REPUBLIC OF TÜRKİYE
ALTINBAŞ UNIVERSITY
Institute of Graduate Studies
Electrical and Computer Engineering

STREAMLINING LIFE CERTIFICATE AUTHENTICATION BIOMETRIC INTEGRATION WITH FINGERPRINT AND VEIN RECOGNITION

Ahmed Safaa Salim SALIM

Master's Thesis

Supervisor

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

İstanbul, 2025

STREAMLINING LIFE CERTIFICATE AUTHENTICATION BIOMETRIC INTEGRATION WITH FINGERPRINT AND VEIN RECOGNITION

Ahmed Safaa Salim SALIM

Electrical and Computer Engineering

Master's Thesis

ALTINBAŞ UNIVERSITY

2025

The thesis titled STREAMLINING LIFE CERTIFICATE AUTHENTICATION BIOMETRIC INTEGRATION WITH FINGERPRINT AND VEIN RECOGNITION prepared by AHMED SAFAA SALIM SALIM and submitted on 30/01/2025 has been **accepted unanimously** for the degree of Master of Science in Electrical and Computer Engineering.

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM
Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Abdullahi Abdu IBRAHIM	Department of Computer Engineering, Altınbaş University	___________
Assoc. Prof. Dr. Sefer KURNAZ	Department of Computer Engineering, Altınbaş University	___________
Asst. Prof. Dr. Tarik Abed MOHAMMAD	Department of Computer Engineering, Kirkuk University	___________

I hereby declare that this thesis meets all format and submission requirements for a Master's thesis.

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Ahmed Safaa Salim SALIM

Signature

DEDICATION

With deep gratitude, I dedicate this thesis to my parents, who have been a great support in every step I took, to my friends and family members, and to everyone who stood by me during this important and challenging phase. Thank you, Mom and Dad, for your unwavering encouragement and strength, which helped me overcome obstacles and achieve this accomplishment.

PREFACE

Thanks to Allah for giving me this opportunity, the strength, and the patience to finally complete my thesis after all the challenges and difficulties. First and foremost, I would like to express my greatest gratitude to my advisor, Asst. Prof. Dr. Abdullahi Abdu Ibrahim, has guided and helped me a lot throughout my MSc study and research. I am particularly grateful to my family. Finally, I would like to take this opportunity to thank all my friends and colleagues. To those who indirectly contributed to this research, your kindness means a lot to me. Thank you very much.

ABSTRACT

STREAMLINING LIFE CERTIFICATE AUTHENTICATION: BIOMETRIC INTEGRATION WITH FINGERPRINT AND VEIN RECOGNITION

SALIM, Ahmed Safaa Salim

M.Sc., Electrical and Computer Engineering, Altınbaş University,

Supervisor: Asst. Prof. Dr. Abdullahi Abdu IBRAHIM

Date: 01/2025

Pages: 79

With the rapid advancement of technology worldwide, there is an increasing demand for innovative solutions to address challenges in managing and delivering public services, particularly for pensioners. One key challenge faced by institutions responsible for disbursing financial entitlements to pensioners is the "proof of life" verification process, which is often time-consuming and prone to errors. This thesis proposes a digital solution that enhances security and accuracy by combining two biometric authentication methods—fingerprint and vein recognition. By integrating these complementary biometric techniques, the system significantly improves the accuracy of the "proof of life" process. Experimental results demonstrated that the dual-authentication system achieved higher accuracy compared to using a single method, providing over 87.07% accuracy in verifying pensioners' identity, with verification times under 4 seconds. This efficient and secure approach ensures that eligible pensioners can continue receiving their pensions without delays, benefiting both pensioners and service providers.

Keywords: Vein Recognition, Fingerprint Recognition, Security Enhancement, Biometric Verification, Proof of Life Verification, Accuracy Improvement.

TABLE OF CONTENTS

Pages

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

BBVA	:	Banco Bilbao Vizcaya Argentaria
BPDFHE	:	Brightness Preserving Dynamic Fuzzy Histogram Equalization
CDF	:	Cumulative Distribution Function
CN	:	Crossing Number
DLC	:	Digital Life Certificate
FFT	:	Fast Fourier Transform
NADRA	:	National Database and Registration Authority
NMS	:	Non-Maxima Suppression
NRI	:	Near Infrared
PTAD	:	Pension Transitional Arrangement Directorate
RIO	:	Region of Interest
SSL	:	Secure Sockets Layer

1. INTRODUCTION

1.1 BACKGROUND

A Life Certificate is a document requested by retirement agencies from retirees to continue receiving their retirement pensions. Pension recipients who have not obtained a Life Certificate for this year in a timely manner can use a blank form for the purpose of the Life Certificate. Once a year, Germain retirees living in the United States receive a form 'Lebensbescheinigung' (Life Certificate) which requests confirmation that they are still eligible to receive the retirement pension. Retirees must submit an annual Life Certificate to continue receiving their retirement pensions[1][2].the Life Certificate proves that the pension holder is alive and deserves to receive the pension. Traditionally, to obtain a Life Certificate, the pensioner needs to submit the original and one copy of the Life Certificate form provided by the retirement authorities, after filling it out and properly signing it as the applicant. The current valid passport of the original applicant and a copy of it are also required. A notary cannot stamp and sign a document without a certification certificate, although many people mistakenly make this request. In the absence of this document, the embassy will issue the Life Certificate in its own format [3] [4][5]. The process of obtaining a Life Certificate is straightforward, and it is important for the pensioner to follow the correct procedure.

