying Repeated Line Tracking (RLT):

Input Finger Vein Image	Image after applying RLT on Input Image

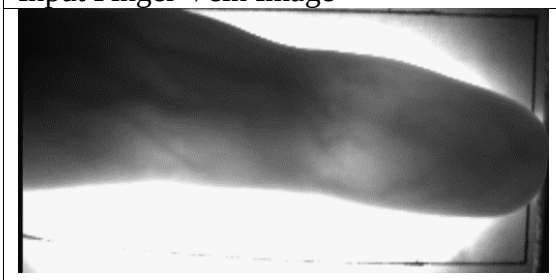
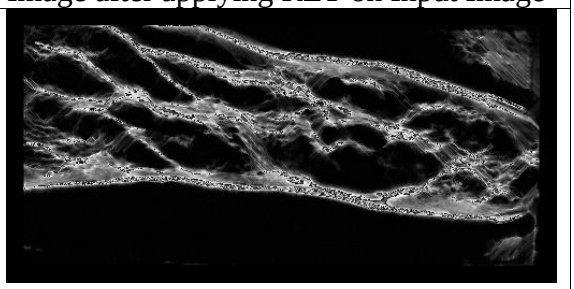

	

Figure 13. Input Image (HKPU Database)	**Figure 14.** Output Image after applying RLT on the input image (HKPU Database)

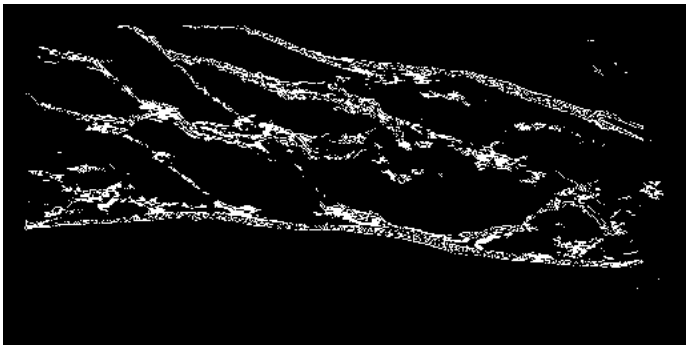


Figure 15: Binarized Image (HKPU Database)

Pixel Sr. No.	Pixel Position	Grey Value	Pixel Sr. No.	Pixel Position	Grey Value
1	(0,0)	8	…..	…..	…..
2	(1,0)	8	…..	…..	…..
3	(2,0)	8	…..	…..	…..
4	(3,0)	8	…..	…..	…..
5	(4,0)	8	…..	…..	…..
6	(5,0)	9	…..	…..	…..
7	(6,0)	10	…..	…..	…..
8	(7,0)	9	…..	…..	…..
9	(8,0)	11	…..	…..	…..
10	(9,0)	10	…..	…..	…..
11	(10,0)	11	…..	…..	…..
12	(11,0)	11	…..	…..	…..
13	(12,0)	12	…..	…..	…..
14	(13,0)	12	…..	…..	…..
15	(14,0)	12	…..	…..	…..
16	(15,0)	13	…..	…..	…..
17	(16,0)	13	…..	…..	…..
18	(17,0)	13	…..	…..	…..
19	(18,0)	13	…..	…..	…..
20	(19,0)	14	…..	…..	…..
21	(20,0)	14	…..	…..	…..
22	(21,0)	15	131318	(502,255)	25
23	(22,0)	15	131319	(503,255)	19
24	(23,0)	15	131320	(504,255)	15
25	(24,0)	16	131321	(505,255)	8
26	(25,0)	15	131322	(506,255)	8
27	(26,0)	16	131323	(507,255)	8
28	(27,0)	16	131324	(508,255)	8
29	(28,0)	16	131325	(509,255)	8
30	(29,0)	16	131326	(510,255)	8
31	(30,0)	17	131327	(511,255)	8
32	(31,0)	17	131328	(512,255)	8

Table 4: Raw Image Pixel Grey Values (HKPU Database)

Table 3 describe pixel intensity (grey value) of every pixel in the raw finger vein image from finger vein image database. Figure 13 is showing raw image from HKPU database and Figure 14 is showing image after applying Repeated Line Tracking (RLT) on the image.

Grey Value Histogram (HKPU DB):

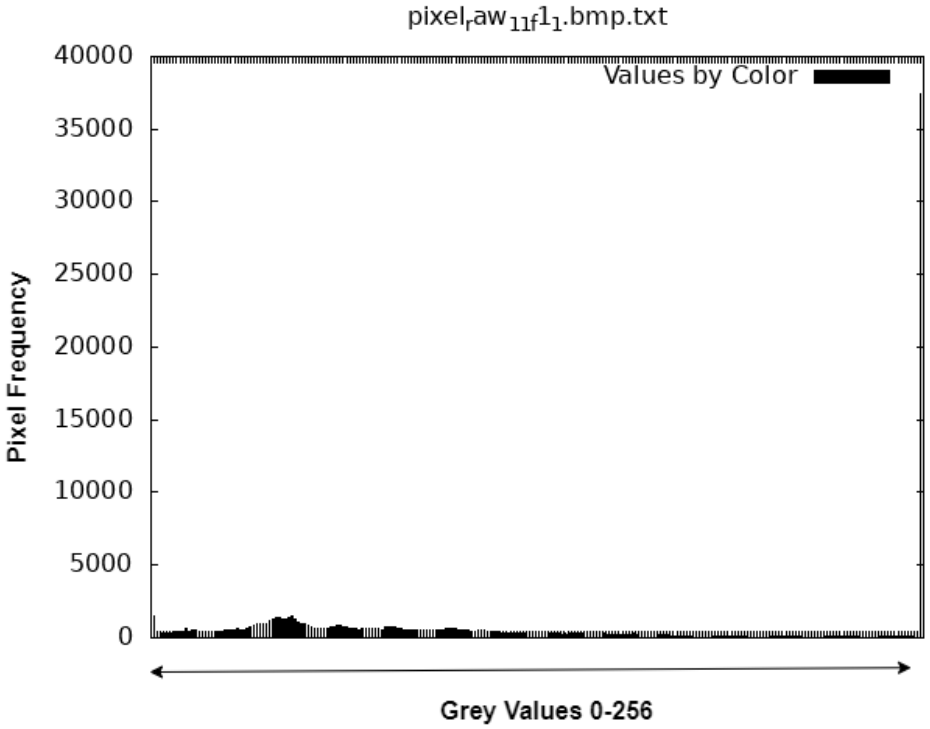


Figure 16. Histogram of the Input Image (from HKPU database)

Histogram of the input image is shown in Figure 16, which is showing grey values on x-axis and pixel frequency on y-axis.

Grey Value of some of pixels of RLT image (displayed in Figure 14 above):

Feature Coordinates	**Grey Value after applying RLT**	**Original Grey Value**	**Feature Coordinates**	**Grey Value after applying RLT**	**Original Grey Value**
(87,16)	156	21	(169,17)	211	47
(88,16)	203	22	(170,17)	166	47
(89,16)	195	21	(171,17)	162	47
(90,16)	216	22	(172,17)	202	48
(91,16)	195	22	(173,17)	231	48
(92,16)	156	22	(182,17)	184	52
(93,16)	161	23	(95,18)	198	24
(94,16)	167	23	(96,18)	214	25
(135,16)	158	39	(98,18)	228	25

(136,16)	180	40	(100,18)	243	25
(137,16)	197	40	(101,18)	174	26
(138,16)	222	40	(144,18)	157	40
(139,16)	233	40	(159,18)	160	43
(140,16)	245	40	(164,18)	165	45
(141,16)	216	40	(175,18)	160	48
(149,16)	230	43	(178,18)	167	49
(151,16)	252	43	(179,18)	211	49
(153,16)	244	43	(180,18)	214	50
(154,16)	248	44	(183,18)	181	51
(161,16)	252	45	(184,18)	180	52
(176,16)	193	50	(99,19)	208	25
(181,16)	176	52	(100,19)	164	25
(86,17)	157	22	(102,19)	168	26
(87,17)	181	22	(103,19)	172	26
(88,17)	212	22	(182,19)	238	50
(89,17)	228	22	(185,19)	201	51
(94,17)	240	23	(189,19)	192	53
(98,17)	215	26	(99,20)	199	25
(99,17)	156	26	(102,20)	239	26
(140,17)	162	40	(103,20)	184	26
(141,17)	202	40	(104,20)	191	27
(143,17)	177	41	(183,20)	175	50
(144,17)	172	40	(184,20)	200	50
(146,17)	189	41	(187,20)	166	51
(147,17)	173	41	(189,20)	251	52
(151,17)	180	42	(191,20)	182	53
(152,17)	182	43	(192,20)	165	53
(153,17)	167	43	(100,21)	206	25
(155,17)	175	44	(101,21)	227	26
(156,17)	231	44	(105,21)	237	27
(157,17)	225	43	(184,21)	163	49
(158,17)	193	41	(185,21)	182	48
(159,17)	176	43	(187,21)	190	50
(160,17)	175	43	(189,21)	224	51
(163,17)	186	46	(190,21)	202	51
(164,17)	176	46	(191,21)	254	52
(165,17)	167	47	(194,21)	228	54
(166,17)	160	47	(101,22)	197	26
(167,17)	179	47	(102,22)	193	26
(168,17)	157	47	(184,22)	157	48

Table 5: Grey values of some of the pixels of RLT image (HKPU Database)

Pixel wise frequency of grey value of raw image as shown in Figure 13:

Grey Values	Pixel Frequency	Grey Values	Pixel Frequency	Grey Values	Pixel Frequency
0	30221	86	240	172	124
1	12766	87	275	173	116
2	12774	88	279	174	96
3	8815	89	249	175	114
4	5385	90	267	176	111
5	3066	91	260	177	107
6	1869	92	235	178	118
7	1323	93	277	179	100
8	1011	94	228	180	95
9	929	95	205	181	122
10	803	96	239	182	110
11	814	97	218	183	96
12	754	98	236	184	117
13	717	99	248	185	97
14	676	100	222	186	112
15	653	101	248	187	90
16	651	102	239	188	94
17	675	103	222	189	92
18	574	104	239	190	90
19	567	105	214	191	84
20	562	106	234	192	103
21	583	107	225	193	99
22	572	108	201	194	89
23	500	109	208	195	88
24	508	110	224	196	78
25	507	111	203	197	75
26	512	112	220	198	73
27	475	113	230	199	90
28	471	114	203	200	94
29	426	115	204	201	79
30	463	116	225	202	77
31	431	117	216	203	67
32	452	118	189	204	63
33	440	119	221	205	66
34	439	120	187	206	87
35	424	121	184	207	78
36	413	122	186	208	77
37	400	123	205	209	76
38	426	124	175	210	77
39	374	125	214	211	73
40	400	126	207	212	60
41	383	127	179	213	69
42	431	128	184	214	82
43	408	129	177	215	60

44	376	130	189	216	64
45	415	131	184	217	66
46	342	132	171	218	72
47	379	133	184	219	65
48	332	134	199	220	53
49	336	135	194	221	55
50	363	136	183	222	64
51	322	137	166	223	58
52	334	138	151	224	63
53	330	139	148	225	77
54	316	140	189	226	70
55	317	141	168	227	82
56	328	142	153	228	71
57	296	143	187	229	63
58	315	144	175	230	54
59	313	145	175	231	49
60	329	146	177	232	55
61	281	147	158	233	56
62	292	148	163	234	43
63	310	149	179	235	47
64	310	150	140	236	53
65	325	151	143	237	70
66	310	152	137	238	63
67	308	153	157	239	63
68	291	154	154	240	63
69	310	155	160	241	53
70	246	156	146	242	55
71	290	157	131	243	52
72	268	158	143	244	57
73	274	159	156	245	46
74	299	160	138	246	45
75	304	161	129	247	45
76	280	162	118	248	51
77	248	163	140	249	56
78	273	164	141	250	48
79	279	165	136	251	44
80	265	166	133	252	49
81	254	167	118	253	47
82	261	168	136	254	57
83	248	169	108	255	49
84	266	170	112		
85	269	171	112		

Table 6: Pixel wise frequency with respect to grey value of the image obtained after applying RLT (on image shown in Figure 5)

Histogram of image grey value vs pixel frequency (using Table 4 above):

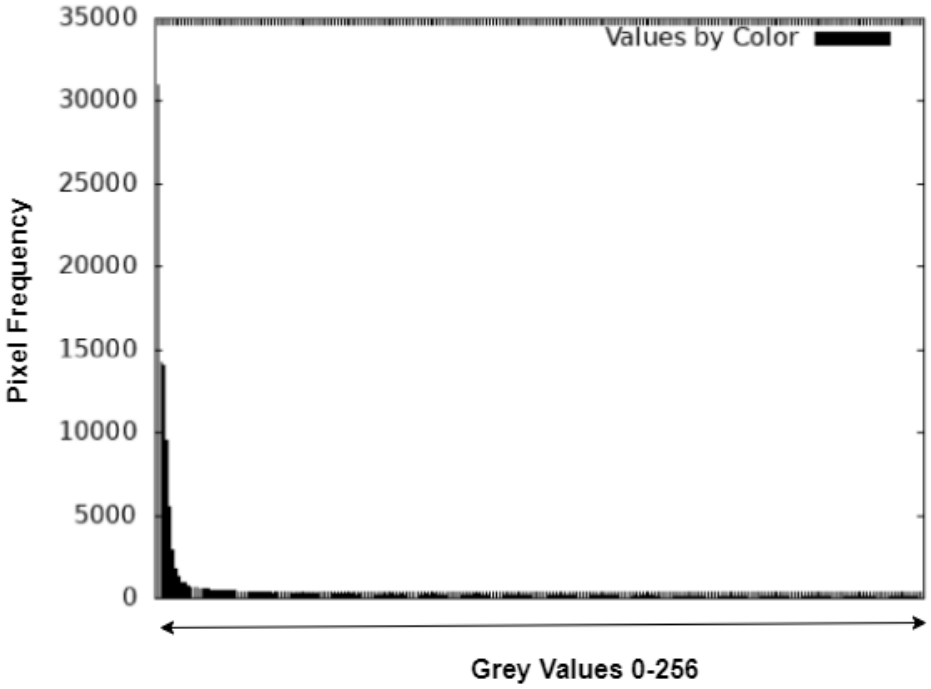


Figure 17. Histogram based on Table 4 values (of image obtained after applying RLT algorithm).

3.3 Features Extraction using RLT Algorithm (FV-USM Database)

Input Image and Image after applying Repeated Line Tracking (RLT) on Dr. Fendi database:

Input Finger Vein Image	Image after applying RLT on Input Image

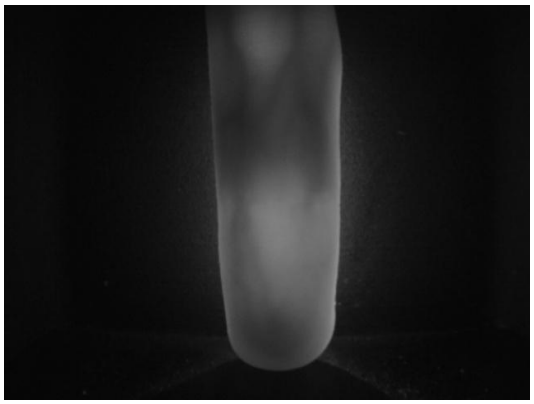
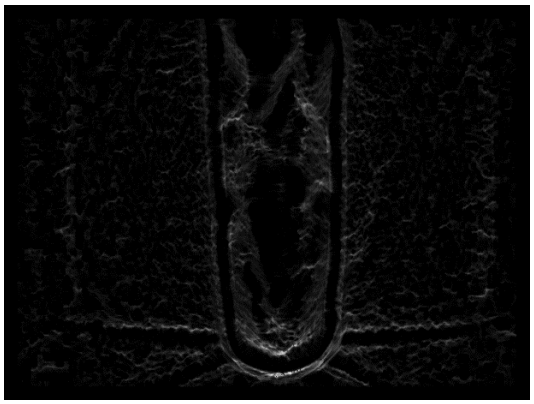

	

Figure 18. Input Image (Dr. Fendi database)	**Figure 19.** Output Image after applying RLT on the input image (Dr. Fendi Database)

Figure 20: Binarized image (Dr. Fendi Database) – Image Scaled to 2000*1326 Pixels

Pixel Sr. No.	Pixel Position	Grey Value	Pixel Sr. No.	Pixel Position	Grey Value
1	(0,0)	8	…..	…..	…..
2	(1,0)	8	…..	…..	…..
3	(2,0)	8	…..	…..	…..
4	(3,0)	8	…..	…..	…..
5	(4,0)	8	…..	…..	…..
6	(5,0)	8	…..	…..	…..
7	(6,0)	8	…..	…..	…..
8	(7,0)	8	…..	…..	…..
9	(8,0)	8	…..	…..	…..
10	(9,0)	8	…..	…..	…..
11	(10,0)	8	…..	…..	…..
12	(11,0)	8	…..	…..	…..
13	(12,0)	8	…..	…..	…..
14	(13,0)	8	…..	…..	…..
15	(14,0)	8	…..	…..	…..
16	(15,0)	8	…..	…..	…..
17	(16,0)	8	…..	…..	…..
18	(17,0)	8	…..	…..	…..
19	(18,0)	8	…..	…..	…..
20	(19,0)	8	…..	…..	…..
21	(20,0)	8	…..	…..	…..
22	(21,0)	8	307190	(629,479)	7
23	(22,0)	8	307191	(630,479)	7
24	(23,0)	8	307192	(631,479)	7
25	(24,0)	8	307193	(632,479)	7
26	(25,0)	8	307194	(633,479)	7
27	(26,0)	8	307195	(634,479)	7
28	(27,0)	8	307196	(635,479)	7
29	(28,0)	8	307197	(636,479)	7
30	(29,0)	8	307198	(637,479)	7
31	(30,0)	8	307199	(638,479)	7
32	(31,0)	8	307200	(639,479)	7

Table 7: Raw Image Pixel Grey Values (Dr. Fendi Database)

Table 7 describe pixel intensity (grey value) of every pixel in the raw finger vein image from finger vein image database. Figure 18 is showing raw image from Dr. Fendi database and Figure 19 is showing image after applying Repeated Line Tracking (RLT) on the image from Dr. Fendi Database.

Grey Value Histogram (Dr. Fendi DB):

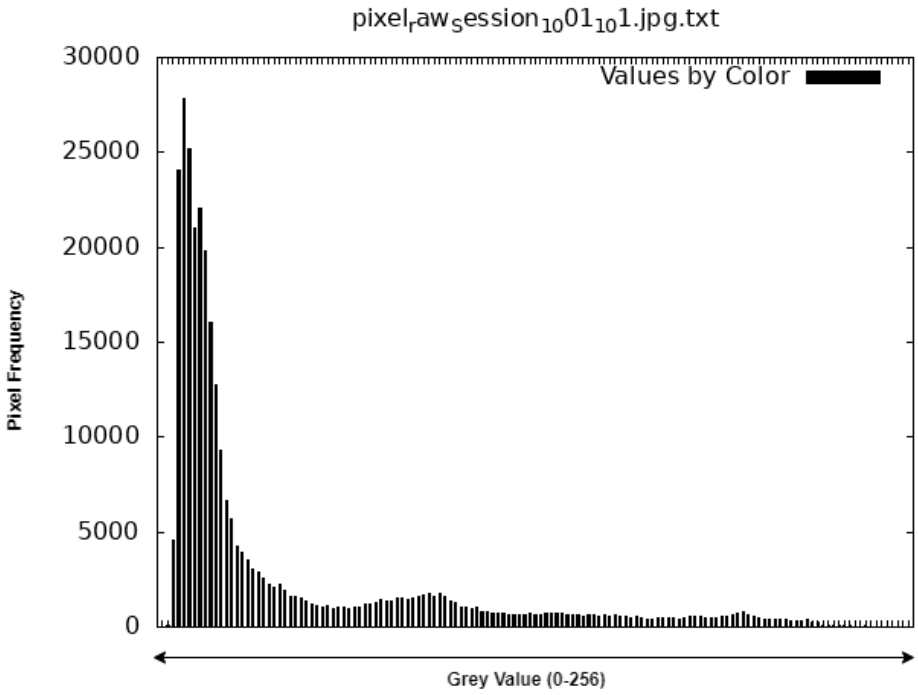


Figure 21. Histogram of the Input Image (from Dr Fendi database)

Histogram of the input image grey value is shown in Figure 18, which is showing grey values on x-axis and pixel frequency on y-axis.