Life Certificate is one of the measures retirement pension providers use to deter pension fraud and identify cases where some individuals have become incapable of managing their own affairs. It ensures that the pensioner has not died and is also entitled to receive the pension. The Life Certificate is beneficial to the pensioner and the pension provider. Thus, the pensioner continues to receive the pension, and the pension provider makes sure the right person gets the pension[6]The Life Certificate is essential and cannot be overlooked. In brief, a Life Certificate is an essential document that pensioners require to continue receiving their retirement pension. It verifies that the pensioner is alive and eligible to receive the pension. The process of obtaining a Life Certificate is straightforward, and it is important for the pensioner to follow the proper procedure. The Life Certificate benefits both the pensioner and the pension provider by preventing fraud and ensuring that the pension is paid to the correct person. It is crucial for all retirees to obtain a Life Certificate annually to continue receiving their retirement pensions.

1.2 DIGITAL LIFE CERTIFICATE AND HOW DOES IT WORK

The digital life certificate (DLC) for retirees can be considered an online tool that enables retirees to prove that they are still alive and thus enables retirement agencies to disburse their pensions without the need to physically visit retirement offices, consulates, or embassies. This certificate is considered particularly suitable for the elderly who suffer from problems. They are on the move, or they live in remote areas far from retirement offices, or they may live outside the country, so it is difficult for them to visit retirement offices. However, the use of digital technologies and tools is still very limited among the elderly. While digital literacy is associated with better retirement outcomes, it has not It is widely spread among older people who face a fundamental digital divide [7][8]. In addition, the elderly are selective about spending their time, as they often prefer traditional means of communication over social media[9]. Retirement also affects the health of retirees, as retirees suffer of health problems such as ill health and difficulty in performing daily activities such as walking[10]. However, these effects can be reduced through social support, physical activity, and part-time work after retirement[11]. Furthermore, research indicates that many retirees face financial deficits due to a lack of basic financial knowledge and understanding of economic concepts [12]. developing mechanisms to address these challenges through new services that promote on-the-job learning can be an effective way to improve retirement outcomes and ensure a fulfilling life after retirement[13]. Understanding the different patterns of digital use among older adults, which are influenced by digital skills, can also be useful in promoting the use of digital tools among this population [14].

1.3 DIGITAL TRANSFORMATION'S IMPACT ON RETIREMENT SYSTEMS

Around the globe, digital transformation has been the key driver for transforming retirement systems with the use of technology to streamline their internal operations and enhance consumer satisfaction. Nevertheless, insufficiency of the digital infrastructure, digital skill gap as well as excluding effects which include lack of internet access or banking service for citizens represent significant perils associated with the successful application of digitalization into the retirement system [15]. Targeted strategies should be developed for this so that, rather than being an additional barrier to inclusivity especially among vulnerable groups, digital transformation will indeed promote equity in education [15]. One major target of the Digital Transformation Project in the Islamic Republic of Iran is digital inclusion: the government supplies SIM cards for nothing and related training free of charge as a means of hooking people.

up to the digital services [15]. To date, to make the customer's transition to electronic branches easier, in Jordan, the customer service center has launched a dedicated call center system (Call Center) that has provided high increases in transaction rates on electronic branches. Likewise, in Saudi Arabia, the General Organization for Social Insurance, which falls under the General Organization for Social Insurance, is accelerating its transition to digital transformation due to increasing customer demands and the covid-19 situation [15]. A number of organizations worldwide are reengining their business processes so as to incorporate digital-based workflows that will serve customers' demands and share services among institutions and external agencies. Besides, new technological innovations like big data technology, machine learning, and artificial intelligence have been employed to improve performance, fight corruption, and offer personalized services. However, it is necessary for adaptability of regulatory approaches as well as competencies of employees in order to realize the potential use of information and communications technology within SIs [15]

1.4 PROBLEM STATEMENT

Traditional life certificates, which are usually used to prove that the retiree is still alive and thus his continued entitlement to a pension, represent an important part in the management of retirement systems. Despite this, these paper certificates face many challenges that negatively affect both the entities to which they are issued and the retirees themselves. These problems:

a. Possibility Of Forgery: Paper life certificates are usually easy to forge, which increases the risk of fraud.

b. Expensive bureaucratic procedures: Obtaining a life certificate is often subject to a series of complex procedures that require time and effort from the person concerned to obtain it.

c. Periodic need for verification: Retirement and social security institutions require periodic verification that the retiree is still alive to continue disbursing his retirement pension, which used to be every 6 months or a year.

d. Financial costs for issuing documents: Documents often require costs for issuance, stamps, and printing, regardless of the transportation costs to reach consulates or retirement offices.

1.5 THESIS OBJECTIVES

The Purpose of this thesis is to create a DLC system for retirees who live outside their country or in remote areas so that these retirees can prove that they are still alive and that they are still eligible to receive a pension without the need to come to government institutions or authorized agents. Below are some of the goals. What the system can achieve through a DLC

a. Simplifying procedures: This comes by providing a quick means for retirees to be able to prove that they are still alive to the relevant institutions.
b. Preventing fraud: The proposed system uses two fraud prevention techniques, namely fingerprints and vein scans, to increase security and prevent fraud.

c. Enhancing administrative efficiency: The life verification process is completely automated, thus reducing the administrative burden and improving the efficiency of the retirement system.
d. Security and privacy: This system provides security to protect the personal information of retirees, and therefore only authorized persons can view the retiree's data.

In general, this system works to improve and modernize the retirement system, which benefits the body that grants the pension and the retirees themselves.

1.6 MOTIVATION

The motivation for working on the DLC is to use information technology to automate government transactions, which leads to efficiency and speed in completing government transactions. Here are some of the main motivations for using digitization to complete a life certificate.

a. Convenience and Accessibility: Using digitization to prove life allows retirees to prove that they are still alive based on a smart digital system. This is very useful for retirees who have a mobility disability or live in remote areas such as the countryside.

b. Time and Cost Efficiency: One of the motivations for using digitization in the process of proving life is to reduce the time and costs associated with the traditional process of proving life. By using a DLC, there is no need for papers or travel, and this leads to a reduction in the time cost on the retiree himself and on the body issuing the DLC

c. Reduce errors and improve accuracy: The digital transformation process usually helps reduce errors, such as data entry errors, by creating automated checkpoints.

d. Real-time Processing and Feedback: Digital systems often allow for immediate processing of submissions, providing real-time feedback or confirmation, which is not possible with manual submissions.

e. Integration with other systems: One of the motivations for using a DLC is that it can be easily integrated with other systems, providing a seamless data sharing and verification process.

In summary, using digitization in completing the life certificate provides comfort and efficiency, as it facilitates access to the retiree and vice versa. It also contributes to improving the user experience and increasing transparency.

1.7 THESIS CONTRIBUTION

DLCs contributes significantly to improving the efficiency and security of administrative procedures. Below are some of the main contributions made by this study:

a. Streamlining administrative processes: DLC streamlines administrative procedures, allowing individuals to prove life within minutes and issue a certificate.

b. Enhancing security measures and mitigating counterfeiting: DLCs are designed to be more secure than paper certificates, incorporating encryption and other digital security techniques to protect and ensure data integrity.

c. Using DLC enables faster verification of identity for digital verification and authentication. For example, a QR code can be used to verify the authenticity of the certificate.

d. By auditing the life certificate, the systems can record and track the processing details of each certificate, thereby reducing the risk of unauthorized use or forgery.

1.8 THESIS STRUCTURE

Through this study, a digital system was proposed to verify that the retiree is still alive Using fingerprints, this study consists of five chapters as follows:

Chapter 1: Provides a comprehensive overview of the life certificate concept, its importance, and the challenges it presents for retirees and pension disbursement agencies. It discusses the significance of using a digital life certificate as part of digital transformation as a quick replacement for traditional life certificates, outlining the main goals and motivations for adopting digital life certificates.

Chapter 2: Reviews biometric technologies, starting with an overview followed by a discussion on biometric traits and how these technologies operate. The chapter focuses on fingerprint and finger vein biometrics, outlining methods for capturing these patterns and highlighting the advantages and disadvantages of each. It also distinguishes between identification and verification, focusing on approaches for matching finger vein patterns.

Chapter 3: Outlines the proposed biometric verification system, covering the enrolment phase, where fingerprint and finger vein data are captured, digitized, securely transmitted, and processed. The processing involves enhancing and segmenting images as well as extracting key features, concluding with the verification of both fingerprint and finger vein data.

Chapter 4: Addresses the testing and implementation of the system, including fingerprint evaluation tests, finger vein evaluation tests, and the full system implementation.

Chapter 5: Presents the conclusion and discusses future work to improve and develop the system.

2. COMPREHENSIVE LITERATURE REVIEW

2.1 OVERVIEW

With the development of electronic systems technology, methods, and techniques for proving life have developed, and the pension disbursement authority requires retirees to appear in person to prove their lives. However, many retirement authorities in various countries have begun to introduce alternative procedures for submitting life certificates, including the DLC.

There are different ways to prove life, starting with the traditional methods of personal presence to more advanced and effective methods such as online verification[15].Traditional visits require retirees to attend embassies and consulates in person, as in Iraq, where the Iraqi Embassy in Detroit in America published the requirements for issuing a life certificate and asked retirees to come in person to obtain a life certificate[16].

In Mexico, the retirement system necessitates regular confirmation of the continued existence of its beneficiaries. In a collaborative effort, BBVA bank and Veritas Company have introduced an innovative solution enabling retirees to authenticate their existence remotely through voice biometrics. This streamlined process allows pensioners to affirm their life status via a brief telephone call, typically completed within three seconds. Initially, retirees are required to record their voice signature once. Subsequently, they can validate their existence from any location, obviating the need for physical travel or in-person appearances. This system is adept at both verifying individual identities and ensuring the uniqueness of each voice, thereby preventing any potential impersonation or fraudulent activities[17].

In Nigeria, the pension transitional arrangement directorate (PTAD)has introduced the "I am alive" platform, enabling retirees to verify their ongoing survival through two ways[18].

a. Facial verification: where retirees log in to the PTAD website using the retiree's number and bank account number, then take a photo of their face and complete the life test by tracking a body across the screen[18].

b. Fingerprint verification: Here the retiree will need a computer equipped with a fingerprint, in addition to installing specific programs, then providing personal information, how much in the first case, and then verifying with a fingerprint[18].

This verification is usually requested on an annual basis from retirees. They are notified via text messages that they must provide proof of life. The continued payment of salaries to the retiree depends on this verification process. Failure to adhere to this procedure within 6 months usually leads to suspension of the pension payment[19].

In Pakistan, the National Database and Registration Authority (NADRA), a governmental agency, plays a pivotal role in the registration of Pakistani citizens, biometric verification, and related operations. It implements various mechanisms to verify the life status of retirees.

a. Ordinary Biometric Verification: This approach is standardized, requiring retirees to visit a bank branch and undergo biometric verification biannually as part of the verification process[19], [20].

b. Tasdeeq service, where a retiree whose fingerprint or face does not appear due to old age or some illness can prove his life by answering three personal questions using artificial intelligence technology[21].

c. In the event of disability, illness, or when fingerprints are not available, the retiree can provide a life certificate signed by an authorized person as an alternative to biometric verification[22].

In India, the government has innovatively implemented a digital system known as "Jeevan Pramaan," designed to facilitate the issuance of digital life certificates. This system represents a significant shift in the administration of governmental processes, particularly aimed at simplifying the life certification process for retired government employees. Through Jeevan Pramaan, retirees can electronically submit proof of their existence using advanced biometric technologies, including fingerprint and facial recognition. This method not only provides convenience and efficiency for the users but also enhances the accuracy and security of data in government operations[23].

In the Australian, pensioners residing overseas who are aged over 80 are mandated to submit a life certificate. This process involves the completion and signing of a specified document.