Grey Value of some of pixels of RLT image (displayed in Figure 19 above):

Feature Coordinates	**Grey Value after applying RLT**	**Original Grey Value**	**Feature Coordinates**	**Grey Value after applying RLT**	**Original Grey Value**
(282,138)	158	34	(334,424)	204	43
(284,138)	179	34	(335,424)	196	43
(220,391)	160	12	(336,424)	229	44
(355,412)	187	54	(337,424)	203	44
(323,413)	158	43	(338,424)	181	44
(351,413)	191	52	(339,424)	163	45
(353,413)	227	53	(340,424)	167	45
(354,413)	234	53	(384,437)	177	19

(355,413)	176	54	(383,438)	156	18
(356,413)	163	55	(370,439)	181	19
(312,414)	160	44	(367,440)	159	18
(350,414)	188	52	(364,441)	228	18
(351,414)	165	52	(365,441)	184	18
(355,414)	193	54	(362,442)	177	17
(313,415)	198	44	(363,442)	225	16
(314,415)	193	44	(358,443)	179	16
(324,415)	165	41	(359,443)	232	16
(315,416)	172	44	(361,443)	187	16
(316,416)	233	43	(355,444)	188	15
(318,417)	248	43	(358,444)	246	15
(319,417)	193	43	(313,445)	190	13
(347,417)	191	49	(351,445)	200	16
(346,418)	202	48	(354,445)	241	14
(347,418)	162	49	(355,445)	200	14
(338,420)	158	45	(345,446)	193	14
(336,421)	166	44	(346,446)	230	14
(337,421)	201	45	(347,446)	243	14
(338,421)	224	45	(348,446)	255	14
(339,421)	177	45	(349,446)	253	15
(342,421)	247	46	(351,446)	185	15
(343,421)	185	46	(354,446)	191	15
(329,422)	156	42	(331,447)	164	13
(335,422)	159	44	(332,447)	225	13
(337,422)	172	44	(333,447)	206	13
(338,422)	199	45	(334,447)	205	13
(339,422)	196	45	(335,447)	174	13
(340,422)	203	45	(341,447)	174	14
(341,422)	208	46	(343,447)	173	14
(333,423)	157	44	(344,447)	176	16
(334,423)	156	44	(345,447)	169	15
(335,423)	173	44	(346,447)	199	15
(336,423)	178	44	(347,447)	215	15
(337,423)	175	44	(348,447)	242	15
(338,423)	200	44	(349,447)	235	14
(339,423)	207	45	(350,447)	176	14
(340,423)	170	45	(321,448)	164	13
(341,423)	199	46	(322,448)	168	13
(333,424)	178	43	(325,448)	164	13

Table 8: Grey Value of some of pixels of RLT image (Dr. Fendi Database)

Pixel wise frequency of grey value of raw image as shown in Figure 18:

4	5	51	1513	98	484
5	109	52	1571	99	465
6	4609	53	1686	100	508
7	24062	54	1754	101	434
8	27864	55	1632	102	491
9	25207	56	1759	103	545
10	20980	57	1574	104	554
11	22083	58	1340	105	556
12	19790	59	1318	106	469
13	16003	60	1067	107	493
14	12765	61	1035	108	516
15	9267	62	942	109	558
16	6651	63	1019	110	527
17	5657	64	835	111	658
18	4254	65	810	112	728
19	3914	66	692	113	830
20	3493	67	686	114	667
21	3087	68	762	115	595
22	2883	69	651	116	471
23	2560	70	647	117	402
24	2208	71	671	118	413
25	2067	72	645	119	366
26	2253	73	684	120	424
27	1915	74	602	121	385
28	1602	75	666	122	349
29	1583	76	702	123	301
30	1484	77	692	124	352
31	1372	78	729	125	420
32	1243	79	700	126	280
33	1088	80	614	127	228
34	1056	81	642	128	114
35	1091	82	652	129	55
36	999	83	600	130	57
37	1017	84	602	131	71
38	1080	85	680	132	65
39	943	86	596	133	47
40	1010	87	675	134	40
41	1037	88	596	135	34
42	1170	89	650	136	42
43	1175	90	594	137	28
44	1294	91	530	138	33
45	1454	92	507	139	29
46	1348	93	525	140	12
47	1374	94	465	141	4
48	1489	95	408	142	3
49	1500	96	385	144	1
50	1446	97	449	146	1

Table 9: Pixel wise frequency with respect to grey value of the image obtained after applying RLT (image shown in Figure 19)

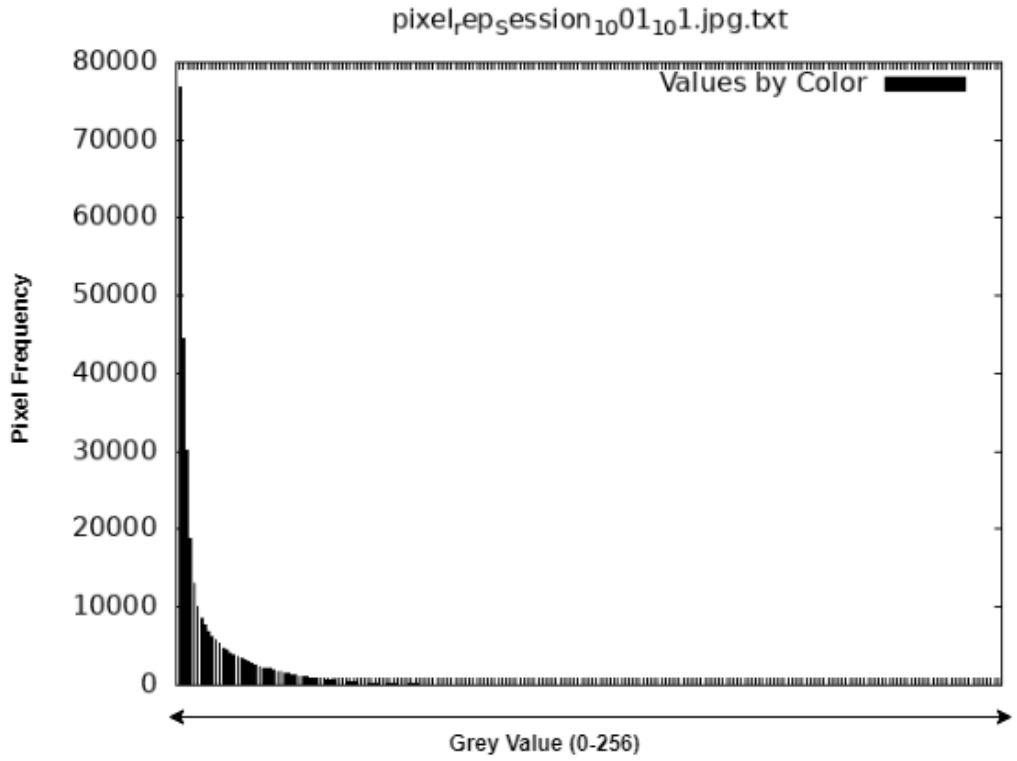


Figure 22. Histogram based on Table 6 values (of image obtained after applying RLT algorithm).

3.4 Cancelability on Features Extracted using RLT

3.4.1 Fingerprint template protection using multiline neighbouring relation

Biometric template protection schemes are:

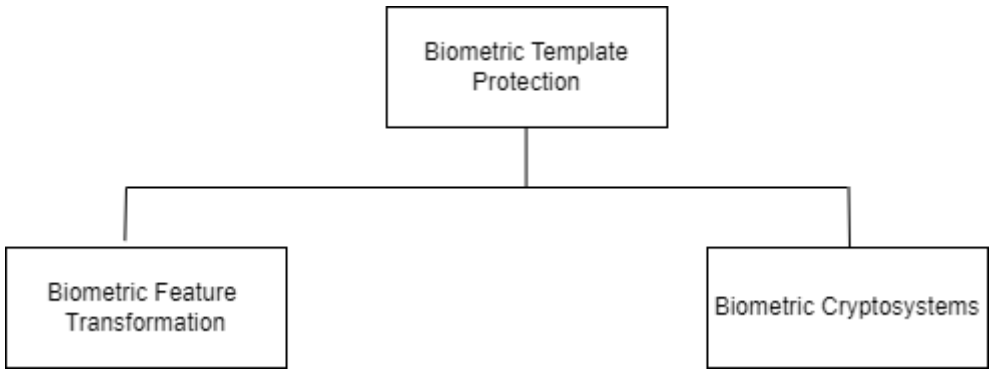


Figure 23: Biometric Template Protection Classification

Biometric feature transformation is referred as cancellable biometrics. A systematic transformation is applied to biometric data, resulting in the generation of a transformed template known as a cancellable template.

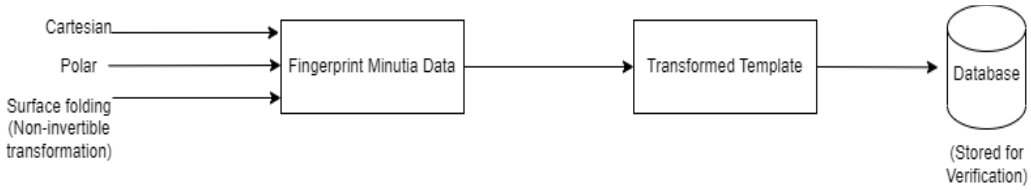


Figure 24: Fingerprint template protection process.

If an enrolled cancellable template is compromised, it will be replaced with a new transformed template. The primary objectives of cancellable biometric template design are as follows:

- Irreversible
- Accuracy
- Diversity
- Revocability

Irreversibility: Ensure that it is computationally impossible to retrieve the original template from the transformed template.

Accuracy: Maintain a consistent recognition rate between the transformed template and the original template.

Diversity: Enable the generation of multiple unique transformed templates from a single original template.

Revocability: Allow for the generation of a new and distinct template from the same fingerprint impression if the enrolled template is compromised.

Multiline neighbouring relation method deals with neighbourhood relationship around minutia. High level steps involved in multiline neighbouring relation method are:

- Draw “M” number of rectangles around every reference minutia.
- Select the minutia which fall in the rectangles and calculate the distance and orientation angle of the minutia.
- The invariant distance and orientation (calculated above) is called neighbouring relationship.
- This neighbouring relation is projected on a plane to generate a fixed length bit string.

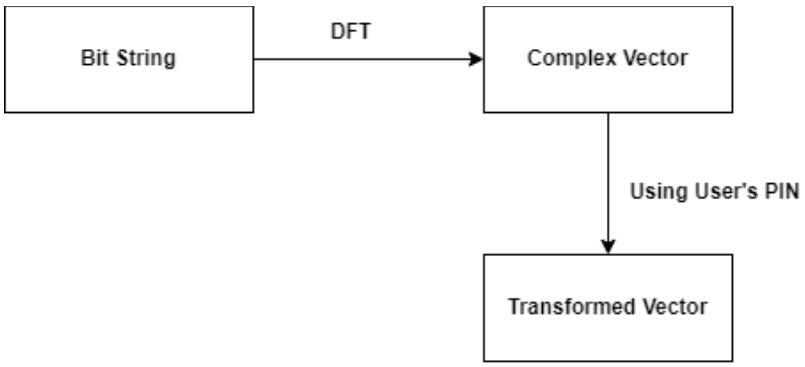


Figure 25: Bit String and Transformed Vector Generation

Multiline Neighbouring Method:

This consists of following steps:

- Multiline neighbouring relation generation.
- Plane based quantization and bit string generation.
- Cancelable template generation
- Matching

Multiline neighbouring relation generation:

Extract the minutia from fingerprint impression.

Suppose minutiae set is N_i. Let us suppose, we have 9 features (minutiae) extracted from fingerprint,

So, k=9 (No. of minutiae in the fingerprint)

Now, minutiae set N_i is represented as:

$$\begin{bmatrix} (x_1, y_1, \theta_1) & (x_2, y_2, \theta_2) & (x_3, y_3, \theta_3) \\ (x_2, y_1, \theta_4) & (x_2, y_2, \theta_5) & (x_2, y_3, \theta_6) \\ (x_3, y_1, \theta_7) & (x_3, y_2, \theta_8) & (x_3, y_3, \theta_9) \end{bmatrix}$$

Figure 26: Minutiae set representation

Out of the minutiae set, select any one minutiae which can be called as reference minutiae. It is denoted as (x_r, y_r, θ_r)

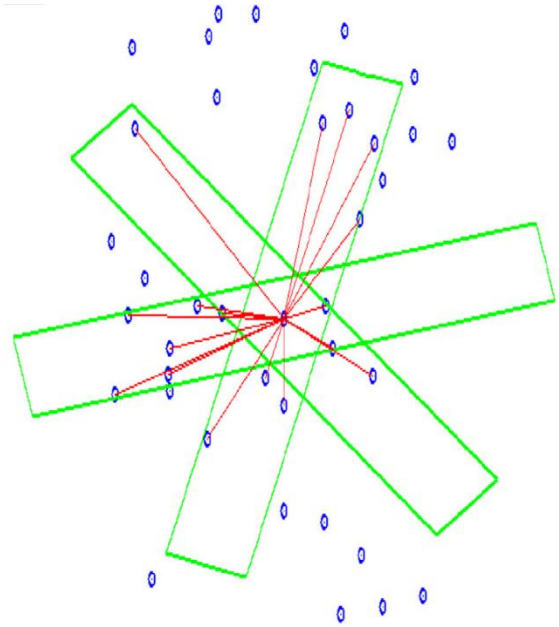


Figure 27: M rectangles with different orientation around reference minutiae.

Construct M no. of rectangles (in our case, M=3 as there are 3 rectangles) around the reference minutiae, reference point will be in center (x_r,y_r).

Length of rectangle = l

Width of rectangle = w

Orientation of rectangles are:

$$\theta_r, \theta_r + \frac{\pi}{M}, \theta_r + \frac{2\pi}{M}, \ldots\ldots, \theta_r + \frac{(M-1)\pi}{M}$$

In our case, M=3. So, orientation of rectangles are

$$\theta_r,\ \theta_r + \pi/3_+,\ \theta_r + 2\pi/3$$

Now, select the minutiae which fall in every rectangle constructed around reference minutiae.

The selected minutia (common in all rectangles), distance and orientation angle to calculate from reference minutiae.

For explanation,

$$\chi = (x_j - x_r)\cos\theta_r + (y_j - y_r)\sin\theta_r$$
$$\gamma = (x_j - x_r)\sin\theta_r - (y_r - y_r)\cos\theta_r$$

χ and Υ are the horizontal and vertical directions on a coordinate plane

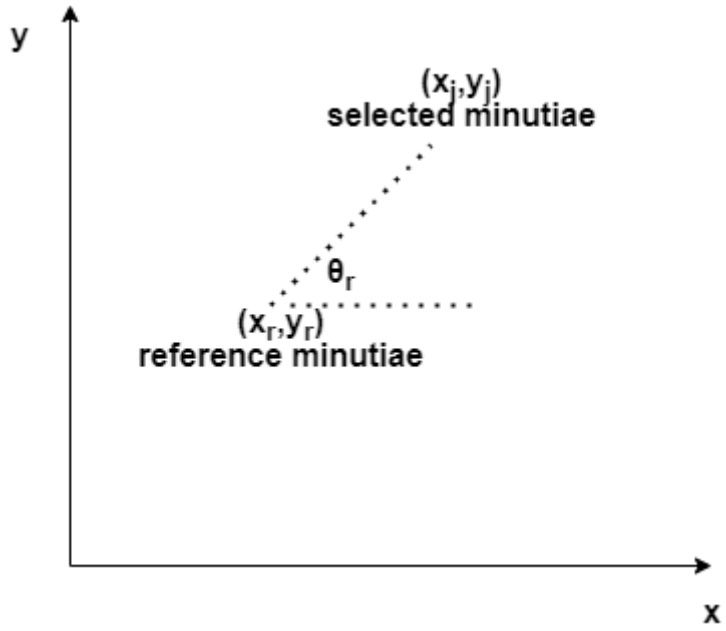


Figure 28: Distance and Orientation between reference minutiae and selected minutiae.

$$\chi^2 + \Upsilon^2 = r^2$$

here, $r=d_{ij}$

So, we can rewrite it as

$$d_{ij} = \sqrt{\chi^2 + \gamma^2}$$

and

$$\theta_{ij} = \begin{cases} \theta_j - \theta r & \text{if } \theta_j > \theta r \\ \theta_j - \theta_r + 360 & \text{Otherwise} \end{cases}$$

d_{ij} means distance from reference minutiae to i^{th} minutiae in the j^{th} rectangle.

and

Θ_{ij} means angle of i^{th} minutiae in j^{th} rectangle.

m, n, o = no. of minutiae which fall in 1^{st}, 2^{nd} and M^{th} rectangle

For understanding purpose, we have 3 rectangles, so

m = number of minutiae points in 1^{st} rectangle.

n = number of minutiae points in 2^{nd} rectangle.

O= number of minutiae points in 3^{rd} rectangle.

Distance and minutiae orientation calculated is called as multiline neighbouring relation around reference minutiae.

Multiline neighbouring relation is represented as L_r (in vector form).

e.g., for first rectangle

$L_r = \{[d_{11}, \Theta_{11}], [d_{21}, \Theta_{21}], [d_{31}, \Theta_{31}], \ldots\ldots\ldots\ldots, [d_{m1}, \Theta_{m1}]\}$

$L_1 = \{[d_{11}, \Theta_{11}], [d_{21}, \Theta_{21}], [d_{31}, \Theta_{31}]\}$

To understand the concept, suppose

m = 3

n = 2

o = 4

It means, in 1st rectangle, there are three minutiae (referred as m),

in 2nd rectangle, there are two minutiae (referred as n) and

in 3rd rectangle, there are four minutiae (referred as o)

It means that $[d_{11}, \Theta_{11}]$ belongs to rectangle 1

and d_{11} means distance from reference minutiae to 1st minutiae in rectangle 1.

Similarly, Θ_{11} means orientation angle of 1st minutiae in 1st rectangle.

Multiline neighbouring relation for 2nd rectangle can be represented as

$L_2 = \{[d_{12}, \Theta_{11}], [d_{22}, \Theta_{22}]\}$

Similarly,

$L_3 = \{[d_{13}, \Theta_{13}], [d_{23}, \Theta_{23}], [d_{33}, \Theta_{33}], [d_{43}, \Theta_{43}]\}$

Multiline neighbouring relation around a particular reference point can be represented as:

$L_r = \{L_1, L_2, L_3\}$

In similar manner, change reference minutiae and calculate multiline neighbouring relation vector for ever minutiae.

The fingerprint template will contain all multiline neighbouring relations generated using every reference minutia. This can be represented as:

$L = \{L_r, L_v, L_{f,} \ldots\ldots\ldots\ldots L_g\}$

Where r,v,f….., g are different reference minutiae.

We store distance of minutiae and orientation in vector L; which is a reference minutiae in a given triangle.

Plane Based Quantization and Bit String Generation:

As explained in previous section,

L_r is represented as a 2-D vector.

L= {L1, L2, L3} (in our example, for understanding purpose)

Technically, $L_r = \{d_{ij}, \Theta_{33}\}$

Suppose, $L_r = \{[d_{13}, \Theta_{13}], [d_{23}, \Theta_{23}], [d_{33}, \Theta_{33}], [d_{43}, \Theta_{43}]\}$

(The L_r is for 3rd rectangle)

Plot this vector L_r on plane

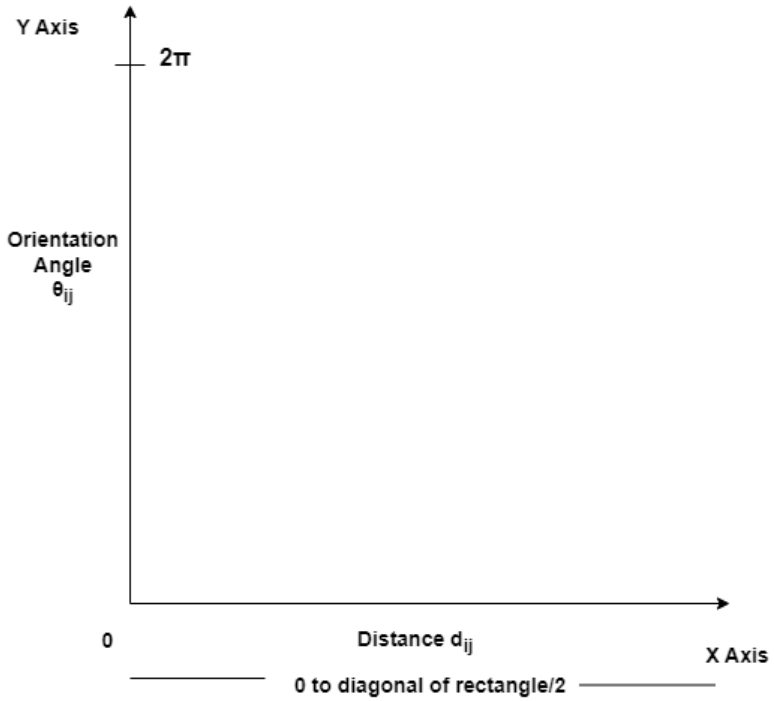


Figure 29: Plane Based Quantization

In our example, we are taking 3rd rectangle and for understanding purpose, suppose diagonal of rectangle is 12.

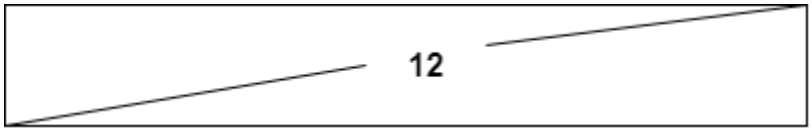


Figure 30: Rectangle Diagonal Illustration

Now, vector L_r is quantized on the plane

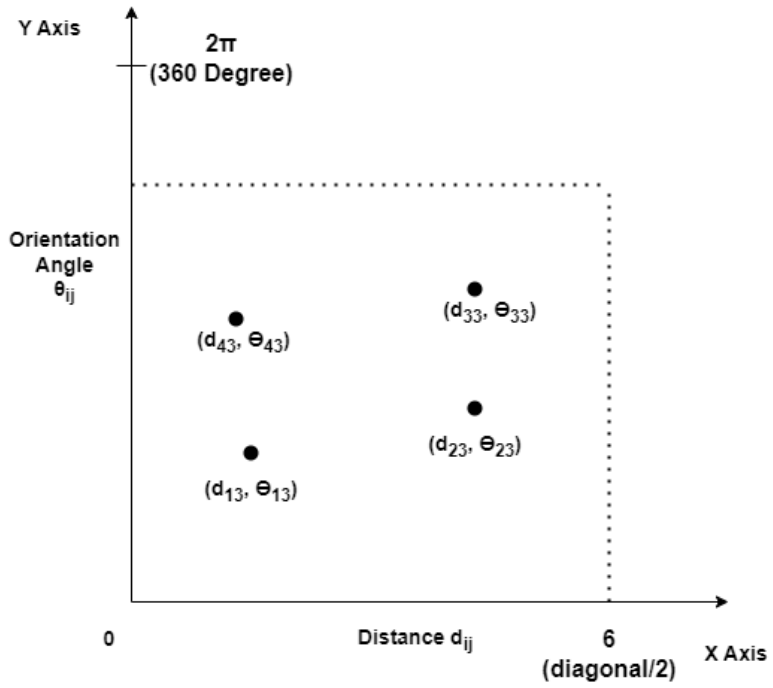


Figure 31: Quantized Vector L_r on the plane

Now, the quantized plane looks like

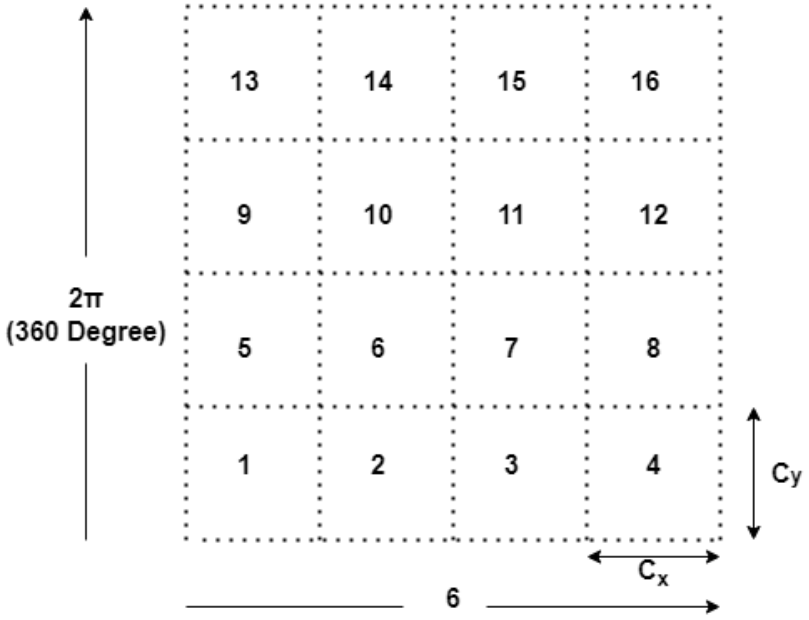


Figure 32: Cell wise quantized plane

On x-axis, 6 represents "length of diagonal of rectangle/2" whereas y axis represents orientation angle.

Divide the plane into cells, cells have size C_x,C_y

U= No. of Cells (Horizontal) = $6/C_x$

V= No. of Cells (Vertical) = $2\pi/C_y$

Now, the locate minutiae of L_r plane to check which minutiae falls in which cell.