The document's authenticity must be verified by an authorized individual within the country, who may be an accredited lawyer, the head of an embassy, a certified doctor, or similar authorities[24], [25].

In Italian, pensioners living overseas are required to undertake an annual certification of their continued existence. The National Institute for Social Security has implemented electronic procedures for verifying the existence of pensioners. This can be done through authorized personnel at Italian diplomatic offices or patronage institutes, who can directly upload forms or life existence certificates to the bank's computer system. This eliminates the need for postal delivery[26].

In Brazil, the government has tested new facial recognition software on 10,000 retired government employees to streamline the periodic verification used to confirm eligibility for retirement benefits, ZDNet reports. Participants in the trial will perform biometric check-ins using a mobile public services app designed by the federal government[27].

Through a quick look at many countries' experiences about life certificates, we find that most methods of proving life were based on biometric evidence such as voiceprint, fingerprint, or facial expressions.

2.2 BIOMETRIC TECHNOLOGIES

Biometric technologies refer to the use of physiological and behavioral traits to identify and verify individuals. These features are unique and permanent, allowing for accurate identification. Biometric recognition systems integrate many technologies and methods to enhance security in applications such as surveillance, access control, and criminal investigations. Some commonly used biometric attributes include fingerprints, facial features, iris patterns, voice, and signature. etc. Biometric systems can be built using a single method or multiple methods, combining different biometric features to improve accuracy. The development of biometric systems is driven by the need for convenience, efficiency, and increased security in transactions, as well as the uniqueness and wide acceptance of biometric features. These systems are widely used in many applications, including mobile devices, ATMs, smart cards, and networks. The future of biometric technology looks promising, with advances in 3D imaging and the integration of various recognition technologies[28].

2.3 BIOMETRIC TRAITS

Biometric trait refers to a characteristic that cannot be repeated between individuals and that can be relied upon to determine an individual's identity and verify it in a safe and effective way. This characteristic is considered unique and difficult to counterfeit or imitate. Therefore, it is considered important and valuable tools in security verification. With the development of technologies, it has become possible to scan and analyse. Biometric trait can be generally classified into two basic types called physiological trait and behavioral trait shown in (Figure 2.1).

Physiological traits, including fingerprints, hand geometry, ear patterns, DNA, retina, and more, are widely accepted due to their collectability, uniqueness, permanence, and affordability for verification and identification, making them a valuable tool for enhancing personal security.

Behavioural traits are characteristics that describe an individual's personality and behaviours, such as gait, keystroke, signature, handwriting, and speech, each trait of these has characteristics by which it can be identified or verified [29].

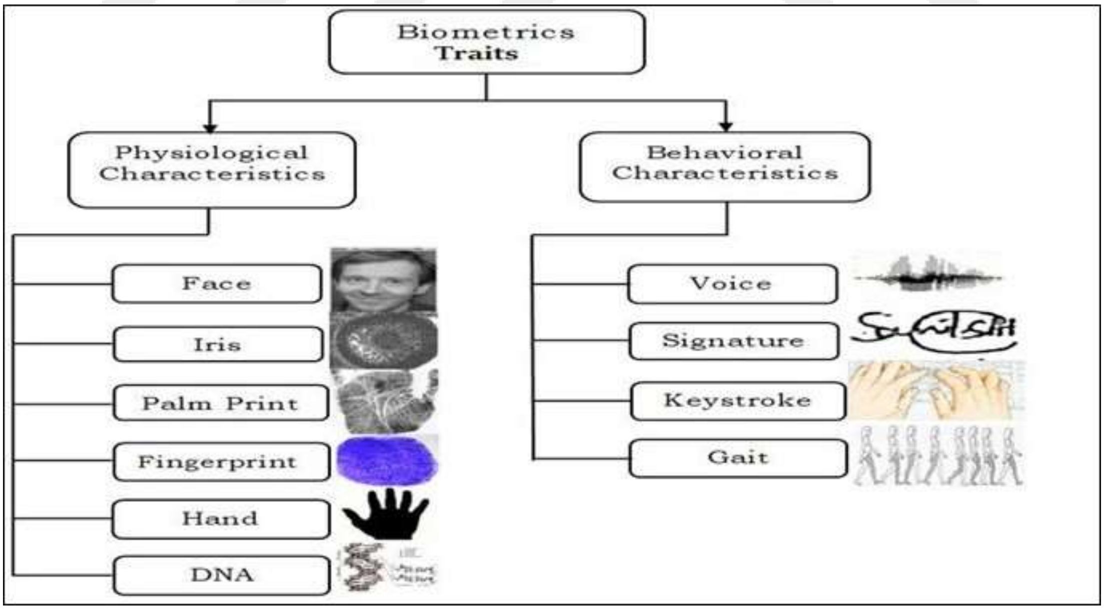


Figure 2.1: Different Types of Biometric Traits.

Table 2.1: Common Biometric and its Traits.

Biometric	Traits	Using
Fingerprint	Unique patterns of ridges and valleys on an individual's fingertips.	Used for its uniqueness in phones, computers, and security.
Signature	The style and pattern of a person's handwritten signature	Document verification
Facial geometry	Distinctive features of a person's face, including the shape	Used in smartphones, security systems, and for identity verification in various applications
Iris Recognition	Unique patterns in the coloured ring around the pupil of the eye	Used in high-security areas
Hand geometry	Shape, size of the palm, and lengths/widths of fingers	Used in some access control and time-attendance systems
Vein recognition	Vein pattern of the back of the hand	used in high-security applications
Voice	Pitch, tone, and rhythm	Useful for remote authentication over the phone or with smart devices

2.4 HOW BIOMETRIC TECHNOLOGIES WORK

In the realm of biometric technologies, despite the diversity in their complexity, capabilities, and performance levels, there are inherent similarities that unify these systems. This is evident in the foundational principles and operational mechanisms that underpin their function.