To understand the concept, lets understand it in detail and consider:

L_3= {[d_{13}, Θ_{13}], [d_{23}, Θ_{23}], [d_{33}, Θ_{33}], [d_{43}, Θ_{43}]}

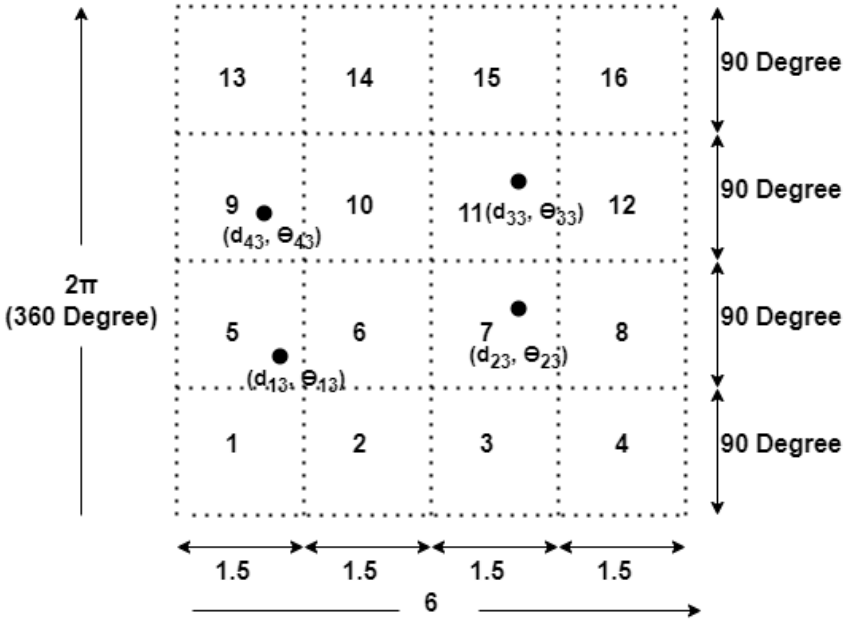


Figure 33: Cell wise minutiae location in quantized plane

For understanding purpose, suppose:

d_{13}=2, d_{23}=3, d_{33}=4.2, d_{43}=5.5 and

Θ_{13}=80, Θ_{23}=130, Θ_{33}=250, Θ_{43}=320

The above plane is represented as x & y axis instead of (d_{ij} & Θ_{ij})

So, corresponding x value and y value can be calculated using formula

$\chi_i=d_{ij}/c_x$

$\Upsilon_i= \Theta_{ij}/c_y$

Considering four coordinates on plane, four χ and Υ are calculated from four d_{ij} and Θ_{ij}.

Therefore,

$\chi_1=d_{13}/c_x$

i.e., 2/1.5 = 1.33

$\Upsilon_1= \Theta_{13}/c_y$

i.e., 80/90 = 0.88

Similarly,

$\chi_2=d_{23}/c_x$

i.e., 3/1.5 = 2

$\Upsilon_2 = \Theta_{23}/c_y$

i.e., 130/90 = 1.44,

$\chi_3 = d_{33}/c_x$

i.e., 4.2/1.5 = 2.8

$\Upsilon_3 = \Theta_{33}/c_y$

i.e., 250/90 = 2.77,

$\chi_4 = d_{43}/c_x$

i.e., 5.5/1.5 = 3.66

$\Upsilon_3 = \Theta_{43}/c_y$

i.e., 320/90 = 3.55

The goal of quantization of plane is to represent vector in the from:

$\{[d_{13}, \Theta_{13}], [d_{23}, \Theta_{23}], [d_{33}, \Theta_{33}], [d_{43}, \Theta_{43}]\}$

to quantized vector

$\{[\chi_1, \Upsilon_1], [\chi_2, \Upsilon_2], [\chi_3, \Upsilon_3], [\chi_4, \Upsilon_4]\}$

To understand the concept,

Vector L_r {(2,80), (3,130), (4.2,250), (5.5,320)}

is represented in quantized form as:

{(1.33,0.88), (2,1.44), (2.8,2.77), (3.66,3.55)}

Now, 1 D (one dimensional) bit string is generated.

As number of cells in quantized plane are 16, so 1D bit string (H_w).

It implies that:

H_w = {contains values equal to no. of cells in quantized plane}

Initially, H_w is represented as

H_w = {- - - - - - - - - - - - - - - -}

It denotes null value initially and "- "represents no. of cells (16 in this case).

Every cell in the plane is visited sequentially. If a cell has more than one (x_i,y_i) , value of cell (bit) in H_w is set to 1 else value is set to 0.

On applying above logic, finally binary string (H_w) looks like:

H_w = {0,0,0,0,0,1,0,0,0,0,0,0,0,0,0,0}

Binary string H_w is referred as one dimensional (1-D) bit string.

Note: Number of bits in the bit string (H_w)

B=U*V (i.e., no. of cells in the plane)

Cancelable Template Generation

If bit string is compromised, the vector L_r can be revealed.

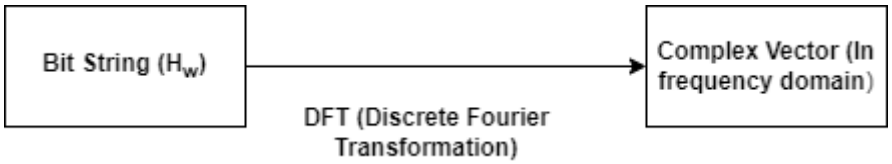


Figure 34: Bit String to Complex Vector Transformation using DFT

$$D_i = \sum_{w=0}^{B-1} H_w e^{-j2\pi iw/B}, \quad i = 0, 1, \ldots, B-1$$

D_i is called B-Point Discrete Fourier Transformation on H_w

Now, complex vector D = $[D_0, D_1, \ldots\ldots\ldots, D_{B-1}]^T$

To secure complex vector D, generate a user specific random matrix (R) using a user's pin.

R=p*q

Q=B (size of bit string i.e., U*V; which is number of cells in the plane)

P<q

T=Resulting vector of size p*1 transformed complex vector

Transformation is given by

RD=T

For verification,

Same random matrix (R) can be generated using same user's PIN which is used for enrolment of the user's fingerprint.

Perform step 2 (plane-based quantization and bit string generation) and step 3 (cancellable template generation) for all remaining vectors in L.

After performing the bit string and template generation for all neighbouring relations

L= $\{L_1, L_2, L_3, L_4, \ldots\ldots\ldots\ldots, L_k\}$

k= number of minutiae in fingerprint.

Cancellable template contains 'k' number of transformed multiline neighbouring relations.

3.4.2 Concept of GAR (Genuine Acceptance Rate) and False Acceptance Rate (FAR)

GAR is Genuine Acceptance Rate and FAR is False Acceptance Rate. In the domain of biometrics, the Genuine Acceptance Rate (GAR) is a critical performance metric used to evaluate the accuracy and reliability of a biometric system. GAR represents the percentage of

genuine users who are correctly identified by the system as genuine. In other words, it measures the rate at which the biometric system correctly accepts and authenticates individuals who are indeed authorized to access the system.

To calculate the Genuine Acceptance Rate, the biometric system compares the biometric data of an individual (such as fingerprints, face, iris, voice, etc.) with the stored reference template associated with that individual. If the comparison result indicates a sufficiently high similarity score, the individual is deemed genuine, and the GAR is increased. If the similarity score falls below a predefined threshold, the individual is considered an imposter or unauthorized user, and the system should reject their access attempt.

GAR is an essential metric in assessing the effectiveness of biometric systems, especially in security-critical applications where accurate identification and authentication are crucial. Alongside GAR, biometric systems are also evaluated using other metrics such as False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (EER), and Receiver Operating Characteristic (ROC) curves to provide a comprehensive understanding of system performance.

It's important to note that achieving a high Genuine Acceptance Rate while keeping the False Acceptance Rate low is a key challenge in biometric system design. A balance must be struck between ease of use and security to ensure the system is both user-friendly and robust against imposters.

In summary, Genuine Acceptance Rate (GAR) is a critical performance measure in biometrics that quantifies the correct acceptance of genuine users by the system, making it a fundamental factor in evaluating the overall reliability and accuracy of biometric authentication systems.

The Genuine Acceptance Rate (GAR) in the field of biometrics is typically calculated using the following formula:

GAR = (Number of Genuine Matches / Number of Genuine Attempts) * 100

In this formula:

Number of Genuine Matches refers to the number of times the biometric system correctly identifies and accepts genuine users as genuine.

Number of Genuine Attempts refers to the total number of times genuine users attempt to access the system.

By dividing the Number of Genuine Matches by the Number of Genuine Attempts and then multiplying by 100, we get the Genuine Acceptance Rate expressed as a percentage.

The GAR is a critical performance metric used to evaluate the accuracy and reliability of a biometric system in correctly accepting genuine users. A higher GAR value indicates a more accurate and reliable system, as it correctly identifies genuine users with a higher success rate. It is essential to balance the GAR with the False Acceptance Rate (FAR) to ensure both accuracy and security in biometric authentication systems.

In the domain of biometrics, the False Acceptance Rate (FAR) is a significant performance metric used to assess the accuracy and security of a biometric system. FAR represents the percentage of imposters or unauthorized users who are incorrectly identified as genuine by the system. In other words, it measures the rate at which the biometric system mistakenly accepts individuals who should not be granted access.

To calculate the False Acceptance Rate, the biometric system compares the biometric data of an individual (such as fingerprints, face, iris, voice, etc.) with the stored reference template associated with that individual. If the comparison result indicates a similarity score that exceeds a predefined threshold, the individual is incorrectly recognized as genuine, and the FAR is increased. This means that the system mistakenly allows unauthorized users to access the system.

FAR is a critical factor in evaluating the security of biometric systems, particularly in applications where access control and identity verification are essential. A high FAR can pose serious security risks as it indicates that the system is vulnerable to imposters and unauthorized access.

To design an effective biometric system, it is crucial to find the right balance between the False Acceptance Rate (FAR) and the Genuine Acceptance Rate (GAR). Lowering the FAR to reduce security risks may inadvertently increase the False Rejection Rate (FRR), where genuine users are incorrectly rejected. Achieving a good trade-off between FAR and FRR is crucial to providing both accurate identification and robust security.

Biometric systems are often tuned by adjusting the threshold to optimize the FAR and FRR for specific applications. The goal is to minimize the FAR while still maintaining an acceptable level of user convenience and system usability.

In summary, False Acceptance Rate (FAR) is an essential performance measure in biometrics that quantifies the rate at which unauthorized users are incorrectly accepted by the system. It is a critical factor in evaluating the security of biometric authentication systems and plays a crucial role in achieving the right balance between accuracy and usability.

The False Acceptance Rate (FAR) in the field of biometrics is typically calculated using the following formula:

FAR = (Number of False Matches / Number of Impostor Attempts) * 100

In this formula:

Number of False Matches refers to the number of times the biometric system incorrectly identifies an imposter as a genuine user.

Number of Impostor Attempts refers to the total number of times imposters or unauthorized users attempt to access the system.

By dividing the Number of False Matches by the Number of Impostor Attempts and then multiplying by 100, we get the False Acceptance Rate expressed as a percentage.

The FAR is a critical performance metric used to evaluate the security of a biometric system in preventing imposters or unauthorized users from gaining access. A lower FAR value indicates a more secure system, as it correctly rejects imposters with a higher success rate. It is essential to balance the FAR with the Genuine Acceptance Rate (GAR) to ensure both security and accuracy in biometric authentication systems.

The curve between GAR and FAR denote the relationship between the two rates. Ideally GAR should be 1 which denotes that all the genuine scores are perfect match. In other words, a user's own fingers got matched with his/her finger features accurately an ideally FAR should be 0 which denotes that the false matches should be 0 and there should not be any false match allowed into the system. Typical ROC (receiver operating characteristics) characteristic where typical signal values, m5 > m4 > m3 > m2 > m1 are used and "m0" is assumed to be zero. The ideal characteristics would be GAR = 1 and FAR = 0 and the worst scenario, GAR = FAR which is diagonal solid line marked as "Worst Performance" in Fig. 35. It is observed that as

the signal value increases, the ROC curve shifts toward the ideal curve and the detection performance improves (https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-019-0089-z).

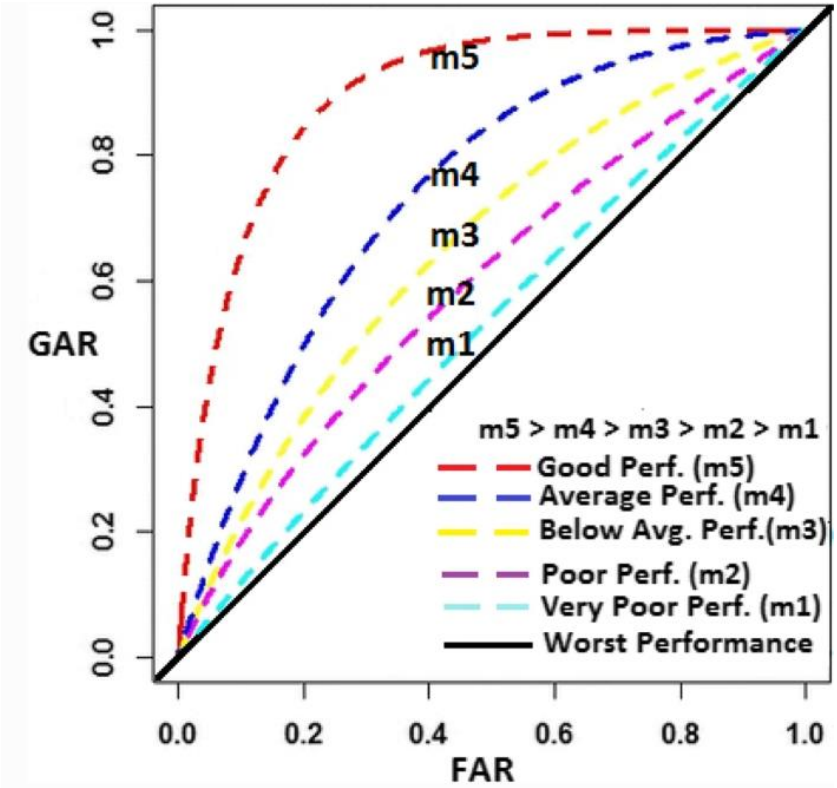


Figure 35: FAR and GAR Graph

The performance of a biometric system can be assessed using two metrics: false acceptance rate (FAR) and false rejection rate (FRR). FAR represents the probability of incorrectly accepting an authentication attempt by an impostor, while FRR represents the probability of incorrectly rejecting an authentication attempt by a genuine user. The values of FAR and FRR depend on the system's predetermined threshold. Another metric, the Equal Error Rate (EER), indicates the point where acceptance and rejection errors are equal (EER = FAR = FRR). A lower EER signifies higher accuracy in the biometric system.

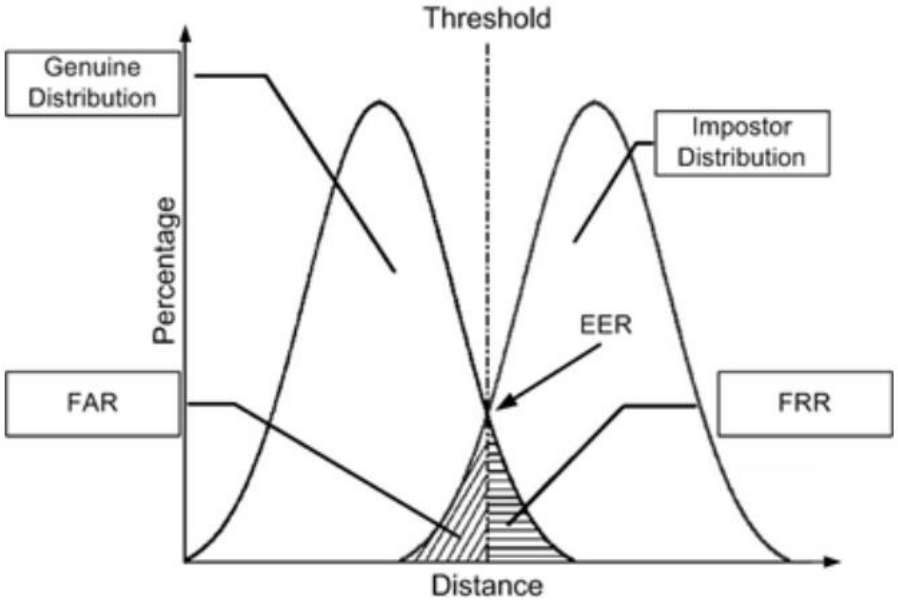


Figure 36: Genuine and impostor distributions as a function of distance between enrolment and authentication templates

Figure 36 provides a visual representation of the genuine and impostor distributions in a biometric system based on the distance between enrolled and authentication templates. Genuine users are associated with small distances, while impostors have larger distances. The overlapping area between the two distributions indicates instances where the system cannot distinguish between genuine users and impostors. The threshold value, shown in figure 36, is set at the point where the two curves intersect. This threshold divides the overlapping area into two sub-areas: the left sub-area represents the false acceptance rate (FAR), and the right sub-area represents the false rejection rate (FRR). The intersection point defines the Equal Error Rate (EER), where FAR and FRR are equal (EER = FAR = FRR). A biometric system performs optimally when there is no overlap between the genuine and impostor curves, resulting in FAR and FRR values of 0. Conversely, as the overlapping area increases, the authentication performance deteriorates.

3.4.3 Calculation of EER and DPRIME Value on Different Finger vein Databases

3.4.3.1 University of Twente:

The University of Twente Finger Vein Pattern (UTVP) dataset consists of 1440 finger vascular pattern images obtained from 60 volunteers at the university during the 2011-2012 academic year. The images were captured in two sessions with an average time-lapse of 15 days. Each session involved capturing the vascular pattern of the index, ring, and middle fingers of both

hands, resulting in four captures for each finger. The images have a resolution of 672 × 380 pixels and a pixel density of 126 pixels per centimetre (ppcm). They are stored in the lossless 8-bit greyscale Portable Network Graphics (PNG) format. Approximately 73% of the data subjects are male, and 87% are right-handed. The dataset primarily represents a young population, with 82% of the subjects falling in the age range of 19-30 years. Sample images from the dataset are shown in Figure 37. While the quality of the captured images may vary among subjects, there is minimal variation within the images from the same subject.

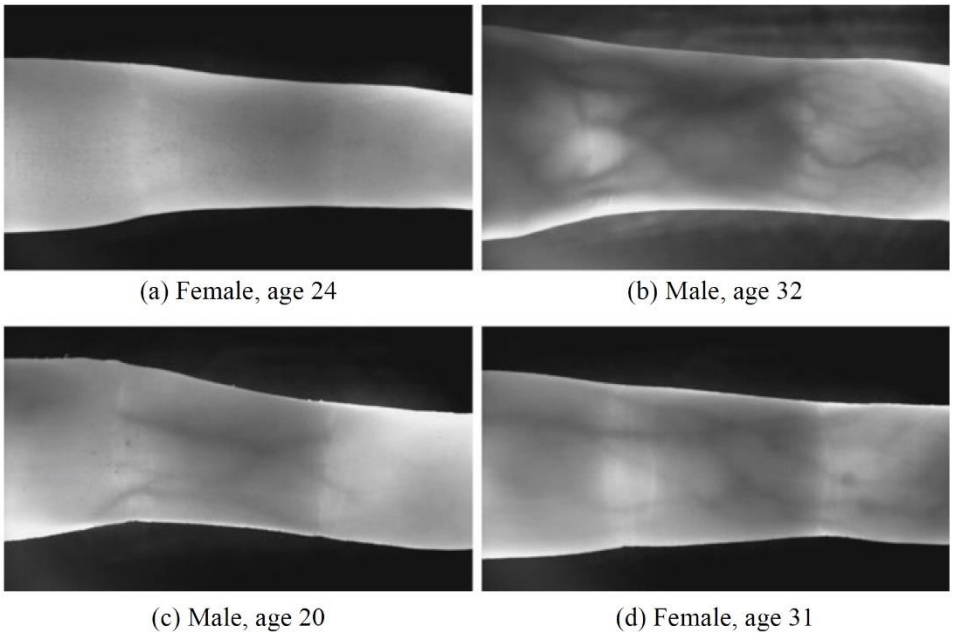


Figure 37: Sample images of the left-hand ring finger from the collected dataset. (University of Twente Finger Vein Pattern (UTVP) dataset)

The width of the visible blood vessels ranges from 4–20 pixels which, using a pixel density of 126 pixels per centimetre, corresponds to vessel widths of approximately 0.3–1.6 mm. The pixel density was determined by placing a piece of flat graph paper at exactly the same position as the finger and counting the number of pixels per centimetre in the recorded image. This resulted in a pixel density of 126 pixels per centimetre.

On applying cancelability on finger vein features using multiline neighbouring relations, EER and DPRIME values are calculated using different keys. The values are listed in Table 10.

Key	EER	DPRIME	Template with Complex values
1400	0.0085	4.8481	1400*1
1700	0.0061	5.0012	1700*1
1100	0.0077	4.8818	1100*1

Table 10: University of Twente database EER and DPRIME Values based on different Keys

Sample Template for 1700 Key (After applying Cancelability)
-285.705779243688 - 65.1830063137017i
-709.469869794415 - 265.546707007000i
-357.854933446591 + 586.868021450045i
337.942862489556 - 523.681437517808i
132.291613837678 - 125.134150870527i
320.642731632355 + 54.0051882993646i
221.705928045422 - 205.353811077538i
481.298456261681 + 316.859336788364i
916.938865330447 + 416.567555271649i
-32.8347093265702 - 314.847471389331i

Table 11: Sample cancelability template using 1700 as key (UTVP Database)

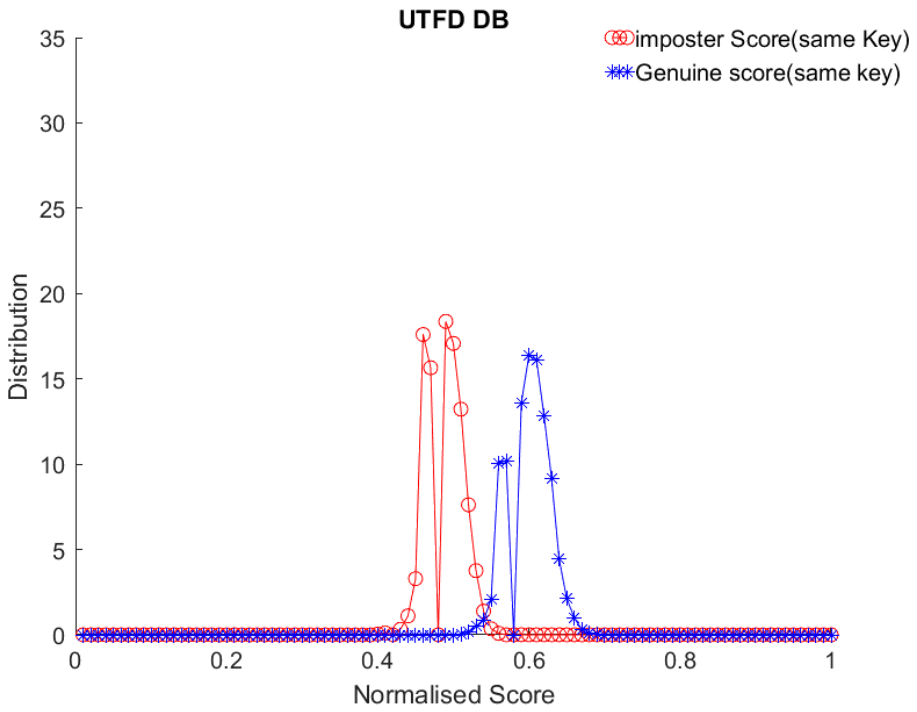


Figure 38: UTFD Distribution Curve 1100 (Imposter Score and Genuine Score)