In all biometric systems, acquisition devices are used, such as cameras, fingerprint readers, or scanners, to capture biometric characteristics, and computer programs are used to extract, encrypt, and compare these characteristics. biometric systems involve three similar processes: enrollment, storage, and comparison[30]

Enrollment processes typically commence with the individual providing proof of identity, such as an identity card, ensuring their name and identity number are duly registered. Subsequently, the person's biometric data, like fingerprints or iris patterns, are captured. Following this, relevant features from this data are extracted and converted into a template utilizing specific algorithms. This template is stored in databases or on the server, sometimes it is stored in the device itself. The quality of the stored template is crucial as it directly impacts the efficacy of the verification or authentication process and may need to be updated over time. Verification is done by comparing the sample with the reference template based on the special identifier, while identification is done by comparing the sample with all the stored templates[31].

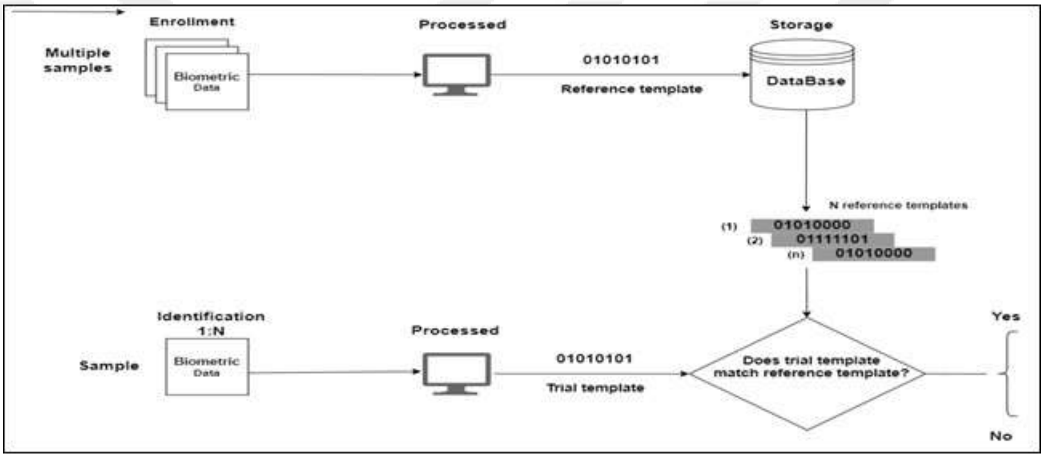


Figure 2.2: Identification Process.

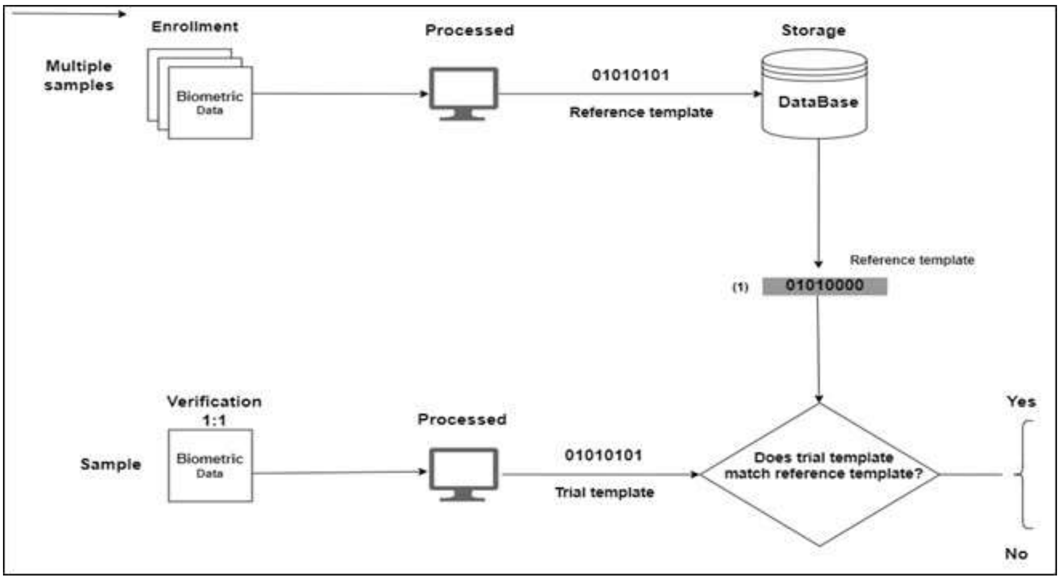


Figure 2.3: Verification Process.

2.5 BIOMETRIC FINGERPRINT

There are many human fingerprints, including fingerprints on the limb's fingers, including the senses, such as the eyes and others[32], fingerprints have been used for decades, hundreds of years, and for many purposes. a fingerprint consists of prominent lines (ridges) surrounding hidden lines (furrows) as shown in Figure 2.4 [33] . It takes different shapes on the skin of the fingertips and palms from the inside, each person has a distinctive appearance that differs from the other[34]. the indicated lines usually leave their mark on every object you touch, especially on smooth surfaces[32] It has been proven that it is not possible for two people to have the same fingerprint, that is, identical and identical, and this is impossible even in identical twins that originate from a single egg[35]. The fingerprint begins to form when the fetus is in its mother’s womb, specifically in the fourth month, and the fingerprint remains constant and distinctive for it throughout its life[34]. Two fingerprints can also be remarkably close in shape, but they never match. Therefore, the fingerprint is a conclusive and distinctive piece of evidence of a person’s personality and is applicable in every country in the world[36].