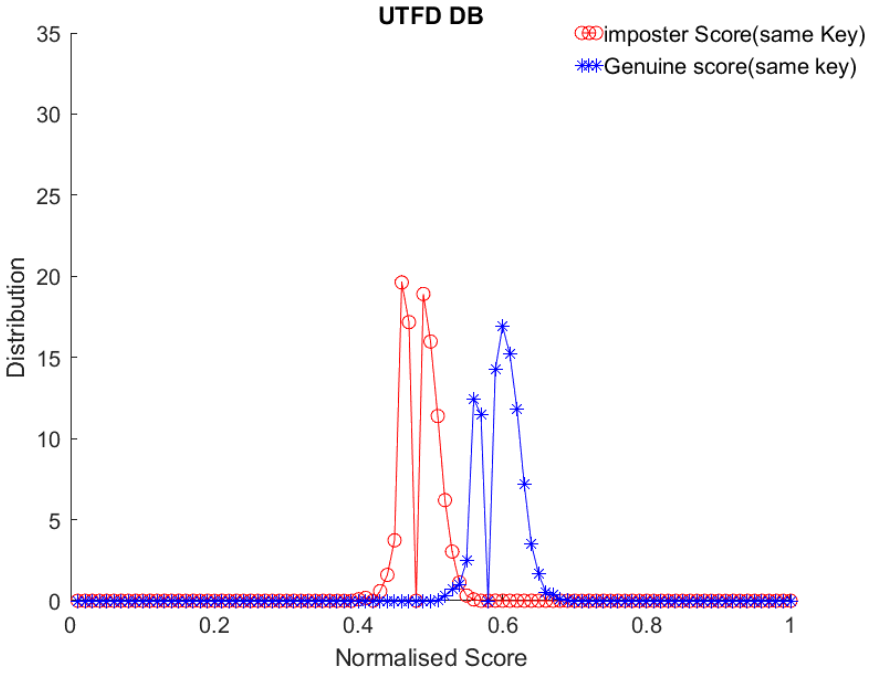


Figure 39: UTFD Distribution Curve 1400 (Imposter Score and Genuine Score)

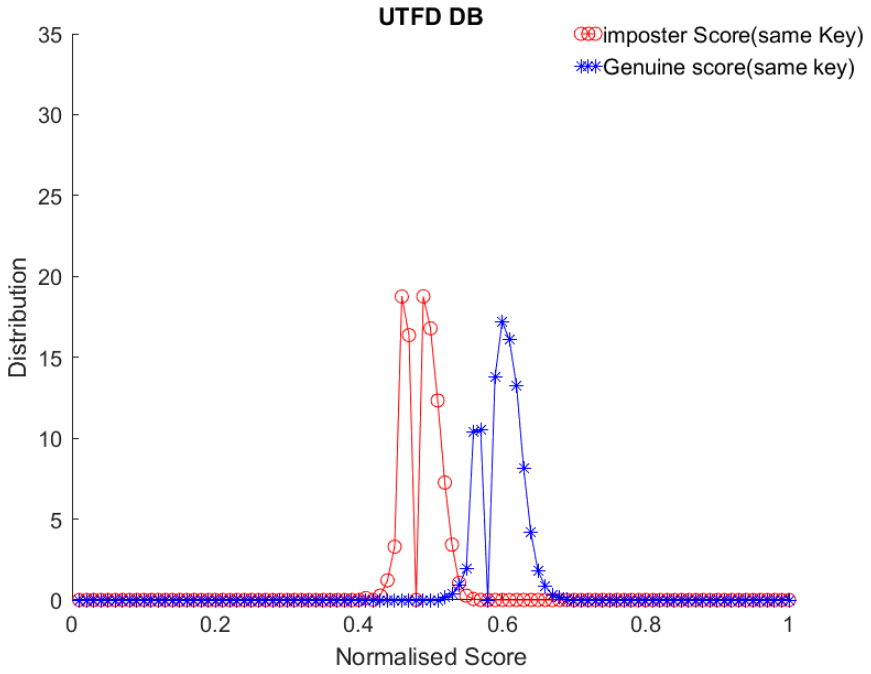


Figure 40: UTFD Distribution Curve 1700 (Imposter Score and Genuine Score)

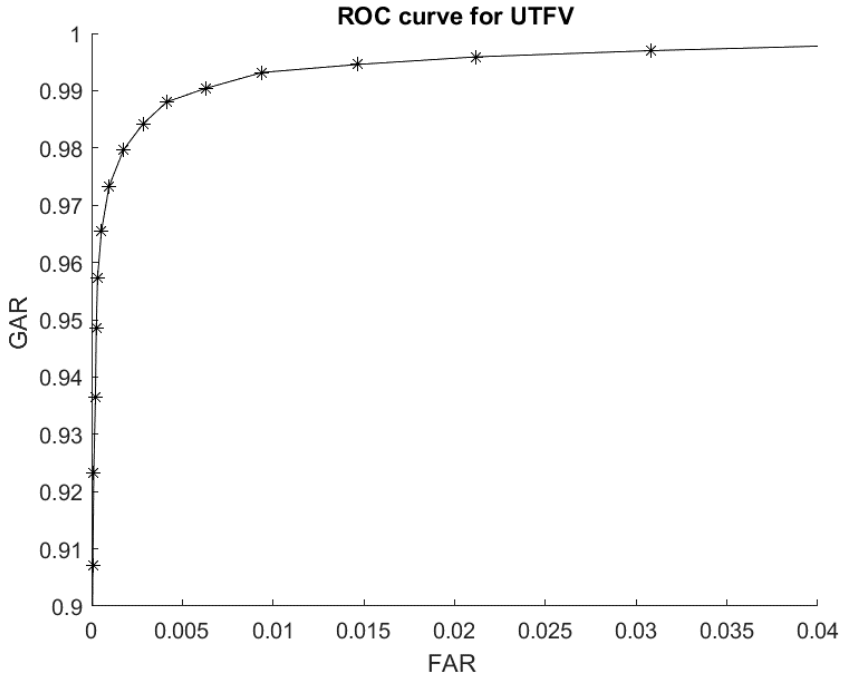


Figure 41: UTFD GAR FAR Curve with Key 1100

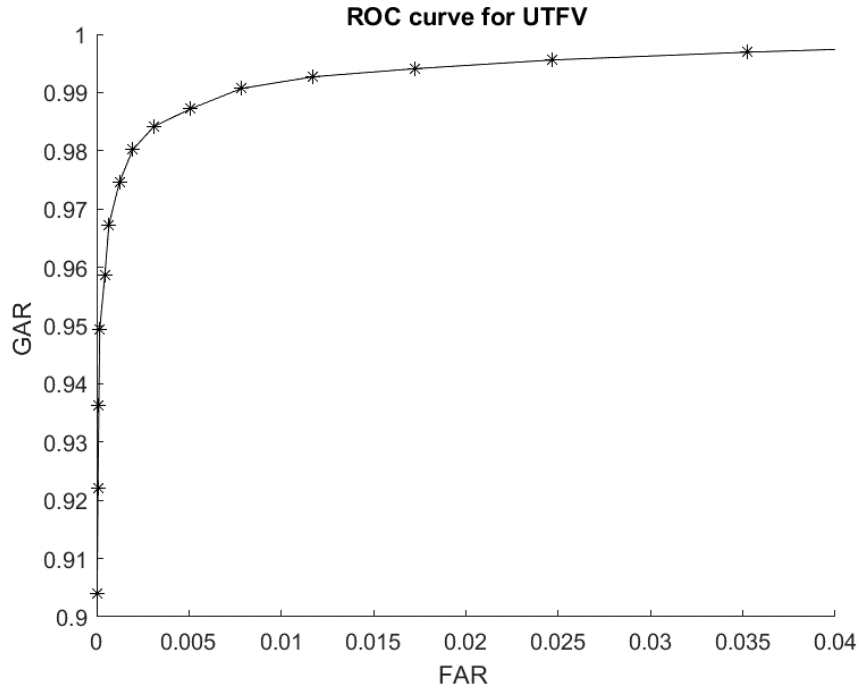


Figure 42: UTFD GAR FAR Curve with Key1400

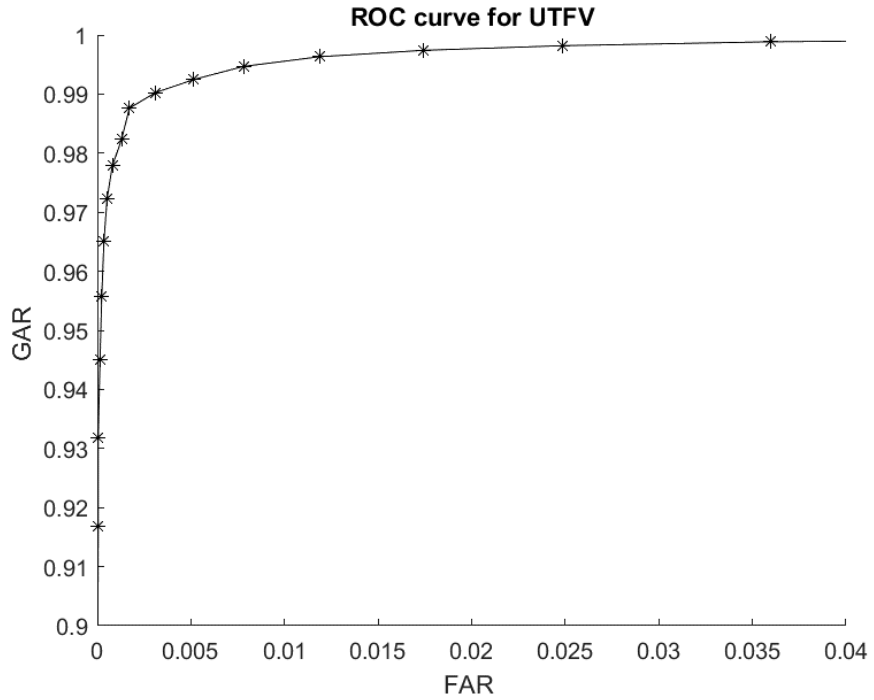


Figure 43: UTFD GAR FAR Curve with key1700

3.4.3.2 Hong Kong Polytechnic University Database:

We have extracted features from Hong Kong University finger vein image dataset in the required format (x axis y axis original grey value).

The image dataset description is:

The currently available database has 2520 images from the 105 subjects, all the images are in bitmap (*.bmp) format. In this dataset about 93% of the subjects are younger than 30 years. The finger images were acquired in two separate sessions with a minimum interval of one-month, maximum interval of over six months and the average interval of 66.8 days. In each session, each of the subjects provided 6 image samples from index finger middle finger respectively, and each sample consisted of one finger vein image and one finger texture image from the left hand. Therefore, each subject provided 24 images in one session.

Attaching corresponding features files for 2520 images.

Key	EER	DPRIME	Template with Complex values
1400	0.0557	3.1047	1400*1
1700	0.0532	3.1693	1700*1
1100	0.0512	3.1994	1100*1

Table 12: HKPU database EER and DPRIME Values based on different Keys

Sample Template for 1700 Key (After applying Cancelability)
-285.705779243688 - 65.1830063137017i
-709.469869794415 - 265.546707007000i
-357.854933446591 + 586.868021450045i
337.942862489556 - 523.681437517808i
132.291613837678 - 125.134150870527i
320.642731632355 + 54.0051882993646i
221.705928045422 - 205.353811077538i
481.298456261681 + 316.859336788364i
916.938865330447 + 416.567555271649i
-32.8347093265702 - 314.847471389331i

Table 13: Sample cancelability template using 1700 as key (HKPU Database)

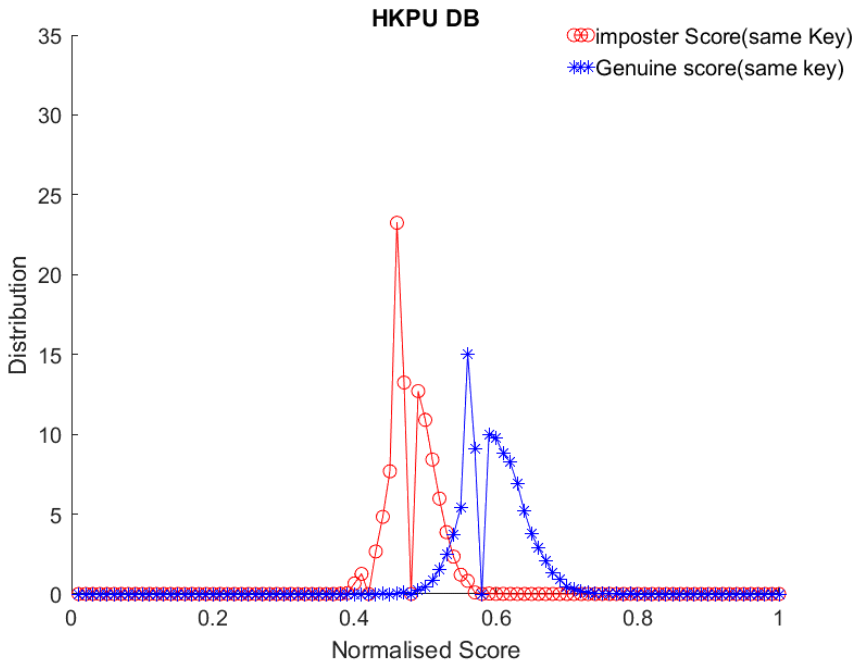


Figure 44: HKPU Distribution Curve 1100 (Imposter Score and Genuine Score)

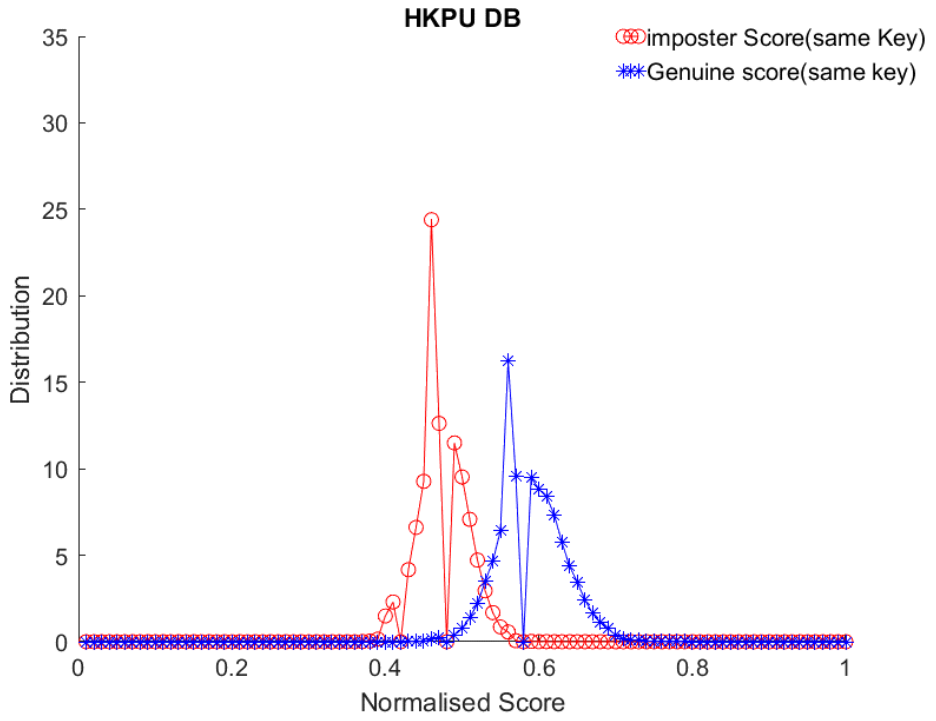


Figure 45: HKPU Distribution Curve 1400 (Imposter Score and Genuine Score)

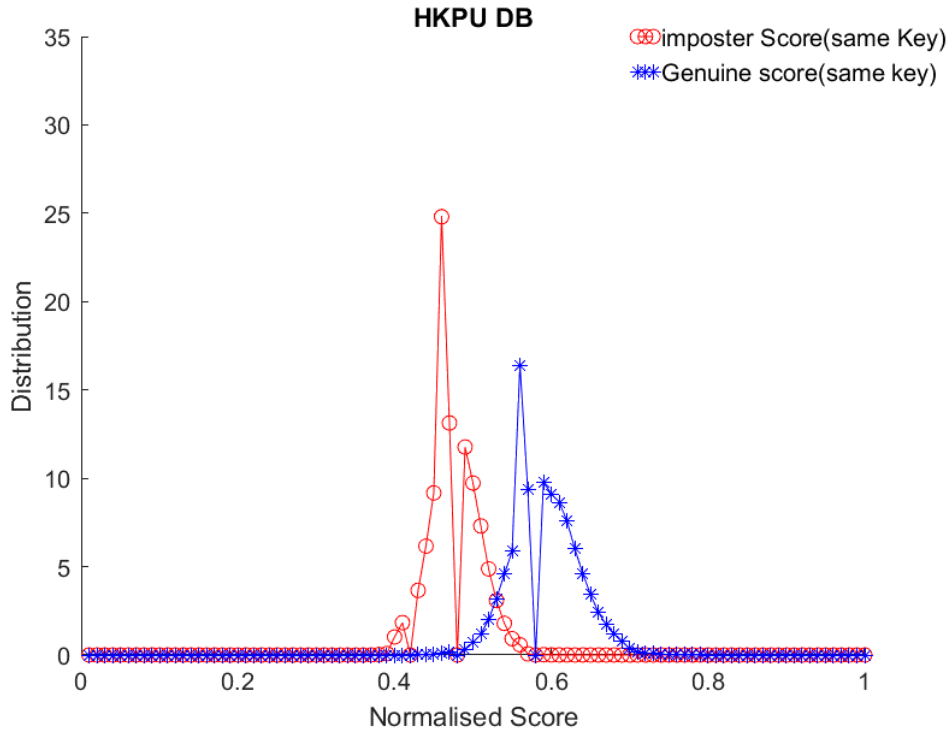


Figure 46: HKPU Distribution Curve 1700 (Imposter Score and Genuine Score)

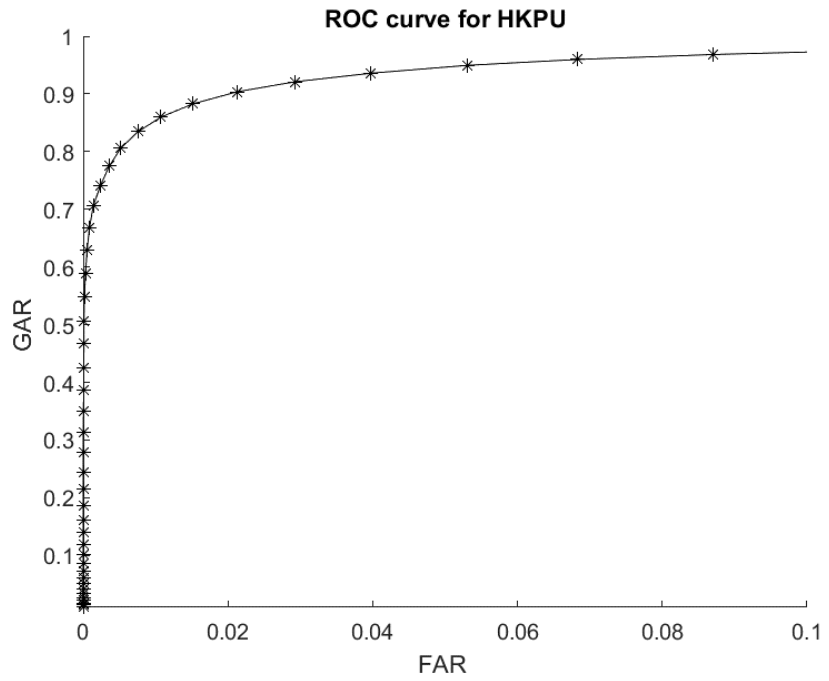


Figure 47: HKPU GAR FAR Curve with key 1100

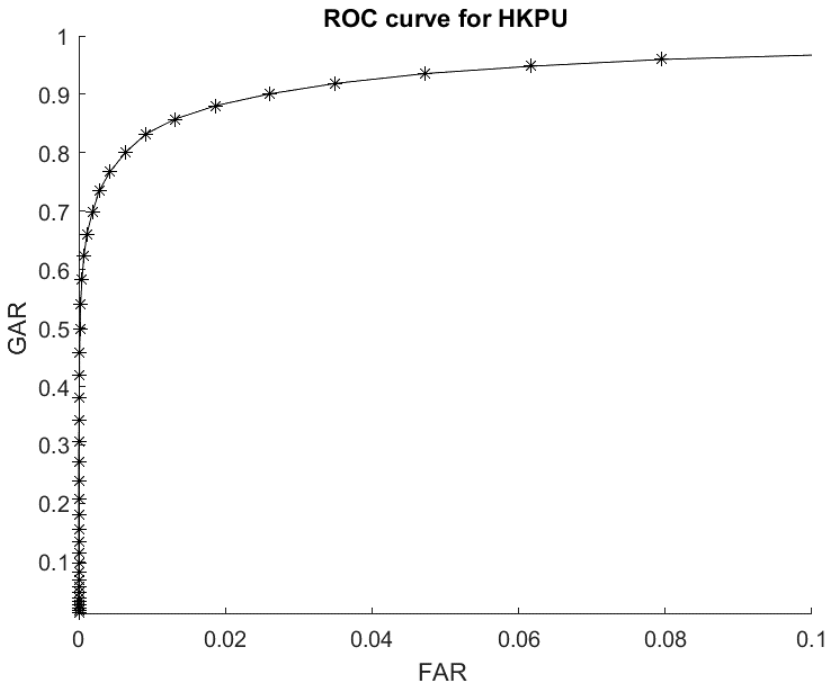


Figure 48: HKPU GAR FAR Curve with key 1400

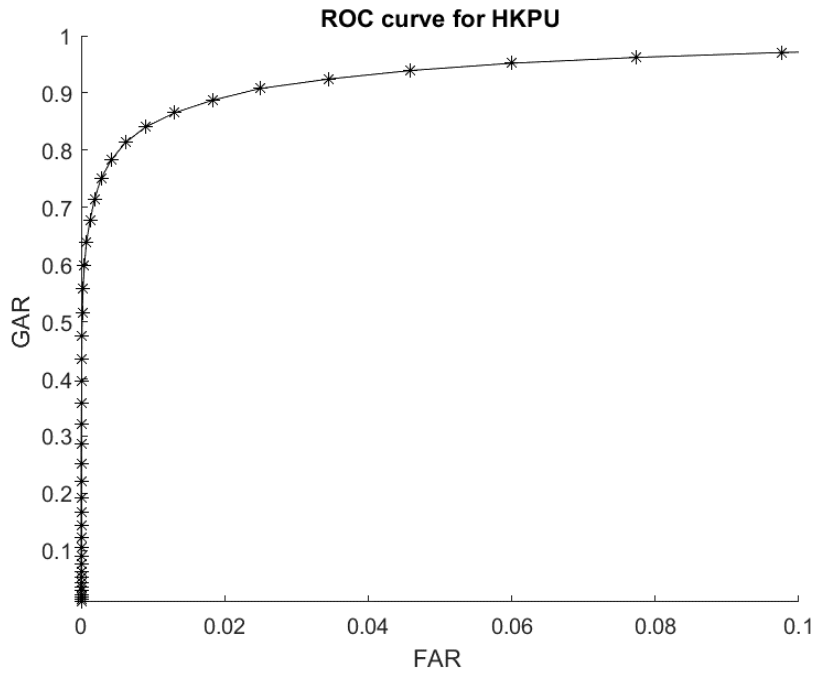


Figure 49: HKPU GAR FAR Curve with key 1700

3.4.3.3 Dr. Fendi Database:

We have extracted features from Dr. Fendi finger vein image dataset in the required format (x axis y axis original grey value).

The image dataset description is:

The study utilized a database consisting of images obtained from 123 volunteers, comprising 83 males and 40 females, who were staff and students of Universiti Sains Malaysia. The age of the participants ranged from 20 to 52 years. Each volunteer contributed four fingers (left index, left middle, right index, and right middle), resulting in a total of 492 finger classes. Six images were captured for each finger in one session, and each participant underwent two sessions with a gap of over two weeks. In the initial session, a total of 2952 images were collected (123 participants x 4 fingers x 6 images). Combining both sessions, a total of 5904 images from 492 finger classes were obtained. The captured finger images had a spatial resolution of 640 x 480 pixels and a depth resolution of 256 grey levels.