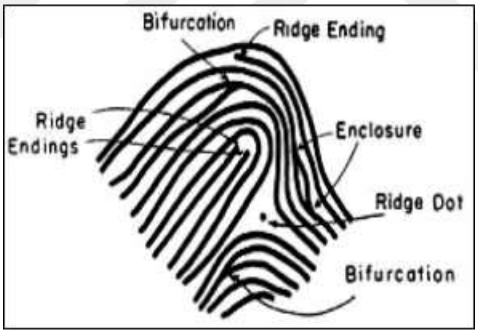


Figure 2.4: Series of Ridges, Grooves, and Points on Fingerprint Image.

Fingerprints were used by the Chinese and Japanese to seal contracts and documents, and the British used them in the nineteenth century in the Bengal region in India to differentiate between prisoners and workers, and currently those in charge of investigating criminal cases rely on them to detect criminals and thieves. This is why fingerprinting has become a reality in the world of crime. The world has undergone numerous exploratory stages before the true nature of fingerprints was comprehensively understood. In the seventeenth century, the Italian atomic scientist, Professor Marcello at the University of Bologna, included the lines of fingerprints in his research on anthropology. He elaborated on the prominent lines, their surrounding contours, and the circular patterns within them, as he elucidates[37]. But he did not clarify the possibility of using it to distinguish between people. In the year 1878, the Scottish physicist Dr. Henry, who works in Japan, discovered through laboratory traders that fingerprints are permanent and are considered the only distinguishing feature of humans. The discovery of the English scientist Henry Henry also had a great impact on the use of fingerprints to distinguish between individuals, which opened wide horizons in this field. In the year 1900, a council in India recommended that the fingerprints of criminals be taken and classified by the Indian state agencies, but the implementation of the recommendation began in the year 1903, which was considered the basis for the modern fingerprint identification system. In 1980, the US Federal Bureau of Investigation (FBI), after eight years of experiments, created the first computer system to identify criminals' fingerprints, where all criminals' fingerprints were stored in computers to help.

2.5.1 Fingerprint Patterns

Fingerprint patterns, despite their differences, can be classified into several groups. Each group contains non-identical fingerprints patterns. Fingerprint experts have disagreed on the number of groups. The initial classification was by the scientist Henry, who categorized them into three types: arch, loop, and whorl[38]. Then others followed him and classified them into five, eight, and more than that. However, classifying them into five groups is the most common and widely recognized [39] see table (2.2). Classifying fingerprints into groups is greatly beneficial in reducing the time spent searching for an unknown fingerprint. Instead of searching for the unknown fingerprint across all groups, the search is conducted in only one group, the one to which the unknown fingerprint belongs. This saves time. The scientist Galton was the first to classify fingerprints into three groups, followed by the scientist Henry, and then others followed in increasing the number of classifications[39]. Scientists in the field of fingerprint analysis rely on the classification of fingerprint patterns based on prominent lines, the gaps between them, and their orientations towards the centre. Others base their classifications on the number of points where these prominent lines intersect. This approach to classifying fingerprints is a preliminary step in the process of searching for fingerprints in complex databases. It is instrumental in enhancing the efficiency of searches within large databases, effectively reducing the time needed for these searches. Classifying fingerprints into groups is a method for testing specific properties in a fingerprint and recording it under one of several predefined groups with a specific name.

Table 2.2: The Most Common Classifications in Fingerprint Classification.

	Pattern	Description
1	Whorl	this pattern, ridges form circular or spiral patterns, like tiny whirlpools
2	Arch	This pattern is characterized by ridges that enter from one side, rise in the centre forming an arc
3	Tented arch	Similar to the arch but with a sharper and more pointed peak, giving the appearance of a tent-like structure
4	Right loop	ridges that enter from one side, curve upward to form a loop that opens towards the right, and then exit on the same side from which they entered
5	Left loop	ridges that enter from one side of the finger, curve around to form a loop that opens towards the left, and then exit on the same side from which they entered

Fingerprint classifications vary from country to country. In the United States, three main types of classifications have been adopted, comprising five branches. This includes two branches for the Arch pattern, namely Right Arch and Left Arch, grouped together as the Arch category, and the Ulnar Loop and Radial Loop in a single group called the Loop. Additionally, there's the Whorl category, which includes only one branch: the Plain Whorl. The classifications used in criminal research centers are now based on the Henry System. This system, used by the FBI as shown in Table 2.3, builds a framework based on three groups and their branches, totaling eight categories.

Table 2.3: Classification of Fingerprint Patterns According to the American System.

Main group	Subgroup
Whorl	Plain Whorl
Arch	Plain arch
	Tented arch
Loop	Ulnar Loop
	Radial Loop

The classification of fingerprint patterns fundamentally relies on their intricate characteristics, and accordingly, the classification follows two main directions[40], which are.

a. The General Shape of the Ridges and Furrows and their Convergence at the Center of the Fingerprint

b. The Detailed Shape of the Ridges and the Points of Convergence of the Hidden Lines

The focus of classification in fingerprint information is on the end of the ridge lines, the points where the hidden lines intersect (bifurcation minutiae), the resulting angles, and the centre points (singular points) see Figure 2.5.

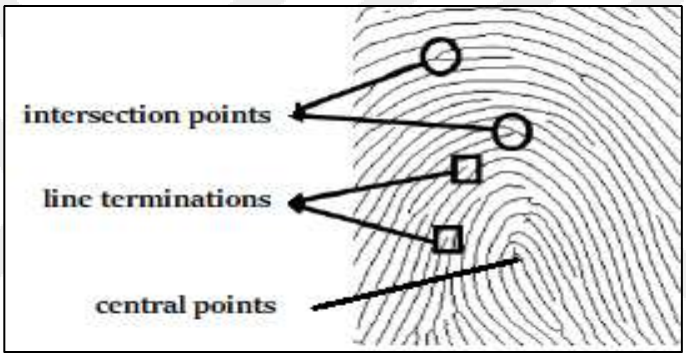


Figure 2.5: Intersection of Prominent and Hidden Lines, and the Central Point**.**

The primary concern of experts in the field was the automation of fingerprint classification to reduce the time expended in searching. For this purpose, numerous algorithms were used. Initially, most methods classified fingerprints into one of the known groups, and many algorithms were developed that include models to assist in classification[41].