Key	EER	DPRIME	Template with Complex values
1400	0.2024	0.7174	1400*1
1700	0.201	0.7253	1700*1
1100	0.1987	0.7322	1100*1

Table 14: Dr. Fendi database EER and DPRIME Values based on different Keys

Sample Template for 1700 Key (After applying Cancelability)
-285.705779243688 - 65.1830063137017i
-709.469869794415 - 265.546707007000i
-357.854933446591 + 586.868021450045i
337.942862489556 - 523.681437517808i
132.291613837678 - 125.134150870527i
320.642731632355 + 54.0051882993646i
221.705928045422 - 205.353811077538i
481.298456261681 + 316.859336788364i
916.938865330447 + 416.567555271649i
-32.8347093265702 - 314.847471389331i

Table 15: Sample cancelability template using 1700 as key (Dr. Fendi Database)

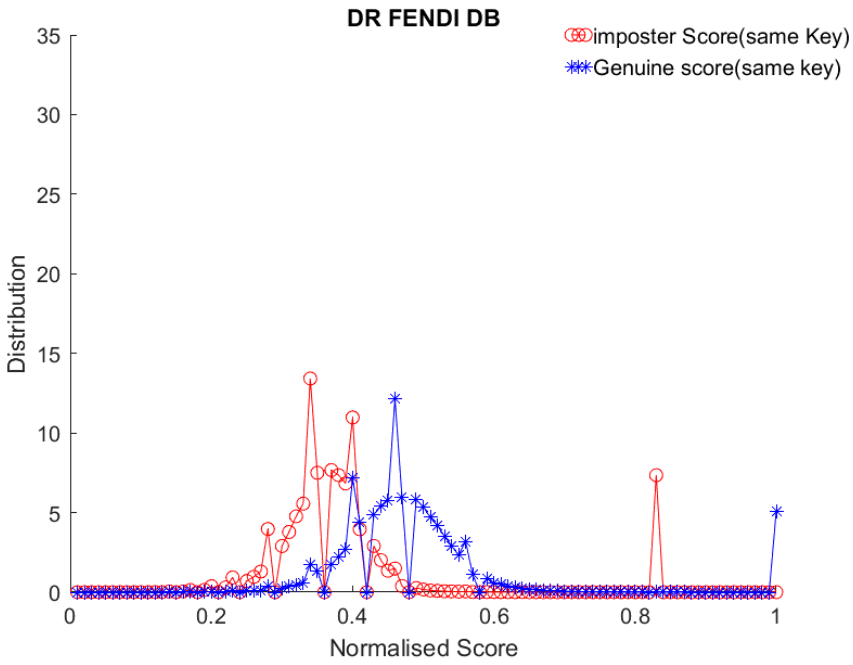


Figure 50: Dr Fendi Distribution Curve 1100 (Imposter Score and Genuine Score)

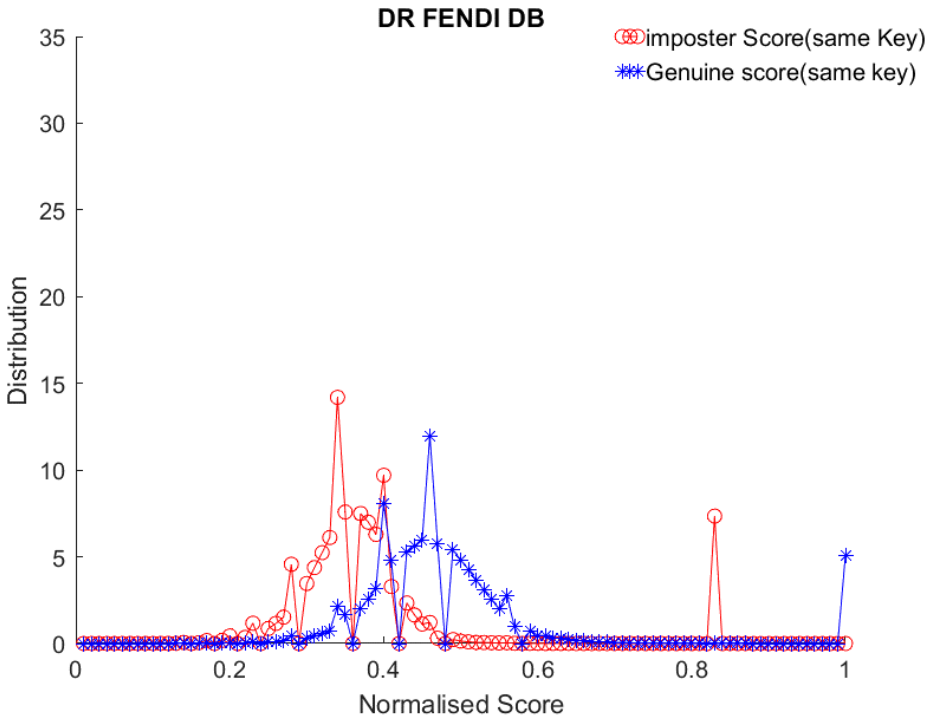


Figure 51: Dr. Fendi Distribution Curve 1400 (Imposter Score and Genuine Score)

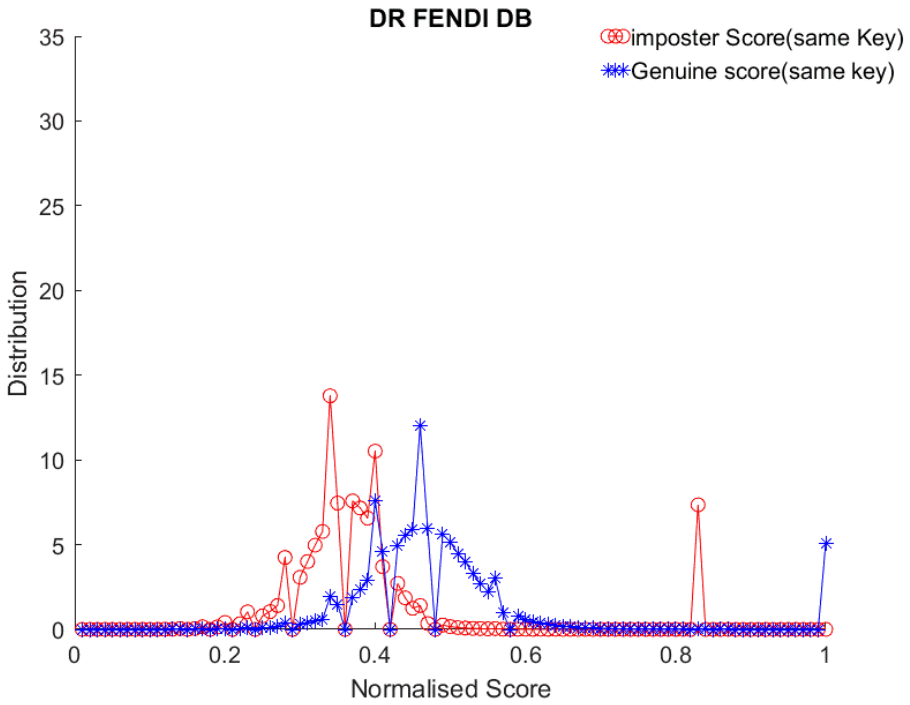


Figure 52: Dr. Fendi Distribution Curve 1700 (Imposter Score and Genuine Score)

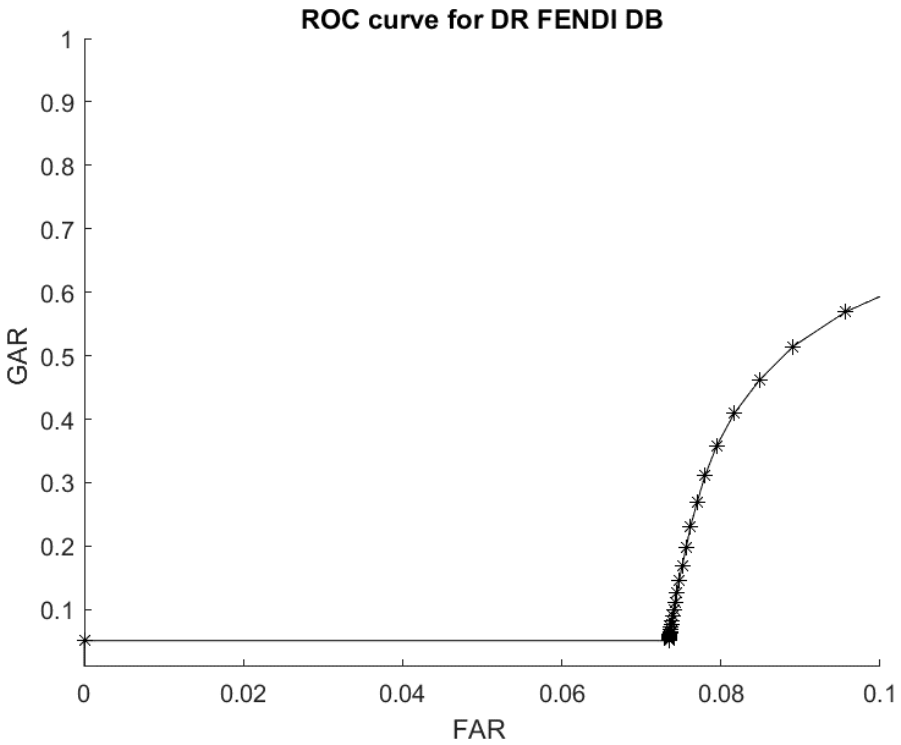


Figure 53: Dr Fendi GAR FAR Curve 1100 (Imposter Score and Genuine Score)

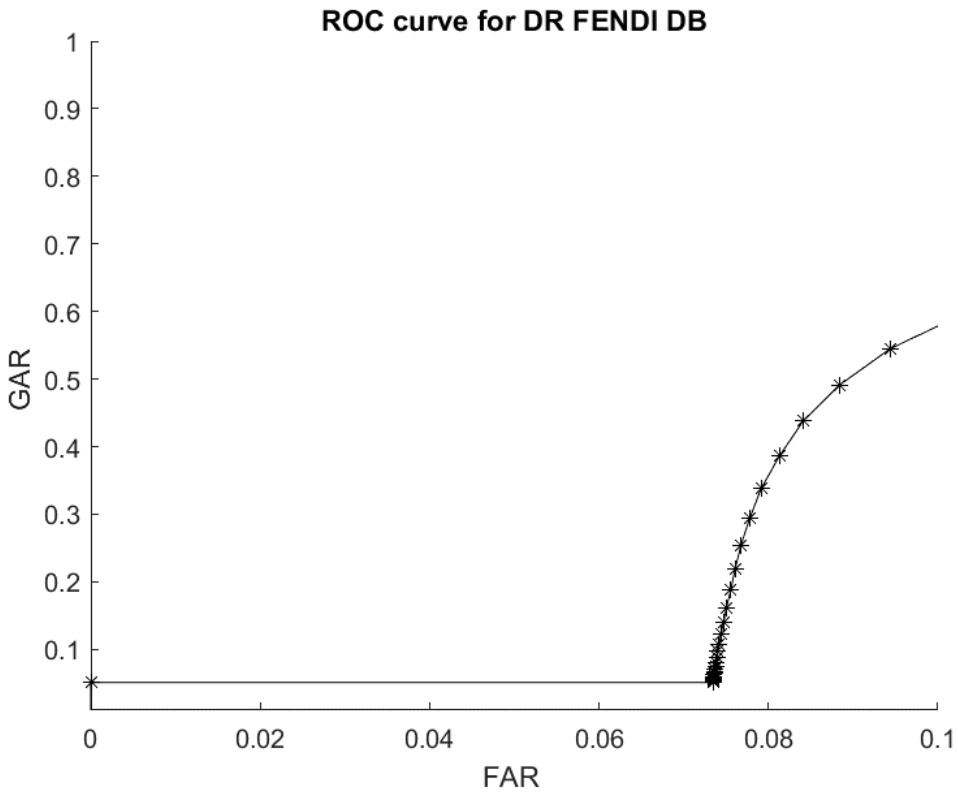


Figure 54: Dr Fendi GAR FAR Curve 1400 (Imposter Score and Genuine Score)

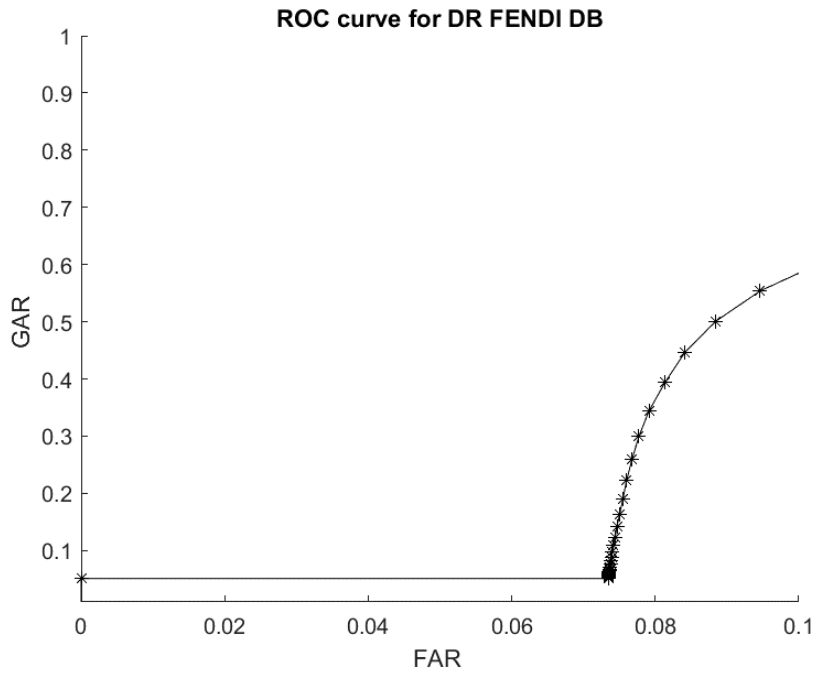


Figure 55: Dr Fendi GAR FAR Curve 1700 (Imposter Score and Genuine Score)

CHAPTER 4

RESULTS AND ITS ANALYSIS

Some of the available finger vein databases available for public use is displayed in Figure 1. We were able to gain access to three databases, namely the UTFV finger vein database, The Hong Kong Polytechnic Unissversity finger vein image database, and the Finger Vein USM (FV-USM) Database. The dataset description is detailed in the following sections.

4.1 UTFV Dataset:

The UTVP dataset, provided by the University of Twente, contains 1440 finger vascular pattern images obtained from 60 volunteers affiliated with the university. The data was collected over two sessions with an average interval of 15 days. During each session, the vascular patterns of the index, ring, and middle fingers from both hands were captured, resulting in four images per finger. The images have a resolution of 672x380 pixels and a pixel density of 126 pixels per centimeter (ppcm).

The dataset comprises predominantly male participants (73%) who are primarily right-handed (87%). The majority of volunteers fall within the age range of 19-30 years. The images are stored in the lossless 8-bit greyscale Portable Network Graphics (PNG) format. While there may be slight variations in image quality across subjects, the within-subject variation is minimal. The visible blood vessel widths range from 4 to 20 pixels, equivalent to approximately 0.3-1.6 mm using the 126 ppcm pixel density. The pixel density was determined by comparing the images with a reference graph paper placed in the same position.

To obtain access to the UTFV dataset, interested individuals can submit an online download request and complete the accompanying license agreement provided by the University of Twente [33].

4.2 The Hong Kong Polytechnic University (HKPU) finger image database

The finger image database from The Hong Kong Polytechnic University contains simultaneous finger vein and finger surface texture images from male and female volunteers. Acquired between April 2009 and March 2010 on the university campus using a contactless imaging device, the database consists of 6264 images from 156 subjects, all in bitmap (*.bmp) format. Around 93% of the subjects are under 30 years old. The images were captured in two sessions, with a minimum interval of one-month, maximum interval of over six months, and average

interval of 66.8 days. Each subject provided six image samples of their index and middle fingers in each session, resulting in a total of 24 images per subject.

4.3 Finger Vein USM (FV-USM) database

The database comprises finger images collected from 123 volunteers, including 83 males and 40 females who were staff and students of Universiti Sains Malaysia. The age of the subjects ranged from 20 to 52 years. Each volunteer provided four fingers: left index, left middle, right index, and right middle fingers, resulting in a total of 492 finger classes.

During the data collection process, each finger was captured six times in one session, and each participant underwent two sessions with a time gap of over two weeks. In the first session, a total of 2952 images were collected (123 volunteers x 4 fingers x 6 captures). Consequently, across the two sessions, a total of 5904 images were obtained, representing the 492 finger classes.

The captured finger images had a spatial resolution of 640 x 480 and a depth resolution of 256 grey levels. Additionally, the database provides extracted Region of Interest (ROI) images specifically for finger vein recognition.

4.4 Synthetic Finger-Vein Image database (The Hong Kong Polytechnic University)

In recent times, various finger-vein image databases have been made publicly available. However, compared to face or iris databases, these finger-vein databases are relatively smaller in size and involve a limited number of subjects. Consequently, it becomes challenging to extensively test the developed identification algorithms. Acquiring large-scale biometric databases is both expensive and inconvenient for the subjects, and it also raises privacy concerns associated with biometric data. To overcome some of these challenges, several synthetic biometric databases have been created. However, it is worth noting that finger-vein image synthesis has not received significant attention from researchers thus far. This project develops synthesis model for generating finger-vein images. The program is available for public use and can be used to generate large number of synthesized finger-vein images.

In this research, three databases are used for experimental purpose:

a) The University of Twente Finger Vascular Pattern (UTFVP) Database
b) The Hong Kong Polytechnic University Finger Image Database
c) Finger Vein USM (FV-USM) Database

In the sections below, the repeated line tracking algorithm is applied to every database and will be discussed in detail.

The summary of the features obtained after binarization of the RLT image using different threshold values are listed below:

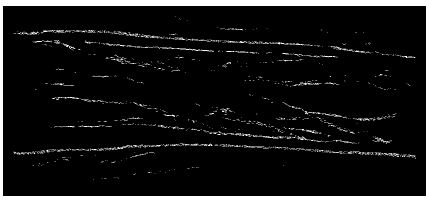
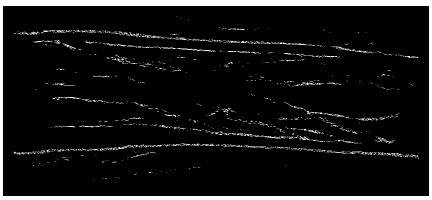
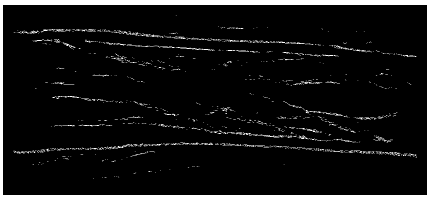
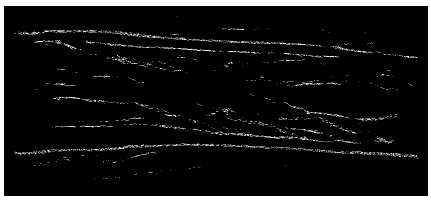
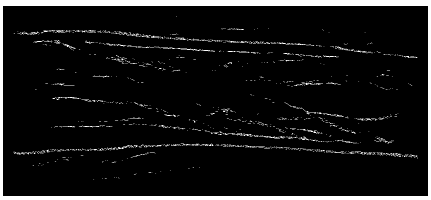
Threshold	Binarized Image	No. of Features (White Pixels)	Black Pixels
151		5755	249605
152		5655	249705
153		5550	249810
154		5441	249919
155		5349	250011

Table 16. Comparison of features extracted after applying RLT algorithm and binarization using different threshold values

Comparison of features extracted after applying RLT algorithm and binarization using different threshold values is shown in Table 16. Upon analysing binary images and feature sets, threshold value of 155 will be utilized in this research. The extracted features set (white pixels) is referred to as biometric template of corresponding input image. In our work, we have

extracted features from three benchmark finger vein databases i.e. HKPU, Dr. Fendi Database and UTVF database. Thereafter, cancelability is applied on the extracted features. Multiline Neighbouring Relations method is used for cancelability. The EER and DPRIME values have been calculated using different key.

Our Results After Applying Cancelability Using Multiline Neighbouring Relations Method:

Database	Key	EER	DPRIME	Template with Complex values
HKPU	1400	0.0557	3.1047	1400*1
	1700	0.0532	3.1693	1700*1
	1100	0.0512	3.1994	1100*1
Dr Fendi Database (FV-USM)	1400	0.2024	0.7174	1400*1
	1700	0.201	0.7253	1700*1
	1100	0.1987	0.7322	1100*1
University of Twente Database	1400	0.0085	4.8481	1400*1
	1700	0.0061	5.0012	1700*1
	1100	0.0077	4.8818	1100*1

Table 17: EER Values after applying RLT for features extraction and cancelability using Multiline neighbouring relations method.

We have analysed existing results on the benchmark finger vein databases (FV-USM, Poly U and UTVF). Experimental evaluations conducted on three different databases demonstrate the effectiveness, reliability, and performance improvement of the different methods for finger vein identification. We will discuss it in below sections.

Full-view 3D representation of finger vein patterns for improved biometric recognition

	Database	
Method	**FV-USM**	**Poly U**
Wang [36]	4.75	
Qiu [37]	2.32	
Qin [38]	1.42	2.7
Qin [39]		2.86
AlexNet [40]	1.01	5.22
VGG-16 [41]	2.01	5.1
ResNet50 [42]	0.61	2.72
Kang [43]	0.94	2.4

Table 18: Investigation of finger vein verification based on full-view 3D technique [43]

The thermal palm vein pattern is a new and promising biometric feature that has gained significant attention in research and applications. Due to its unique characteristics, such as liveness detection and resistance to forgery, several algorithms have been developed for authentication purposes. The authors in [36] propose an efficient palm vein identification method based on Gabor wavelet features. The method consists of five key steps: image acquisition, ROI detection, image preprocessing, feature extraction, and matching. To evaluate the approach, authors [36] conducted tests on 178 palm vein images from 101 individuals. Out of these, 176 images were correctly recognized, with only two failures. The experimental results demonstrate the effectiveness of the proposed approach in palm vein recognition.

In the context of finger vein imaging, uneven illumination is a common issue caused by factors like finger position, posture, near-infrared light uniformity, and ambient light. Current methods for locating phalangeal joints are sensitive to illumination, resulting in unreliable outcomes. To address this, we propose a dual-sliding window model that accurately detects phalangeal joint positions in finger vein images. This model is designed to be robust against varying illumination conditions. To address this, [37] propose a pseudo-elliptical sampling model that retains the spatial distribution of vein patterns while reducing redundant information and minimizing differences between images. Furthermore, we employ two-dimensional principal component analysis for feature extraction by projecting the transformed image. Authors [37] utilize the Euclidean distance. Experimental evaluations conducted on three different databases demonstrate the effectiveness, reliability, and performance improvement of the proposed method for finger vein identification.

Finger-vein biometrics has been extensively studied for personal verification. However, existing solutions heavily rely on domain knowledge and struggle to robustly extract finger-vein features from raw images. Authors [38] proposed a deep learning model that can extract and recover vein features with limited prior knowledge. The first step of the proposed approach involves combining state-of-the-art handcrafted finger-vein image segmentation techniques. This combination aims to automatically identify two distinct regions within the image: a clear region characterized by a high separability between finger-vein patterns and the background, and an ambiguous region with a low separability. The clear region comprises pixels that are consistently labeled as either foreground or background by the segmentation techniques, while the ambiguous region contains the remaining pixels. This approach involves employing this method to automatically eliminate uncertain areas and assign labels to pixels in the unambiguous region, categorizing them as either foreground or background. In a study

conducted by Authors [38], they generated a training dataset by extracting patches centered on the labeled pixels. Subsequently, a Convolutional Neural Network (CNN) was trained on this dataset. The CNN's objective was to estimate the likelihood of each pixel representing a foreground (vein) pixel, given a patch centered around it. By learning to differentiate between vein patterns and background patterns, the CNN adeptly classifies pixels within any region of a test image. Additionally, authors [38] introduce another novel contribution by developing and investigating a Fully Convolutional Network (FCN) to recover missing finger-vein patterns in the segmented image. The FCN aims to fill in the gaps and reconstruct the complete finger-vein patterns. Experimental results conducted on two public finger-vein databases demonstrate a significant improvement in finger-vein verification accuracy using the proposed approach [38]. This indicates the effectiveness and potential of the deep learning model for extracting and recovering finger-vein features without relying heavily on domain knowledge.

Extensive research has been conducted on finger-vein biometrics for personal authentication. However, a significant hurdle in finger-vein verification lies in its vulnerability to image quality degradation. When images are of poor quality, they can contain misleading or missing features, which negatively impact the system's performance [39]. The approach focuses on minimizing verification errors in biometric quality assessment. It assumes that low-quality images are erroneously rejected in a verification system. Based on this assumption, the authors automatically label images as low- or high-quality and proceed to train a DNN using this dataset to predict image quality [39].

In the research [40], researchers trained a large and deep convolutional neural network with the objective of classifying a vast dataset of 1.2 million high-resolution images from the ImageNet LSVRC-2010 contest into 1000 different classes. Our network outperformed the previous state-of-the-art models, achieving top-1 and top-5 error rates of 37.5% and 17.0%, respectively.
The neural network developed is quite extensive, with 60 million parameters and 650,000 neurons. It consists of five convolutional layers, some of which are followed by max-pooling layers, and three fully connected layers, culminating in a final 1000-way softmax layer. To expedite the training process, researchers utilized non saturating neurons and employed a highly efficient GPU implementation for convolution operations. To mitigate overfitting issues in the fully connected layers, authors [40] employed a recently developed regularization technique known as "dropout," which proved to be highly effective. This method helps prevent the neural network from relying too heavily on specific features or neurons during training, enhancing its generalization capabilities.

Researchers [40] participated in the ILSVRC-2012 competition, entering a variant of our model, and achieved a top-5 test error rate of 15.3%. This result surpassed the second-best entry, which achieved a test error rate of 26.2%, thereby demonstrating the superiority of the approach. Overall, the research [40] showcases the power and effectiveness of deep convolutional neural networks for image classification tasks, particularly in terms of achieving significantly improved accuracy compared to previous state-of-the-art models. Authors [41] focused on investigating the impact of convolutional network depth on its accuracy in the context of large-scale image recognition. Primary contribution lies in conducting a comprehensive evaluation of networks with increasing depth, using an architecture that incorporates small (3×3) convolution filters. Through the research, researchers [41] discovered that by increasing the depth of the network to 16-19 weight layers, able to achieve a significant improvement over prior state-of-the-art configuration.

Researchers [42] address the challenge of training deeper neural networks, which tend to be more difficult to optimize. Introduce a novel residual learning framework that facilitates the training of significantly deeper networks compared to previous approaches. Instead of directly learning the intended underlying functions, the authors [42] adopt a different approach by redefining the network layers to learn residual functions relative to the layer inputs. This novel strategy has demonstrated improved optimization and enables the construction of deeper networks with enhanced accuracy. In their evaluation using the ImageNet dataset, the researchers evaluate residual networks with depths of up to 152 layers, which is eight times deeper than VGG nets, while still maintaining lower complexity. Through an ensemble of these residual networks, they achieve an impressive 3.57% error rate on the ImageNet test set, securing the top position in the ILSVRC 2015 classification task. Furthermore, the authors [42] present comprehensive analysis and results on the CIFAR-10 dataset, demonstrating the scalability and effectiveness of their approach across different scales, including the successful implementation of networks with 100 and 1000 layers. The depth of representations plays a vital role in various visual recognition tasks, and extremely deep representations yield remarkable improvements. Specifically, on the COCO object detection dataset, the deep residual networks achieve a 28% relative improvement. Overall, the work [42] demonstrates the power and effectiveness of deep residual networks in training significantly deeper neural networks, achieving state-of-the-art performance in various visual recognition tasks.

The finger vein modality in biometrics has unique advantages, but current vein verification systems face limitations in vein imaging and information acquisition. Commonly, these

systems rely on a monocular camera to capture a 2D vein image from a single viewpoint on one side of the finger. However, this approach presents two main challenges. Firstly, it results in limited vein pattern information available for verification purposes. The captured image may not contain sufficient details to ensure accurate identification. Secondly, there are variations among samples of the same individual due to different finger positions when using contact-free modes. These variations can affect the consistency and reliability of the system, making it more challenging to achieve consistent and accurate authentication. These issues adversely affect system performance, especially in relation to positional variations caused by pitch and roll movements. To address these challenges comprehensively, researchers [43] propose a novel system comprising a hardware and software platform.

In this approach [43], researchers present a new method for 3D reconstruction that enables the generation of a complete 3D finger vein image, providing a full view of the veins. This allows for a more comprehensive representation of the finger vein patterns. Additionally, we employ a feature extraction and matching strategy specifically designed for 3D finger vein data. Our strategy utilizes a lightweight convolutional neural network (CNN) that incorporates depth-wise separable convolution, enabling efficient and effective processing of the 3D vein information. Through extensive experimentation, we have validated the potential of our proposed system. In comparison to the traditional single-view 2D approach for finger vein recognition, our system demonstrates significant improvements in recognition performance. By leveraging the additional valuable information provided by finger vein biometrics in the form of 3D data, we achieve enhanced accuracy and reliability in the recognition process. The approach efficiently addresses the limitations of existing systems and demonstrates the benefits of utilizing a full-view 3D representation of finger vein patterns for improved biometric recognition [43].

Convolutional Auto-Encoder Model for Finger-Vein Verification

Dataset	**Features**	**Linear**	**Poly**	**RBF**
FV-USM		**EER**	**EER**	**EER**
	16	17	0.21	1.54
	32	4.37	0.12	0.92

Table 19: Convolutional Auto-Encoder Model for Finger-Vein Verification [44]

In their study, the authors [44] proposed FV-GAN, a pattern extraction model based on CycleGAN, for finger vein verification. FV-GAN utilizes deep learning techniques to learn a

deep pattern representation and predict the probability of pixels being veins or background. By leveraging adversarial training, FV-GAN robustly extracts vein patterns from finger vein images, leading to significant improvements in verification performance in terms of accuracy and equal error rate (EER).

In their future research, the authors plan to explore several interesting aspects to further enhance finger vein verification. Firstly, they aim to collect a larger database to improve the generalization and scalability of their model. Secondly, they acknowledge the challenges and instability of training GANs (Generative Adversarial Networks) even with advanced techniques like WGAN, CycleGAN, and DCGAN. Therefore, they intend to investigate alternative deep learning techniques to make the training of GANs more stable and easier to converge. Another intriguing aspect they highlight is the comparison between the generated finger vein images and the raw finger vein images. The generated images exhibit reduced noise and outliers, indicating the potential for enhancing finger vein images and extracting finger vein skeletons. This generative process holds promise for addressing various problems in finger vein verification. For example, the generator could be further developed to expand the finger vein database. Vein patterns from raw data can be extracted using conventional or deep learning-based methods and input into the generator with random noise. The generated results, while different from each other due to noise variations, would share the same finger vein skeletons as the raw images. This approach offers a means to expand the raw database, and the authors emphasize the need for further investigation into these promising outputs.

Convolutional Neural Network for Finger-Vein-based Biometric Identification

Paper	**Database**	**Subjects**	**Feature Extraction Method**	**Classifier**	**EER**
Xi et al. [45]	HKPU	105	Discriminative Binary Codes (DBC)	SVM	1.44%
Bakhtiar et al. [46]	FV-USM	123	Modified Gaussian Filter(MGF) enhanced & displacement corrected images	Band Limited Phase Only Correlation (BLPOC)	2.34%
Yang et al. [47]	HKPU	105	Anatomy Structure Analysis Based Vein Extraction (ASAVE)	Elastic Matching	0.38%

Ton et al. [48]	UTFVP	60	Maximum Curvature	Correlation Based Comparison	0.40%
Kauba et al. [49]	UTFVP	60	Different feature level fusion	Correlation Based Comparison	0.19%

Table 20: Convolutional Neural Network for Finger-Vein-based Biometric Identification

In [45], the authors propose a novel method called Discriminative Binary Codes (DBC) learning for finger vein recognition. The goal is to develop binary templates that capture the vein characteristics of subjects in a discriminative and representative manner. The optimization problem is formulated to ensure that the transformed templates are both discriminative and informative about the subjects. This is achieved by maximizing the distance between templates from different subjects and maximizing the amount of information provided by the templates. The obtained binary templates are then used to provide supervised information for training instances, and Support Vector Machines (SVMs) are trained as the code learners for each bit. The DBC (Dynamic Binary Code) method in finger vein recognition offers several advantages compared to existing binary codes. Firstly, DBCs are more discriminative and shorter, providing a more effective and efficient representation. Furthermore, DBCs take into account the relationships among subjects, which has the potential to enhance the performance of finger vein recognition even further. The effectiveness and efficiency of the DBC method are evaluated through experiments conducted on the PolyU database and MLA database. The experimental results demonstrate the superiority of DBCs for finger vein recognition and retrieval tasks, validating the proposed method's effectiveness in capturing vein characteristics and its potential for improving recognition performance [45].

A multimodal finger biometrics approach is proposed by the authors [46] to enhance performance by combining finger vein recognition and finger geometry recognition. The method utilizes Band Limited Phase Only Correlation (BLPOC) for measuring the similarity of finger vein images, which improves robustness against noise, occlusions, and rescaling factors. For finger geometry recognition, a novel geometric feature called Width-Centroid Contour Distance (WCCD) is introduced, which combines finger width with Centroid Contour Distance (CCD) to capture comprehensive geometric information. The fusion of these two features enhances the accuracy of finger geometry recognition compared to using a single

feature type. The fusion of finger vein and finger geometry recognition is achieved using a score-level fusion method based on the weighted SUM rule. This integration combines the recognition scores from both modalities to obtain a final decision. Experimental evaluation on a database collected from 123 volunteers demonstrates the effectiveness of the proposed approach. The equal error rate (EER) achieved is 1.78%, and the total processing time is 24.22 ms, indicating efficient and accurate recognition performance. Overall, the proposed multimodal finger biometrics approach, combining finger vein and finger geometry recognition, offers enhanced accuracy and robustness, making it a promising solution for reliable and secure biometric authentication [46].

A novel framework is introduced by the authors [47] to enhance the performance of finger vein recognition methods. The framework includes two components: an anatomy structure analysis-based vein extraction (ASAVE) algorithm and an integration matching strategy. The ASAVE algorithm focuses on analysing the anatomical structure of the finger to improve the accuracy of vein extraction. The integration matching strategy combines multiple matching algorithms or techniques to achieve more reliable and robust matching results. The ASAVE algorithm focuses on accurately extracting vein patterns by considering the finger's anatomical structure. The integration matching strategy combines vein patterns from multiple sources to enhance recognition accuracy. Overall, this framework aims to enhance the reliability and accuracy of finger vein recognition. The ASAVE algorithm focuses on analysing the anatomy structure and imaging characteristics of vein patterns. This extraction method helps to address the issues related to defective vein networks and weak matching. Furthermore, the extracted vein pattern undergoes thinning and refinement processes to obtain a more reliable vein network. In addition to the vein network, the framework also mines relatively clear vein branches from the vein pattern, known as the vein backbone. These vein backbones serve as an additional feature for matching and contribute to overcoming finger displacements, which can occur during the capture process. The matching process involves the calibration of the vein network using the vein backbone information. The overlap degree of corresponding vein backbones is also integrated into the similarity computation to improve accuracy. The effectiveness of the proposed framework is validated through extensive experiments conducted on two public finger vein databases. The results demonstrate that the framework achieves improved performance in terms of finger vein recognition accuracy and reliability. Overall, the proposed framework, incorporating the ASAVE algorithm and integration matching strategy, provides a comprehensive approach to finger vein recognition by leveraging the analysis of anatomy

structure and imaging characteristics. This approach shows promising results in addressing the challenges associated with defective vein networks, weak matching, and finger displacements, thereby advancing the field of finger vein recognition [47].

The authors [48] introduce a new finger vascular pattern dataset that addresses the scarcity of available datasets in the field. The dataset consists of 1440 high-resolution images with a known pixel density. What sets this dataset apart is the inclusion of additional meta data, such as age, gender, and handedness of the volunteers, which makes it unique compared to existing datasets. The capturing device used to obtain the images is custom-designed, and the paper discusses the various aspects involved in its design. This information provides insights into the technical details and considerations necessary for capturing high-quality finger vascular patterns. The evaluation metric used is the equal error rate (EER), which measures the point at which false acceptance and false rejection rates are equal. The presented results indicate that the new dataset has enabled achieving remarkably low EERs, with values as low as 0.4% being attained. Overall, this contributes to the field of finger vascular pattern recognition by introducing a new dataset with high-resolution images and accompanying meta data. The availability of this dataset and the achieved performance figures serve as important resources for researchers and facilitate advancements in the development and evaluation of algorithms for finger vascular pattern recognition [48].

The paper [49] highlights the importance of accurate vein pattern extraction in finger-vein-based authentication systems. Due to variations in image quality, a single feature extraction technique may not always capture the vein pattern correctly, leading to poor recognition performance. To address this issue, the authors [49] propose the use of biometric fusion, specifically feature level fusion, to enhance the quality of extracted vein patterns and improve feature extraction accuracy. The study involves experimenting with different feature extraction techniques, such as maximum curvature, repeated line tracking, and wide line detector, among others. These techniques extract vein patterns from the input images. Additionally, various fusion techniques, including majority voting, weighted average, and STAPLE, are employed to combine the outputs of multiple feature extractors. The UTFVP finger-vein dataset is used for conducting the experimental study. The results demonstrate that feature level fusion can enhance recognition accuracy, as measured by the equal error rate (EER), compared to using a single feature extraction technique alone. The fusion of multiple feature extractors' outputs helps mitigate the limitations and variations associated with individual techniques, resulting in improved vein pattern extraction and subsequently better recognition performance. Overall, the

paper [49] emphasizes the effectiveness of feature level fusion in finger-vein recognition systems. By combining the strengths of multiple feature extraction techniques, the accuracy of vein pattern extraction is enhanced, leading to improved authentication performance.

The authors [50] propose a CNN-based finger-vein identification system for accurate identification under diverse environmental conditions. Extensive experiments using multiple databases demonstrate a rank-1 accuracy of over 95%. The study emphasizes dataset diversity, training data quantity, and the impact of image quality on system performance. Training with data from multiple sessions improves identification accuracy under varying lighting conditions. Overall, the research presents a robust CNN-based system for finger-vein identification [50].

From Noise to Feature: Exploiting Intensity Distribution as a Novel Soft Biometric Trait for Finger Vein Recognition

	Database: FV-USM	
	EER Values	
	SM	**HM**
LBP+AM&V	0.257%	0.216%
WLD+AM&V	0.772%	0.379%
HOG+AM&V	0.433%	0.108%
SIFT+AM&V	0.243%	0.237%

Table 21: From Noise to Feature: Exploiting Intensity Distribution as a Novel Soft Biometric Trait for Finger Vein Recognition [51]

The authors [51] address a limitation in previous finger vein recognition research by focusing on the texture feature of finger veins and neglecting the intensity distribution in the background. They propose a soft biometric trait extraction algorithm that takes into account the intensity distribution as an important factor in finger vein recognition. The proposed algorithm consists of several steps. First, the background layer, which does not contain finger vein texture, is extracted using two methods: Image Light Source (ILS) and Gaussian Blur (GB). Then, the intensity distribution in the background layer is described using three soft biometric traits. These traits capture specific characteristics of the intensity distribution. To improve matching accuracy, the authors propose a hybrid matching strategy that combines the primary biometric trait (finger vein texture) with the soft biometric traits. By incorporating the soft biometric traits, the matching accuracy is enhanced compared to using only the primary biometric trait. The experimental results validate the effectiveness of the proposed approach. It is found that GB achieves similar performance to ILS but with less computational time. Furthermore, when

applied to three open-access databases, the fusion of the primary biometric trait and the soft biometric trait leads to a lower Equal Error Rate (EER) compared to using only the primary biometric trait. This demonstrates the efficiency and universality of the proposed soft biometric trait. The performance of the soft biometric trait is shown to be robust across a range of sigma changes, indicating its stability. This preliminary study of the soft biometric trait based on the intensity distribution contributes to the field of finger vein recognition by considering previously overlooked information. Overall, the paper introduces a novel approach that incorporates the intensity distribution as a soft biometric trait in finger vein recognition. The proposed method demonstrates improved matching accuracy and stability, highlighting the potential of considering the background intensity distribution in future finger vein recognition systems [51].

On-the-Fly Finger-Vein-Based Biometric

Paper	**Biometric Identifier**	**Database**		**EER (%)**
		Name	**Class#**	
Xie et al. [47] [53]	Finger Vein	HKPU [10]	302 (156 Users)	0.11%
Jalilian et al. [51] [54]	Finger Vein	UTFVP [42]	360 (60 Users)	4.53%
Kim et al. [55]	Finger Vein	HKPU [10]	302 (156 Users)	0.79%

Table 22: On-the-Fly Finger-Vein-Based Biometric [52]

This system [52] allows for contactless identification of users by simply passing their hand over a sensor, without the need for physical contact. This approach is the first of its kind in the literature. The acquisition module is designed using low-cost sensors to facilitate free hand movement during both enrolment and recognition processes, ensuring user convenience. Deep learning techniques are employed in both scenarios. The analysis demonstrates that using multiple-exposure data enhances the recognition accuracy compared to single-exposure images. Additionally, exploiting multi-channel Low Dynamic Range (LDR) images taken at different exposure times as raw input templates further improves identification accuracy. To address finger vein identification, the authors propose a novel Convolutional Neural Network (CNN) architecture called V-CNN, which surpasses other state-of-the-art CNN architectures in performance. Furthermore, the authors introduce the novel use of temporal information related to hand movement over the sensor [52].

This paper [53] focuses on automated personal identification using vascular biometrics, specifically finger vein images. Overall, the paper highlights the effectiveness of using CNNs and supervised discrete hashing for finger vein authentication. The proposed approach demonstrates superior performance compared to existing methods and offers the advantage of reduced template size, which is beneficial for storage and processing efficiency [53].

In their study, the authors [54] introduce a novel approach for finger-vein recognition. Their method directly extracts finger-vein patterns from near-infrared (NIR) finger images without requiring any pre- or post-processing steps. They achieve this by utilizing semantic segmentation convolutional neural networks (CNNs), specifically three different network architectures. The authors conduct experiments to identify efficient training and configuration settings for the CNNs. They use manually annotated training data to train the networks, but they also introduce a training model based on automatically generated labels to further improve the networks' performance. In addition to presenting their proposed model and experimental results, the authors contribute to the research community by releasing human annotated ground-truth vein pixel labels for a subset of two well-known finger-vein databases used in their work. They also provide a corresponding annotation tool to facilitate further annotations in this area. According to the experimental results, the proposed model outperforms traditional finger-vein recognition algorithms, demonstrating the effectiveness of the direct extraction approach and the use of semantic segmentation CNNs. The availability of annotated ground-truth data and the annotation tool further support the advancement of research in finger-vein recognition [54].

In this research [55], the authors propose a multimodal biometric recognition system that combines finger-vein and finger shape modalities using a near-infrared (NIR) light camera sensor. The conventional finger-vein recognition methods can suffer from issues such as image misalignment and illumination variation, which can affect the recognition performance. To tackle the challenges associated with finger-vein and fingerprint recognition, researchers have explored multimodal biometric systems that recognize both modalities simultaneously. However, acquiring images for both finger-veins and fingerprints typically necessitates different sensors or a larger device size. To overcome these limitations, the authors propose a multimodal biometric system that combines finger-vein and finger shape recognition. They employ a deep convolutional neural network (CNN) and an NIR light camera sensor for this purpose. By leveraging this approach, they aim to achieve accurate and efficient biometric recognition without the need for additional sensors or increased device size. The CNN is trained to extract discriminative features from the finger-vein and finger shape modalities captured in

NIR light. The experimental results demonstrate that the proposed method outperforms conventional approaches in terms of recognition performance. By leveraging the advantages of deep learning and NIR imaging, the proposed multimodal biometric system offers improved accuracy and robustness compared to handcrafted feature-based methods. It eliminates the need for separate sensors or devices for acquiring finger-vein and fingerprint images. Overall, the research contributes to the field of multimodal biometrics by proposing an effective approach for finger-vein and finger shape recognition using an NIR light camera sensor and deep CNNs [55].

Recognition performance (EER) for the UTFVP data set using 2-fold evaluation

UTFVP	**EER in %**			
	avg	**std**	**min**	**max**
Bozorth3	2.4	0.4	2.0	4.1
Bozorth3*	13.4	0.6	12.1	15.6
IDKit	2.2	0.3	1.7	3.2
IDKit*	1.2	0.2	1.0	2.1
VeriFinger	3.0	0.2	2.6	3.6
VeriFinger*	0.5	0.1	0.3	0.6
MHD	11.4	0.5	11.0	13.8
SML	4.7	1.0	3.7	7.4
PC	0.5	0.2	0.2	1.3
GF	1.7	0.2	1.6	2.5
ASAVE	2.0	0.4	1.4	2.8

Table 23: Recognition performance (EER) for the UTFVP data set using 2-fold evaluation. Methods marked with * indicates that minutiae orientation is set to zero [56].

HKPU-FV	**EER in %**			
	avg	**std**	**min**	**max**
Bozorth3	11.5	0.5	10.8	12.9
Bozorth3*	13.9	1.2	12.6	17.8
IDKit	10.4	0.3	9.7	11.9
IDKit*	8.5	1.3	6.9	12.7
VeriFinger	10.6	0.3	10.1	11.8
VeriFinger*	2.8	0.2	2.5	3.7

MHD	11.6	1.3	9.9	16.2
SML	8.5	0.4	7.7	9.4
PC	2.0	0.3	1.6	3.1
GF	2.9	0.2	2.8	3.4
ASAVE	3.3	0.2	2.9	3.8

Table 24: Recognition performance (EER) for the HKPU-FV data set using 2-fold evaluation [56].