2.5.2 Fingerprint Matching

The process of matching fingerprints is considered a complex and vital topic in the field of information security and identification, as this process depends on comparing two specific fingerprints to calculate the degree of similarity between them or provide a binary decision regarding their matching. A distinction is also made between the registered fingerprint (template) and the fingerprint to be matched (input)

There are many challenges facing the fingerprint matching process, due to the large changes that occur to the finger, which include changes in the shape of the finger itself over time, such as displacement, rotation, and even deformations resulting from pressure on the finger. Skin. All these factors negatively affect the accuracy of the fingerprint, making these challenges more complex. Especially when dealing with poor quality fingerprints, where a small percentage of distortion contributes to a large percentage of errors.

The fingerprint matching process usually includes two main stages: the first is to extract the minutia extraction procedure and the second is to match minutia.

2.5.2.1 Minutia extraction

Accurate representation of fingerprint images is important for the success of fingerprint matching based on features. Detail points and orientation maps provide effective fingerprint discrimination, transforming the problem into a pattern matching of points. To achieve accurate matching even with fingerprint images of varying quality, it is necessary for segmentation algorithms to separate the foreground from the noisy background, while image enhancement algorithms must improve the quality of the images without changing the edge pattern or introducing errors. Finally, detail detection algorithms must identify detailed points accurately and efficiently.

Usually, each minutia can be represented by an equation[42].

$$\mathrm{M}i = [\mathrm{X}_i, \mathrm{Y}_i, \theta_i, \mathrm{T}_i] \tag{2-1}$$

Where:

Xi, Yi: represent locations of the minutia - Θi: minutiae direction or minutiae angle.
Ti: represent the type of minutiae.

See the Figure 2.6 showing the location of minutiae point is at the tip of the ridge or the valley and the direction.

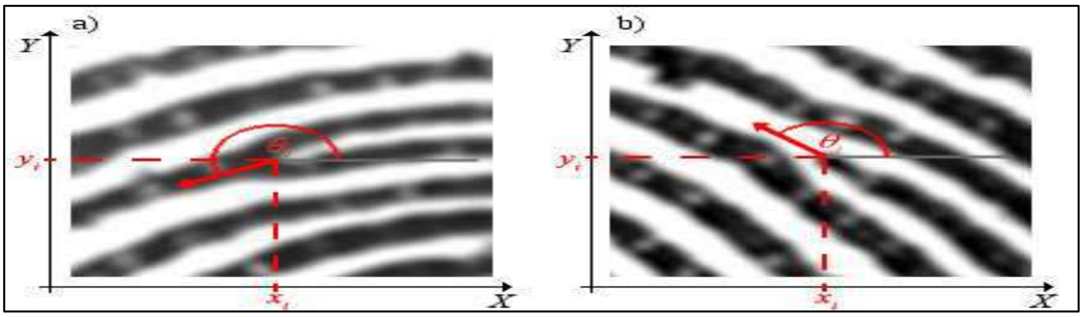


Figure 2.6: Factor of Mintiaa a) Bifurcation b) Ridge Ending.

There are many methods for extracting mintiaa and they can be generally classified into two methods: first one binarized fingerprint images and ridge and second direct greyscale method[42].

In the binarized fingerprint Images, each pixel in the image is converted into two values, black and white. This conversion reduces the complexity of the image and highlights the basic patterns in the fingerprint, thus facilitating the process of processing the image. There are two types of binarized fingerprint images.

a. untinned binarized images: methods in this category analyze pixel patterns without reducing edges to a single pixel width, avoiding information loss that may occur during lamination.

b. thinned binarized images: these methods involve thinning the binarized images to one-pixel-wide ridges, facilitating the detection of minutiae points. the crossing number (CN) is a prevalent technique in this category, defined as:

$$\text{CN} = \frac{1}{2}\sum_{i=1}^{8} | Pi - Pi + 1 | \qquad (2\text{-}2)$$

where $P_i = P_9$ and it helps classify, a pixel based on its local neighbourhood structure in a 3x3 window for the Gray-scale fingerprint method, techniques working directly on gray-scale images avoid the potential information loss due to binarization and thinning. These methods utilize the inherent gray values of the image to detect minutiae.

2.5.2.2 Approaches of fingerprint matching

Fingerprint matching, a cornerstone of biometric identification, relies on various approaches to accurately compare and verify the intricate patterns of individual fingerprints.

a. Minutiae-based matching: it is a method through which the fine details of the finger are extracted and compared with other previously existing details. These details are specific points on the fingerprint, such as the ends of the ridges, bifurcations, and points. These characteristics are extracted from the fingerprint image and used to create a template that can be compared to other fingerprint templates. The accuracy of the matching process depends greatly on the quality of the fingerprint image and, therefore, on the minute details extracted from the image, process of minutiae matching fundamentally involves aligning the template (a set of minutiae in the database) with a subset of minutiae from the input fingerprint through a geometric transformation[42].

b. Correlation-based matching: fingerprint analysis is a method used to verify the match between two fingerprint images. This method involves superimposing the two images and calculating the relationship between corresponding pixels in the images when aligned in different ways. For example, different movements and rotations are considered.In this process, each pixel in the two images is analyzed and compared to determine the degree of similarity. The goal is to find out if the two fingerprints are identical or very similar, indicating that they belong to the same person. This is achieved by adjusting the position and angle of one of the images and comparing the results with the other image to achieve the highest possible degree of match.This method is widely used in forensic science and criminal investigations, where it provides high accuracy in identifying identities through fingerprints.

c. Non-Minutiae feature-based matching: the method works by focusing on different features, as tiny details are hard to pick up in low quality pictures. It uses local direction and frequency which shows how close together the fingerprint lines are spaced out according where they go because each person's print has a unique pattern that follows its own direction line shape too strong, standard better methods typically do this well. It's possible to get these big features from bad pictures, but they are thought as less strong and clear. so, it's hard or impossible know if this same detail stays the same at older times. so, this way is not as accurate as using minutiae-based matching.