DataSet	**Method**	**EER**
UTFVP	VeriFinger*	0.28
	PC	0.23
HKPU-FV	VeriFinger*	2.41
	PC	1.41

Table 25: Recognition performance of data sets using all comparison protocol and best setting. All values are in % [56]

The authors [56] highlight the importance of security and privacy in biometric systems and mention that the use of Match-on-Card (MoC) technology provides advantages in terms of convenience, security, and performance. While MoC technology is already being widely used in high-security smart cards, the authors note that no MoC system currently exists for finger vein recognition. However, there are several minutiae-based MoC solutions available for fingerprint recognition. In this work, the authors propose a minutiae-based approach for finger vein recognition and investigate the integration of finger vein minutiae into MoC systems. They employ a commercial software that offers MoC solutions and is capable of extracting minutiae points from finger vein images. These minutiae points are then compared using a minutiae-based fingerprint template comparison technique. The resulting minutiae data is stored in a standardized biometric data format. By leveraging existing MoC technology and integrating finger vein minutiae into the MoC system, the authors aim to provide a secure and privacy-preserving solution for finger vein recognition. This approach allows for seamless integration of finger vein recognition into MoC systems and potentially opens up new possibilities for utilizing finger vein biometrics in various applications [56].

Method Used	**Finger Vein Databases**		
	HKPU	**FV-USM**	**University of Twente**
Repeated Line Tracking and Multiline Neighbouring Relation (RLMN) framework	0.0512	0.1987	0.0061
Investigation of finger vein verification based on full-view 3D technique [43]	2.4	0.61	Results Not Available
Convolutional Auto-Encoder Model for Finger-Vein Verification [44]	Results Not Available	0.12	Results Not Available
Convolutional Neural Network for Finger-Vein-based Biometric Identification	0.0038	0.0243	0.0019
From Noise to Feature: Exploiting Intensity Distribution as a Novel Soft Biometric Trait for Finger Vein Recognition [51]	Results Not Available	0.0011	Results Not Available
On-the-Fly Finger-Vein-Based Biometric [52]	0.0011	Results Not Available	0.0453
Recognition performance (EER) for the UTFVP data set using 2-fold evaluation. Methods marked with * indicates that minutiae orientation is set to zero [56].	Results Not Available	Results Not Available	0.002
Recognition performance (EER) for the HKPU-FV data set using 2-fold evaluation [56].	0.016	Results Not Available	Results Not Available
Recognition performance of data sets using all comparison protocol and best setting. All values are in % [56]	0.0141	Results Not Available	0.0023

Table 26: Comparison of Finger Vein Recognition Methods: Evaluating EER Values with Cancelability for Enhanced Security

The table [26] presents the EER values for different finger vein recognition methods on three datasets: HKPU, FV-USM, and University of Twente. The RLMN framework achieved remarkably low EER values of 0.0512, 0.1987, and 0.0061 for the HKPU, FV-USM, and University of Twente datasets, respectively. What makes the RLMN framework particularly noteworthy is that it obtained these EER values after applying cancelability, which enhances the security and privacy of the biometric system.

In comparison, other methods evaluated EER values directly on feature extractions without applying cancelability. The RLMN framework's ability to achieve such low EER values with cancelability showcases its effectiveness in providing robust and accurate finger vein recognition. These promising results demonstrate the superiority of the RLMN framework over existing methods, making it a valuable contribution to the field of finger vein recognition.

CHAPTER 5

CONCLUSION AND FUTURE DIRECTIONS

Three benchmark databases i.e. UTFV, HKPU and FV-USM are identified for this research. Experimental setup has been incorporated for features extraction from finger vein images. Upon analysis of different threshold values for binarization, value of 155 as threshold is finalized for this research due to manageable number of extracted features and less noise in output binarized image. Using threshold value of 155, features have been extracted from the listed databases using Repeated Line Tracking (RLT) algorithm.

The multiline neighboring relations generation cancelability technique is applied to the extracted features of different databases, namely the Hong Kong Polytechnic University finger vein image database, Finger Vein USM (FV-USM) Database, and UTVF database.

After applying cancelability, the performance parameter Equal Error Rate (EER) has been evaluated. We compared the existing results (EER values on untransformed finger vein templates and EER values on transformed templates) with our results and found that our research has made a significant contribution to the use of finger vein technology in the field of biometric verification. We were able to achieve an EER value on the transformed biometric template using the Repeated Line Tracking as the feature extraction method with a threshold value of 155, and the multiline neighbouring relations method for cancelability on the extracted features using a key value of 1700.

In the future, this technology needs to be further explored using different feature extraction methods and cancelability techniques. More datasets should be experimented with for research purposes.

FEEDBACK RECEIVED ON MID TERM REPORT

Feedback: "Some research was already done on the above-mentioned technologies earlier. This research aims at improving the reliability and revocability of fingerprint patterns for the use of the Banking Industry which is interesting.

The anticipated benefits of the proposed technologies to the Banks may be spelt out by factoring in the impact on the size, cost of implementation and UIDAI guideline".

Response:

1. **Anticipated benefits of the proposed technologies to the Banks:**

Indeed, finger vein biometrics offer several advantages compared to other forms of biometrics such as fingerprint, face, or iris scans. Some of the key advantages include:

Anti-forgery: Finger vein biometrics are difficult to replicate or spoof, making them highly secure against forgery attempts.

Accuracy and speed: Finger vein recognition systems provide high accuracy and speed, allowing for efficient and reliable authentication.

Insensitivity to environmental factors: Finger vein patterns remain unaffected by factors such as dirt, sweat, grease, or surface injuries, ensuring consistent and reliable recognition.

Uniqueness: Vein patterns are unique to each individual, making them a highly secure form of identification. Unlike PINs and passwords that can be shared or stolen, vein patterns are personal and cannot be easily replicated.

Internal biometric: Finger vein recognition relies on internal biometric features that are difficult to reproduce or manipulate, enhancing security.

Liveness detection: Modern finger vein readers often incorporate liveness detection features, ensuring that a real hand is presented during the authentication process, further enhancing security.

Stability: Vein patterns are established during fetal development and remain stable throughout a person's lifetime. Even changes in weight do not significantly alter the vein pattern, ensuring long-term reliability.

User convenience: Finger vein recognition eliminates the need for multiple passwords and PINs, providing a convenient way for users to log in to their accounts by simply placing their finger on a scanner.

Given these advantages, finger vein biometrics have gained attention, especially in sectors such as banking, where security and user convenience are paramount. They offer a promising

solution to combat fraud and provide a secure and efficient means of authentication, reducing reliance on traditional password-based systems.

2. Anticipated applications of finger vein technology in Banks

ATM: The implementation of finger vein technology in ATMs for cash card-free transactions offers several benefits to users. By leveraging finger vein information along with ID input, users can authenticate themselves securely and conveniently, eliminating the need to carry a physical cash card. Here are some advantages of using finger vein technology in ATMs:

Enhanced security: Finger vein biometrics provide a high level of security as the vein patterns are unique to each individual and difficult to forge or replicate. This helps prevent unauthorized access to the ATM and protects user accounts from fraudulent activities.

Convenience: Users no longer need to carry a physical cash card while performing ATM transactions. Instead, they can simply input their ID and place their finger on the finger vein scanner to authenticate themselves, making the process more convenient and streamlined.

Reduced risk of card-related fraud: With cash card-free transactions, the risk of card-related fraud, such as card skimming or card cloning, is significantly reduced. Since there is no physical card involved, potential vulnerabilities associated with card-based transactions are mitigated.

User-friendly experience: Finger vein technology offers a user-friendly experience by eliminating the need for remembering PINs or passwords. Users can complete transactions quickly and easily by relying on their unique finger vein pattern.

Efficient and faster transactions: Cash card-free transactions using finger vein technology can expedite the ATM transaction process. Users can authenticate themselves swiftly, leading to faster transactions and reduced waiting times at ATMs.

It's worth noting that the implementation of finger vein technology in ATMs requires appropriate security measures to protect the privacy and confidentiality of users' biometric data. Compliance with data protection regulations and robust security protocols are crucial to ensure the safe and responsible use of finger vein technology in ATM systems.

Internet Banking: The development of a finger vein Internet banking system for smartphones is an exciting and promising application of finger vein technology. By incorporating finger vein recognition into personal Internet banking, researchers aim to provide users with a secure and convenient authentication method. Here's how such a system could benefit users:

Enhanced security: Finger vein recognition offers a high level of security, making it difficult for unauthorized individuals to access a user's Internet banking account. The unique vein patterns in the finger are difficult to forge or replicate, providing strong protection against fraudulent activities.

Convenient authentication: With a finger vein Internet banking system, users can conveniently access their accounts by simply placing their finger on the smartphone's built-in finger vein scanner. This eliminates the need for passwords or PINs, streamlining the authentication process and enhancing user convenience.

Mobile accessibility: By integrating finger vein technology into smartphones, users can access their Internet banking services anytime and anywhere. This mobility allows for on-the-go banking transactions and reduces the reliance on physical banking cards or additional authentication devices.

Quick and seamless transactions: Finger vein authentication enables fast and seamless transactions within the Internet banking system. Users can initiate transfers, payments, or other banking activities with a simple finger scan, eliminating the need for manual input or multiple authentication steps.

Protection against device loss or theft: Finger vein recognition adds an extra layer of security in case of smartphone loss or theft. Even if the device falls into the wrong hands, the unique finger vein pattern ensures that only the authorized user can access the Internet banking system.

To implement a finger vein Internet banking system for smartphones, rigorous security measures must be in place to safeguard users' biometric data. Encryption, secure storage, and adherence to privacy regulations are essential to protect the confidentiality and integrity of the stored finger vein information.

Overall, the combination of security and convenience offered by a finger vein Internet banking system for smartphones holds great potential for revolutionizing the way users access and manage their online banking accounts.

Employee Access Control for Banks:

Finger vein authentication technology can be utilized by banks to create a paperless employee access control system. Tablets with connected finger vein authentication units are installed at bank branches for employee authentication. When employees enter or leave a branch, they undergo finger vein authentication on the tablets. Successful authentication records timestamp information to track their entry and exit. The centralized server manages the finger vein data of employees, enabling any branch to implement finger vein authentication after the employees have completed the registration process.

Retail Industry Application of Pay-by-Finger:

A credit card payment service based on finger vein authentication has been developed, eliminating the need for physical cards or smartphones. Users register their credit or bank cards with their finger vein information, enabling payments using finger vein authentication alone. Registration is simple and can be done through a tablet or smartphone application. Stores supporting the service allow users to make payments by placing their fingers over a sensor. The system also facilitates customer loyalty program management based on purchase history. With faster transaction times, users experience shorter waiting times at cash registers. Finger vein authentication was chosen for its security features, including anti-counterfeiting and theft prevention capabilities, as well as the stability of biometric patterns.

Finger-charge Money:

A 1:N sequential fusion authentication scheme has been developed using finger vein technology combined with cancellable technology. This scheme allows users to make payments without the need to enter an ID, relying solely on finger vein authentication. The integration of these technologies has significantly enhanced user convenience during payment transactions.

Walkthrough Finger Vein Authentication:

Finger vein authentication technology has been implemented for the security gates of a high-traffic facility. Users can simply hold their fingers over a sensor while walking through the gates to achieve accurate personal identification. The centralized server manages the finger vein data of employees, enabling any branch to implement finger vein authentication after the employees have completed the registration process. This technology is well-suited for applications in office buildings and event venues that

demand both high accuracy and high-speed throughput. The technology has been evaluated in terms of throughput, long-term authentication accuracy, and usability. The results showed that throughput and usability were comparable to conventional contact-less card systems. Temperature differences had a minimal impact on the false rejection rate, ensuring smooth operation.

Enhanced Convenience through Government-Industry Partnership:

The availability of a facility that connects finger vein templates with Aadhaar cards could enable widespread usage of finger vein authentication for personal identity verification in public settings using camera-equipped devices. This would offer various conveniences, such as opening bank accounts via smartphones without visiting a physical branch or certifying official documents at public terminals (e.g., convenience stores) even without carrying the Aadhaar card. It would provide greater flexibility and accessibility for individuals in performing various transactions and verifications.

3. UIDAI and Finger vein

Liveliness of person is not checked for UIDAI.

Finger print pattern copy can be utilized whereas this is not the case with finger vein.

Finger vein scanner cost is expensive.

UIDAI only use IRIS, and finger print. IRIS is used for identification and finger print is used for verification. Face recognition system in UIDAI is still in POC (proof of concept) phase.

UIDAI can utilize finger vein for verification.

4. Impact on Size and Cost of Implementation and other challenges in adopting this technology in Banks:

The development of finger vein authentication using a visible-light camera required addressing three main technical challenges. Firstly, it was necessary to reliably identify finger vein patterns without relying on infrared light. Secondly, the system had to accurately identify vein patterns irrespective of the finger's orientation over the camera. Lastly, enhancing the authentication accuracy was crucial to enable its application in diverse scenarios.

Cost of implementation of technology is a major challenge. When researching this solution, the researchers had considered other inexpensive biometric authentication methods such as fingerprint authentication.

Traditional finger vein authentication technologies rely on dedicated hardware that uses near-infrared light to capture high-quality images of blood vessels. While this technology ensures high authentication accuracy, it faces challenges in the financial business-to-consumer (B2C) market due to the following reasons:

Price Competitiveness: The cost of the hardware is relatively higher compared to alternative solutions like one-time password (OTP) tokens, making it less feasible for widespread adoption in personal Internet banking and B2C applications.

Limited Portability: Finger vein authentication units are commonly peripheral devices that connect to a PC or host device using USB. This dependency on a host device and cables restricts their portability and convenience when used outside of a controlled environment.

Product Life Cycle Management: Finger vein authentication units require strict management throughout their entire life cycle, including distribution, operation, upgrades, and secure disposal. Expecting end users in the B2C market to handle these responsibilities is impractical, and there is a risk of unauthorized use, disassembly, or tampering by malicious individuals.
These challenges highlight the need for advancements in finger vein authentication technology to address cost, portability, and product life cycle management concerns for wider adoption in the B2C market.
Researchers have made advancements in finger vein authentication technology by developing a solution that utilizes visible-light cameras. This innovation aims to enable the use of finger vein authentication in the financial B2C market and address the challenges mentioned earlier. Instead of relying on dedicated finger vein authentication units, this technology leverages the widespread availability of visible-spectrum color cameras found in smartphones and tablets. By utilizing color images captured by these cameras, finger vein authentication can be achieved through software alone. This approach offers significant cost reduction by eliminating the need for additional hardware. It also enhances portability by allowing authentication to be performed on widely-used smartphones and tablets. The technology facilitates life cycle management through distribution via app stores, easy addition of functions, and online version updates. Additionally, by eliminating dedicated hardware, the risk of failure in aging products and potential tampering is reduced. At the end of its useful life, the authentication software and associated data can be safely deleted by imposing usage limitations.

The research findings indicate that the technology performs well without any performance issues. Moving forward, further considerations will be needed to customize the product specifications, including size and cost, to align with market requirements. Additionally, exploring commercialization strategies that are viable from a business perspective will be crucial for successful implementation of the technology.

FEEDBACK RECEIVED ON FINAL REPORT AND OUR RESPONSES

1. **Add further details on usability/ deployment of your research work.**

Our Response: The usability of our research work holds paramount significance in the context of the banking and finance sector, where security, privacy, and user experience are critical. Our research offers transformative opportunities for this sector, and we have meticulously considered the practical aspects of implementing our findings:

Enhanced Security: In the banking and finance sector, maintaining the highest level of security is non-negotiable. Our research, with its transformed biometric templates and cancelability techniques, provides an advanced layer of security. It can be deployed to secure access to financial institutions, safeguarding not only the physical premises but also digital assets and customer data.

Fraud Prevention: The finance sector is particularly vulnerable to fraud, including identity theft and fraudulent transactions. Our research can be harnessed to deploy multi-factor authentication systems, where finger vein biometrics add an extra layer of security. This not only verifies the user's identity but also ensures the authenticity of transactions, reducing the risk of fraudulent activities.

Digital Banking and Internet Banking: With the growing trend toward digital banking and online financial transactions, user authentication becomes a pivotal concern. Our research can be integrated into mobile banking applications and online platforms, offering secure yet convenient authentication options. Customers can access their accounts with the assurance that their financial information remains private, even during internet banking sessions.

ATM Security: Automated Teller Machines (ATMs) are a critical touchpoint in the finance sector. Deploying finger vein biometrics at ATMs can drastically reduce the risk of card skimming and unauthorized cash withdrawals. Customers can use ATMs with the confidence that their financial transactions are protected.

Data Center Access: For financial institutions, secure data center access is vital. Our research can be applied to control access to data centers where sensitive financial data

is stored. This ensures that only authorized personnel can enter these highly secure environments.

Regulatory Compliance: The finance sector is subject to stringent regulatory requirements. Our research aligns with regulatory demands for robust user authentication and data protection. Implementing our findings aids financial institutions in complying with regulations such as GDPR and PCI DSS.

Customer Trust: Trust is the bedrock of the banking and finance industry. By deploying our research, financial institutions can demonstrate their commitment to customer data protection and privacy, particularly in the realm of Internet banking. This fosters trust among clients, potentially attracting more customers to use online banking services.

Scalability: We recognize that the finance sector often deals with large customer bases. Our research is designed to be scalable, accommodating millions of users without compromising security or performance. This ensures that financial institutions can readily deploy our solutions across their operations, including internet banking platforms.

User Experience: While security is paramount, user experience is also crucial. Our research allows for a seamless and user-friendly experience. Customers can enroll their finger vein biometrics easily, and the authentication process is quick and intuitive, whether they are accessing their accounts at a physical branch or via internet banking.

Deployment:

The architecture comprises seven interconnected components as shown in Figure 56. It begins with the Finger Vein Scanning Device, a specialized hardware system that captures near-infrared images of finger veins. The Features Extraction Software processes these images, extracting relevant features to create digital representations of vein patterns. Biometric Template Generation transforms these features into secure templates. The Cancelability Software enhances security by applying techniques like multiline neighboring relations. High-End Servers securely store these templates. During authentication, Matching compares user-provided data to templates. Finally,

End User Applications, integrated with the architecture, use this biometric data for secure access, making it suitable for applications in banking and finance.

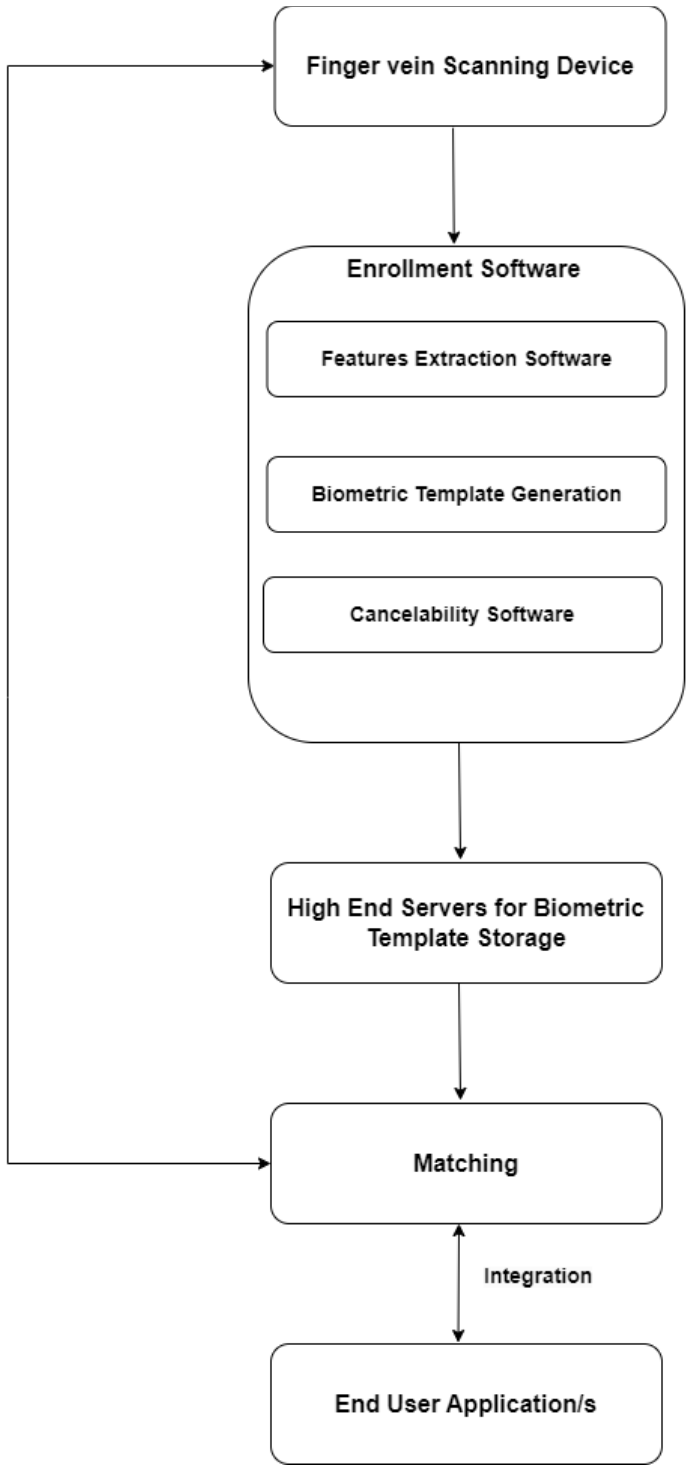


Figure 56: High Level Deployment Architecture of Finger vein with Cancelability

In conclusion, the banking and finance sector, including Internet banking, is poised to benefit significantly from the usability and deployment of our research. It offers

enhanced security, fraud prevention, regulatory compliance, and a better overall experience for both customers and institutions, particularly in the rapidly evolving landscape of online and digital banking. We are committed to collaborating with financial organizations to integrate our findings into their systems, ultimately fortifying the sector against emerging threats and providing peace of mind to customers. Our research aligns with the sector's vision of a secure, efficient, and customer-centric financial ecosystem across physical and digital channels.

2. Find Use Case/s

Our Response: Our research on finger vein biometrics and cancelability techniques holds substantial promise for practical implementation within the banking and finance sector, offering several impactful use cases. These applications align with the industry's growing need for robust security, user authentication, and fraud prevention. Here are prominent use cases:

Multi-Factor Authentication (MFA): The banking and finance sector relies heavily on user authentication for account access. Our research provides an ideal solution for implementing MFA. By integrating finger vein biometrics as one of the authentication factors, financial institutions can significantly enhance security. Users would need to provide both something they know (like a password) and something they are (finger vein biometrics), creating a formidable barrier against unauthorized access.

Secure Branch Access: Traditional bank branches still play a pivotal role in the industry. Our research can be deployed to enhance physical security within these branches. Employees can use finger vein biometrics for secure access to restricted areas where sensitive operations are conducted, such as the vault or data center. This reduces the risk of unauthorized access and internal fraud.

ATM Security: ATMs remain a critical service touchpoint. Implementing finger vein biometrics at ATMs can significantly reduce the risk of card skimming and PIN theft. Customers can securely access their accounts by scanning their finger veins, ensuring that only authorized users can withdraw cash or perform transactions.

Internet Banking and Mobile Apps: As digital banking gains prominence, securing online transactions becomes paramount. Our research can be integrated into banking

apps and internet banking platforms to provide a secure and user-friendly authentication method. Users can log in or authorize transactions using finger vein biometrics, ensuring that their online financial activities are safeguarded against unauthorized access.

Call Center Authentication: Call centers are often used for customer support and financial inquiries. By using finger vein biometrics for customer authentication during phone interactions, financial institutions can ensure that confidential information is only disclosed to authorized customers, mitigating the risk of identity theft.

Data Center Security: The security of data centers that store sensitive financial information is critical. Our research can be employed to control physical access to these facilities. Only authorized personnel with registered finger vein biometrics would be allowed entry, fortifying data security.

Compliance and Audit Trails: Regulatory compliance is a cornerstone of the banking and finance sector. Our research can help institutions comply with data security regulations by providing a robust authentication method. Additionally, it can contribute to detailed audit trails, helping organizations monitor and report access to sensitive financial data.

Customer Onboarding: During the customer onboarding process, finger vein biometrics can be used for identity verification, streamlining the Know Your Customer (KYC) procedures. This not only enhances security but also expedites the customer registration process.

Benefits of Finger vein technology over existing biometric technologies:

Innate Liveness Check: Finger vein biometrics inherently includes a liveness check, requiring a live finger with blood flow for authentication. This ensures not only identity verification but also confirms the presence and vitality of the individual during the authentication process.

Stability Over Time: Finger vein patterns remain stable throughout an individual's life, with minimal chances of alteration. This longevity and consistency make it a dependable choice for biometric authentication.

Subdermal Patterns: Finger vein patterns are hidden beneath the skin's surface, making them extremely difficult to forge or tamper with. Unlike surface-level biometrics like fingerprints, finger vein patterns cannot be easily replicated.

Highly Secure: The subdermal nature of finger vein patterns, combined with the requirement for blood flow, adds an extra layer of security, making it resistant to spoofing attempts, including the use of artificial fingers or images.

Non-Intrusive: Finger vein recognition is non-intrusive and contactless, making it more hygienic and user-friendly, especially in applications where hygiene is critical, such as healthcare or finance.

Low False Acceptance Rate: Finger vein technology offers a low False Acceptance Rate (FAR), minimizing the chances of unauthorized access.

Versatile Applications: Finger vein biometrics can be applied in various domains, including access control, financial transactions, healthcare, and identity verification, due to its robustness and security.

These unique features collectively establish finger vein biometrics as a highly secure, reliable, and versatile authentication solution, setting it apart from other biometric technologies.

These use cases demonstrate the versatility and practicality of implementing our research within the banking and finance sector. By integrating finger vein biometrics and cancelability techniques, financial institutions can elevate their security standards, foster trust among customers, and ensure regulatory compliance in an ever-evolving landscape of digital and physical banking services. Our research provides a holistic approach to addressing the sector's security and authentication needs while enhancing the overall customer experience.

3. Estimate probable cost of implementation

Our Response: The estimation of likely implementation costs for our research poses a distinct challenge due to several inherent factors in the current research phase. Notably, the technology remains in its developmental stages, and the availability of commercial products aligning

precisely with our research goals is limited, often introducing various technological and operational constraints.

In light of these obstacles, we have diligently worked to offer a cost estimate that serves as an initial guideline for financial planning. It is crucial to underscore that this estimate is inherently tentative, given the dynamic nature of the technology and the ever-evolving landscape within the banking and finance sector.

Our tentative cost estimation encompasses various elements, including research and development costs, investments in hardware and infrastructure, integration and deployment expenses, initiatives for training and educating users, compliance and security audits, considerations for scaling and maintenance, potential partnerships with vendors, and provisions for miscellaneous expenses. Each of these categories is subject to fluctuations and adjustments as the technology matures and adapts to specific use cases in the banking and finance sector.

It is essential to reiterate that this estimate represents an initial assessment, providing a foundational framework for financial planning rather than a definitive cost projection. The actual implementation costs may vary significantly based on factors such as technological advancements, the availability of commercial solutions, evolving regulatory requirements, and unforeseen contingencies.

As our research continues to advance, our commitment remains unwavering in refining our cost estimation in harmony with the evolving landscape. We will actively monitor technological advancements, explore potential collaborations with industry leaders, and adjust our financial projections accordingly to ensure the most accurate and practical cost assessment for future deployment in the banking and finance sector. Estimating the cost of implementing finger vein biometrics with cancelability in a bank, like SBI, entails numerous variables, including the scope of implementation, branch count, security levels, and technology provider choices. However, we can offer a general cost breakdown to provide insight into the potential expenses associated with such a project:

Method 1: Using Commercial Finger Vein Scanning Devices

Hardware Costs:

Finger Vein Scanning Devices: ₹60,000 to ₹140,000 per unit (assuming an exchange rate of 70 INR per USD).

Number of Devices: Let's assume 100 devices.

Total Hardware Cost: ₹35,00,000 to ₹14,00,0000

Software Development:

Software Development/Procurement: ₹50,00,000

Integration and Customization: ₹20,00,000

Data Storage and Processing:

Data Storage Infrastructure: ₹20,00,000

Data Processing Software: ₹10,00,000

Cancelability Implementation:

Licensing Cancelability Algorithms (Depends upon Finger vein scanner vendor capabilities): ₹20,00,000- ₹50,00,000

Cancelability Algorithms and its integration with Vendor's provided solution: ₹20,00,000

Deployment and Integration:

Deployment and Installation: ₹10,00,000

Integration Costs with final product: ₹20,00,000

Maintenance and Support:

Annual Maintenance: ₹20,00,000

Regulatory Compliance:

Compliance Costs: Varies depending on your location and regulations. Budget accordingly.

Training and User Education:

Training Costs: ₹5,00,000

Contingency and Miscellaneous Costs:

Allocate around 10-20% of the total project budget as a contingency: ₹10,00,000

Total Estimated Cost: ₹2,65,00,000 to ₹2,95,00,000. Please note that these are approximate figures, and the actual costs may vary based on specific project factors and any fluctuations in expenses or exchange rates.

Method 2: Developing Custom Finger Vein Devices

Hardware Development:

Research and Development: ₹30,00,000 (depending on complexity)

Manufacturing Costs: ₹10,00, 000 (Assuming 100 devices)

Note: During our research journey, we have explored design of a finger vein scanning device and can potentially develop it in collaboration with a reputable research institute, university, or organizations like IDRBT (Institute for Development and Research in Banking Technology) or IIBF (Indian Institute of Banking and Finance). Additionally, it's important to note that no commercially available scanning devices provide raw finger vein images; they typically provide templates.

Software Development:

Software Development: ₹5,00,000

Feature Extraction Algorithm: ₹2,00,000

Data Storage and Processing:

Data Storage Infrastructure: ₹20,00,000

Data Processing Software: ₹10,00,000

Cancelability Implementation:

Licensing Cancelability Algorithms: ₹5,00,000

Development: ₹20,00,000

Deployment and Integration:

Deployment and Installation: ₹5,00,000

Integration Costs: ₹10,00,000

Maintenance and Support:

Annual Maintenance: ₹5,00,000

Regulatory Compliance:

Compliance Costs: Varies depending on your location and regulations. Budget accordingly.

Training and User Education:

Training Costs: ₹5,00,000

Contingency and Miscellaneous Costs:

Allocate around 10-20% of the total project budget as a contingency: ₹7,00,000 to ₹14,00,000

Total Estimated Cost (without minimum or maximum range): ₹134,00,000 to ₹141,00,000. Please note that these are approximate figures, and the actual costs may vary based on specific project factors and any fluctuations in expenses or currency exchange rates.

Intended Use of 100 Devices:

The allocation of 100 finger vein scanning devices is a strategic investment aimed at enhancing our banking operations and ensuring a secure and efficient customer experience. These devices will serve as a versatile biometric authentication solution that can be flexibly integrated into various aspects of our banking ecosystem. Our intention is to harness the potential of finger vein technology for multiple use cases, depending on the evolving needs and decisions of our management.

Cost Allocation:

The estimated cost presented in our analysis covers the integration of these 100 finger vein scanning devices with our existing applications and systems. This includes the development or procurement of software, data storage infrastructure, cancelability implementation, deployment, maintenance, training, and compliance-related expenses. It's important to note that this cost estimation is based on the current state of technology and market conditions.

Furthermore, it's crucial to highlight that as technology in the field of finger vein biometrics matures and research progresses, we anticipate significant cost reductions in device production and system implementation. These advancements will contribute to improved cost-efficiency in the long term.

In summary, the allocation of 100 finger vein scanning devices is part of our strategic approach to embracing biometric authentication in the banking sector. These devices will be deployed across various use cases, with the flexibility to adapt to emerging needs. The estimated cost accounts for initial integration, and we anticipate cost savings in the future as the technology evolves.

Our Recommendation:

We strongly recommend pursuing the second method of implementing finger vein technology in the banking sector. This choice is justified by several compelling reasons:

i. Unavailability of Commercially Accessible Finger Vein Images:

Commercially available finger vein scanners typically provide pre-processed finger vein biometric templates rather than raw finger vein images. This limitation makes it impossible to design and develop solutions that require access to the raw finger vein images, such as research into feature extraction algorithms or the creation of custom databases. By opting for the second method, which involves developing an in-house finger vein scanner capable of capturing raw images, we gain direct access to the essential data required for comprehensive research and development.

ii. Limited Availability of Finger Vein Datasets:

In India and globally, the availability of finger vein image datasets for research purposes is scarce. Obtaining permission to access datasets from the few universities and research institutions that possess such resources can be challenging and time-consuming. By pursuing the second method, we mitigate these obstacles. We can create our own dataset, ensuring full control and accessibility, thereby expediting research and development efforts.

iii. Enhanced Security and Data Integrity:

Handling sensitive biometric data, such as finger vein patterns, demands the highest level of security and data integrity. Building an in-house product provides greater control over data storage, encryption, and access protocols, reducing the risk of data breaches or misuse. This approach aligns with industry standards for safeguarding personal identifiable information (PII) and enhances user trust.

iv. Collaboration Opportunities:

The second method opens doors for collaboration with other research institutions, both nationally and internationally. By developing our finger vein scanner and datasets, we can engage in collaborative research projects and knowledge sharing, fostering innovation and staying at the forefront of finger vein technology advancements. Notably, with UIDAI (Unique Identification Authority of India) exploring the potential

use of finger vein technology, our in-house expertise positions us favourably for future collaborations in this critical domain.

v. Cost Savings and Scalability:

As research and technology in finger vein biometrics mature, the cost of devices can be significantly reduced through in-house development. We can scale our solutions without dependency on external vendors like Hitachi, saving substantial amounts of money in the long term. This cost-efficiency aligns with prudent financial management practices and ensures that the banking sector can benefit from this technology without incurring high ongoing expenses.

In conclusion, the second method offers numerous advantages, including enhanced research capabilities, greater control over data, opportunities for collaboration, and substantial cost savings as the technology matures. It aligns with the long-term goals of the banking sector and India's broader biometric authentication landscape, making it the recommended approach for the implementation of finger vein technology in the banking industry.

4. Kindly also add Executive Summary in your report.

Our Response: In an age where secure identity verification is paramount, the field of biometrics has emerged as a transformative technology. This research report represents a comprehensive and pioneering exploration of the promising domain of finger vein biometrics, aimed at advancing understanding and practical applications in this evolving field.

The study embarked on an empirical journey, identifying three benchmark databases—UTFV, HKPU, and FV-USM—as foundational resources for in-depth analysis. Our commitment to thorough experimentation led to the design of a meticulously crafted experimental setup, tailored to extract discriminative features from finger vein images effectively. Crucially, the selection of a binarization threshold value of 155 emerged from extensive testing, offering a finely tuned balance between feature richness and noise reduction in the output binarized image.

A pivotal and innovative contribution of this research is the development and application of the multiline neighbouring relations generation cancelability technique to the extracted features. This technique serves as a linchpin, significantly enhancing the security and privacy aspects of finger vein biometrics. By integrating this technique into our framework, we have fortified the foundations upon which future applications will be built, ensuring that user data remains confidential and protected.

The essence of our pioneering contribution is vividly demonstrated by the remarkable improvement in the Equal Error Rate (EER) achieved through the utilization of transformed biometric templates. In direct comparison to untransformed finger vein templates, this research has unequivocally proven the tangible and transformative enhancements in recognition accuracy and security. This empirical evidence not only substantiates the effectiveness of our methodology but also underscores the profound potential of finger vein biometrics as a secure means of identity verification.

However, this research is not the culmination but the commencement of a remarkable journey into the vast potential of finger vein biometrics. The road ahead is marked by multifaceted exploration and expansion. A multitude of feature extraction methods and cancelability techniques remain untapped, each offering the promise of unveiling new dimensions and possibilities in this field. Our unwavering commitment to diverse experimentation is a testament to our dedication to the relentless pursuit of innovation.

Furthermore, we recognize the imperative for expansion. The inclusion of additional datasets, encompassing a broader spectrum of scenarios and subjects, is not just a scientific imperative but a practical necessity. Such expansion will augment the robustness and reliability of finger vein biometrics, enabling its seamless integration into a myriad of real-world applications, from secure access control to financial transactions.

In conclusion, this research is a shining beacon of innovation and progress within the realm of finger vein technology. It promises to make profound and lasting contributions to the field of biometric verification. As we continue to push the boundaries of what is possible in this exciting frontier, our findings resonate with the potential of biometrics to shape a more secure, connected, and privacy-respecting future. This research is not

merely a report but a clarion call for the continued exploration of the limitless possibilities inherent in finger vein biometrics.

Bibliography

[1] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, A. S. Albahri, O. S. Albahri, M. A. Alsalem and K. I. Mohammed: Real-Time Remote Health Monitoring Systems Using Body Sensor Information and Finger Vein Biometric Verification: A Multi-Layer Systematic Review (2018)

[2] A. H. Mohsin, A. A. Zaidan, B. B. Zaidan, O. S. Albahri, Shamsul Arrieya Bin Ariffini, Ahmed Alemrani, Odai Enaizan, Ali. H. Shareef, Ali Najm Jasim, N. S. Jalood, M. J. Baqeri, A. H. Alamood, E. M. Almahdi, A. S. Albahri, M. A. Alsalem, K. I. Mohammed, H. A. Ameen and Salem Garfani : Finger Vein Biometrics: Taxonomy Analysis, Open Challenges, Future Directions and Recommended Solution for Decentralised Network Architectures(2020)

[3] Babak Maser and Jutta Hämmerle-Uhl: Finger Vein Image Compression with Uniform Background (2019)

[4] Borui Hou and Ruqiang Yan: Convolutional Auto-Encoder Model for Finger-Vein Verification (2019)

[5] Byung-Hoon Lee, Tea-Yeong Hah, Won-Ho Jeong and Kyung-Seok Kim: Enhanced Approach for Finger-Vein Extraction

[6] Chih-Hsien Hsia: New Verification Strategy for Finger-Vein Recognition System (2018)

[7] Dongdong Zhaoa, Hui Maa, Zedong Yanga, Jianian Lia and Wenbo Tiana: Finger vein recognition based on lightweight CNN combining centre loss and dynamic regularization. (2020)

[8] Haiying Liu, Lu Yang, Gongping Yang and Yilong Yin : Discriminative Binary Descriptor for Finger Vein Recognition(2018)

[9] Hanwen Yang, Peiyu Fang and Zhiang Hao : A GAN-based Method for Generating Finger Vein Dataset (2020)

[10] Hengyi Ren, Lijuan Sun, Jian Guo, Chong Han and Fan Wu: Finger vein recognition system with template protection based on convolutional neural network (2021)

[11] Hongyu Ren , Da Xu and Wenxin Li : Modeling the Uncertainty in Finger-Vein Authentication by the Gaussian Mixture Model (2017)

[12] Huafeng Qin and Mounim A. El Yacoubi: Deep Representation for Finger-vein Image Quality Assessment (2017)

[13] Javad Khodadoust, Miguel Angel Medina, Raúl Monroy, Ali Mohammad Khodadoust and Seyed Saeid Mirkamali:A multibiometric system based on the fusion of fingerprint, finger-vein, and finger-knuckle-print(2021)

[14] Jong Ming Song, Wan Kim and Kang Ryoung Park: Finger-Vein Recognition Based on Deep DenseNet Using Composite Image (2019)
[15] Kashif Shaheed , Hangang Liu, Gongping Yang, Imran Qureshi , Jie Gou and Yilong Yin : A Systematic Review of Finger Vein Recognition Techniques (2018)
[16] Lu Yang, Gongping Yang, Yilong Yin, and Xiaoming Xi: Finger Vein Recognition with Anatomy Structure Analysis
[17] Manjit Singh, Sunil Kumar Singla : Convolutional Neural Network Based Deep Feature Learning for Finger-vein Identification
[18] Michael Linortner and Andreas Uhl: Towards Match-on-Card Finger Vein Recognition (2021)
[19] Nada Alay 1 and Heyam H. Al-Baity: Deep Learning Approach for Multimodal Biometric Recognition System Based on Fusion of Iris, Face, and Finger Vein Traits
[20] Ridvan Salih Kuzu, Emanuela Piciucco ,Emanuele Maiorana and Patrizio Campisi : On-the-Fly Finger-Vein-Based Biometric Recognition Using Deep Neural Networks(2020)
[21] Rig Das, Emanuela Piciucco, Emanuele Maiorana, and Patrizio Campisi: Convolutional Neural Network for Finger-Vein-based Biometric Identification (2018)
[22] Shilei Liu, Guoxiong Xu, Yi Zhang and Wenxin Li : A Study of Temporal Stability on Finger-Vein Recognition Accuracy Using a Steady-State Model (2018)
[23] Wan Kim, Jong Min Song and Kang Ryoung Park : Multimodal Biometric Recognition Based on Convolutional Neural Network by the Fusion of Finger-Vein and Finger Shape Using Near-Infrared (NIR) Camera Sensor
[24] Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng, Junaid Chaudhry, Erwin Adi and Craig Valli : Securing Mobile Healthcare Data: A Smart Card based Cancelable Finger-vein Bio-Cryptosystem(2018)
[25] Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng, Jucheng Yang, and Craig Valli : Securing Deep Learning Based Edge Finger-vein Biometrics with Binary Decision Diagram(2019)
[26] Wenming Yang, Changqing Hui, Zhiquan Chen, Jing-Hao Xue and Qingmin Liao : FV-GAN: Finger Vein Representation Using Generative Adversarial Networks(2019)
[27] Wenxiong Kang, Yuting Lu, Dejian Li and Wei Jia : From Noise to Feature: Exploiting Intensity Distribution as a Novel Soft Biometric Trait for Finger Vein Recognition(2018)
[28] Wenxiong Kang, Hongda Liu, Wei Luo and Feiqi Deng : Study of a full-view 3D Finger Vein Verification Technique (2019)

[29] Xianjing Meng, Jinwen Zheng, Xiaoming Xi, Qing Zhang and Yilong Yin : Finger Vein Recognition based on Zone-based Minutia Matching (2020)

[30] Xinwei Qiu, Wenxiong Kang□, Senping Tian, Wei Jia and Zhixing Huang : Finger Vein Presentation Attack Detection Using Total Variation Decomposition(2017)

[31] Yakun Zhang, Weijun Li, Liping Zhang, Xin Ning, Linjun Sun and Yaxuan Lui: Adaptive Learning Gabor Filter for Finger-Vein Recognition

[32] Zhiang Hao, Peiyu Fang and Hanwen Yang : Finger Vein Recognition Based on Multi-Task Learning (2020)

[33] Ton B, Veldhuis R (2012) University of Twente Finger Vascular Pattern UTFVP) dataset. https://www.utwente.nl/en/eemcs/ds/downloads/utfvp/

[34] Khalid, Syazana-Itqan & Radzi, Feeza & Mohd Saad, Norhashimah & Abdul Hamid, Norihan & Bin Mohd Saad, Wira Hidayat. (2016). A Review of Finger-Vein Biometrics Identification Approaches. Indian Journal of Science and Technology. 9. 10.17485/ijst/2016/v9i32/99276.

[35] Miura N, Nagasaka A, Miyatake T. Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification. Machine vision and applications. 2004 Oct;15(4):194-203.

[36] R. Wang, G. Wang, Z. Chen, Z. Zeng, and Y. Wang, “A palm vein identification system based on Gabor wavelet features,” Neural Computing and Applications, vol. 24, no. 1, pp. 161-168, 2014.

[37] S. Qiu, Y. Liu, Y. Zhou, J. Huang, and Y. Nie, “Finger-vein recognition based on dual-sliding window localization and pseudo-elliptical transformer,” Expert Systems with Applications, vol. 64, pp. 618-632, 2016.

[38] H. Qin, and M. A. El-Yacoubi, “Deep representation-based feature extraction and recovering for finger-vein verification,” IEEE Transactions on Information Forensics and Security, vol. 12, no. 8, pp. 1816-1829, 2017.

[39] H. Qin, and M. A. El Yacoubi, “Deep Representation for Finger-vein Image Quality Assessment,” IEEE Transactions on Circuits and Systems for Video Technology, 2017.

[40] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks." pp. 1097-1105.

[41] K. Simonyan, and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” arXiv preprint arXiv:1409.1556, 2014.

[42] K. Simonyan, and A. Zisserman, “Very deep convolutional networks for large-scale image recognition,” arXiv preprint arXiv:1409.1556, 2014.

[43] Kang W, Liu H, Luo W, Deng F. Study of a full-view 3D finger vein verification technique. IEEE Transactions on Information Forensics and Security. 2019 Jul 15;15:1175-89.
[44] Hou B, Yan R. Convolutional autoencoder model for finger-vein verification. IEEE Transactions on Instrumentation and Measurement. 2019 Jun 5;69(5):2067-74.
[45] X. Xi, L. Yang, and Y. Yin, "Learning discriminative binary codes for finger vein recognition," Pattern Recognition, vol. 66, pp. 26–33, 2017.
[46] M. S. M. Asaari, S. A. Suandi, and B. A. Rosdi, "Fusion of band limited phase only correlation and width centroid contour distance for finger based biometrics," Expert Systems with Applications, vol. 41, no. 7, pp.3367 – 3382, 2014.
[47] L. Yang, G. Yang, Y. Yin, and X. Xi, "Finger vein recognition with anatomy structure analysis," IEEE Transactions on Circuits and Systems for Video Technology, vol. PP, no. 99, pp. 1–1, March 2017.
[48] B. T. Ton and R. N. J. Veldhuis, "A high quality finger vascular pattern dataset collected using a custom designed capturing device," in Proceedings of the 2013 International Conference on Biometrics (ICB), Madrid, Spain, 2013, pp. 1–5.
[49] C. Kauba, E. Piciucco, E. Maiorana, P. Campisi, and A. Uhl, "Advanced variants of feature level fusion for finger vein recognition," in 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), Sept 2016, pp. 1–7.
[50] Das R, Piciucco E, Maiorana E, Campisi P. Convolutional neural network for finger-vein-based biometric identification. IEEE Transactions on Information Forensics and Security. 2018 Jun 25;14(2):360-73.
[51] Kang W, Lu Y, Li D, Jia W. From noise to feature: Exploiting intensity distribution as a novel soft biometric trait for finger vein recognition. IEEE transactions on information forensics and security. 2018 Aug 21;14(4):858-69.
[52] Kuzu RS, Piciucco E, Maiorana E, Campisi P. On-the-fly finger-vein-based biometric recognition using deep neural networks. IEEE Transactions on information Forensics and Security. 2020 Feb 3;15:2641-54.
[53] C. Xie and A. Kumar, "Finger vein identification using convolutional neural network and supervised discrete hashing," Pattern Recognit. Lett., vol. 119, pp. 148–156, Mar. 2019.
[54] E. Jalilian and A. Uhl, "Finger-vein recognition using deep fully convolutional neural semantic segmentation networks: The impact of training data," in Proc. IEEE Int. Workshop Inf. Forensics Secur. (WIFS), Dec. 2018, pp. 1–8.

[55] W. Kim, J. M. Song, and K. R. Park, “Multimodal biometric recognition based on convolutional neural network by the fusion of finger-vein and finger shape using near-infrared (NIR) camera sensor,” Sensors, vol. 18, no. 7, p. 2296, Jul. 2018.
[56] Linortner M, Uhl A. Towards match-on-card finger vein recognition. In Proceedings of the 2021 ACM Workshop on Information Hiding and Multimedia Security 2021 Jun 17 (pp. 87-92).