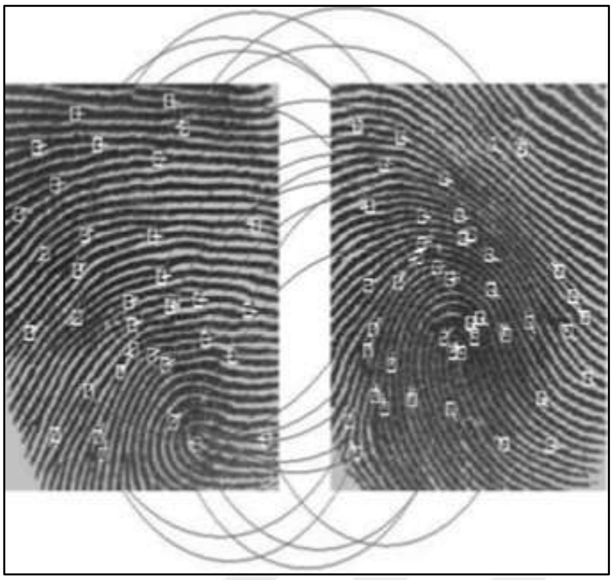


Figure 2.7: Correlation-Based Method is able to Overcome Some of the Difficultiesof the Minutiae Based Approach.

Figure 2.8: Minutiae-Based Techniques , Fine Details of the Finger are Extracted.

2.6 BIOMETRIC FINGER VEIN

The finger vein is a network of blood vessels or veins that spread to take a specific shape under the skin's surface to form a unique pattern (See Figure 2.9). Research has revealed that vein patterns differ from one person to another, and even twins have different patterns of venous fingerprints[43]. All human fingers contain tissues (veins), which in turn work to transport blood to the finger. During the inhalation process, hemoglobin in the blood carries oxygen, giving it a bright red color known as oxygenated hemoglobin. Deoxygenated haemoglobin contains carbon dioxide that accompanies the exhalation process. The difference between oxygenated and deoxygenated haemoglobin is in how they absorb light, specifically infrared rays. Deoxygenated haemoglobin has the ability to absorb infrared rays, and this makes the vein pattern visible by simply shining near-infrared (NRI) on it. Therefore, the biometric finger vein can only be obtained from a person who is still alive, and this is considered a point against counterfeiting[43], [44].

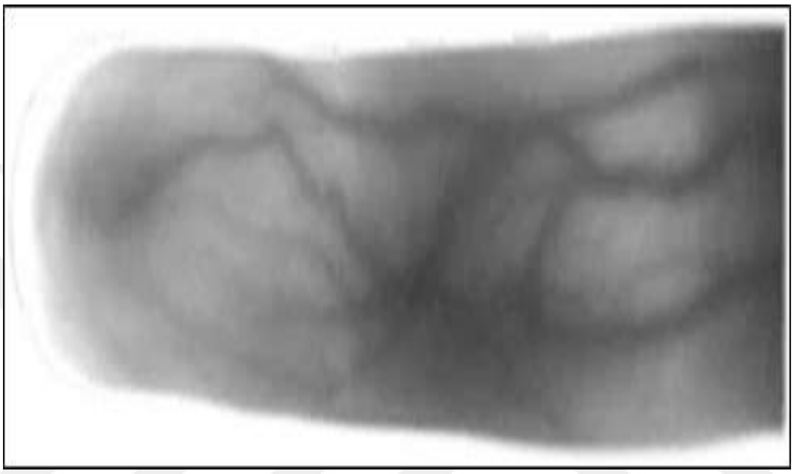


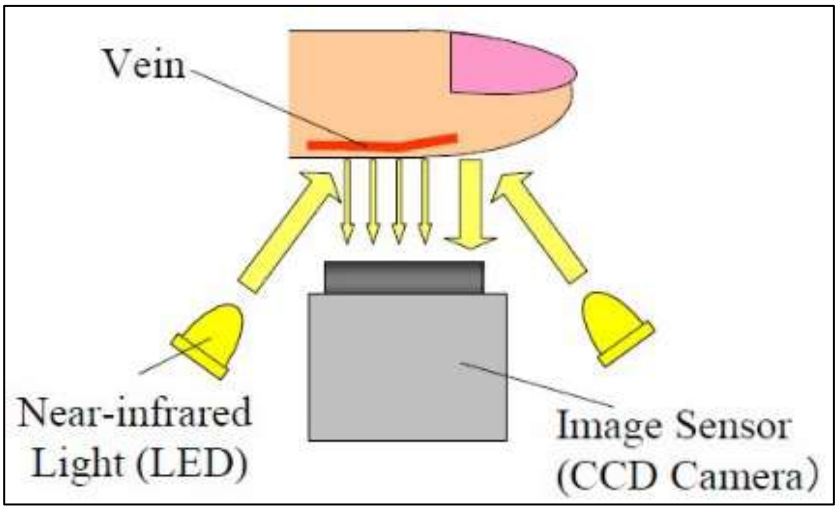
Figure 2.9: Network of Venous Tissue on Finger.

2.6.1 Finger Vein Capturing Methods

Methods of capturing finger veins are divided into two main methods: light reflection method and the light transmission method. Each method has its drawbacks and advantages.

2.6.1.1 Light reflection method

In this method, both the NRI and the image sensor are placed on the same side of the finger, capturing the light that reflects off the surface (see Figure 2.10).



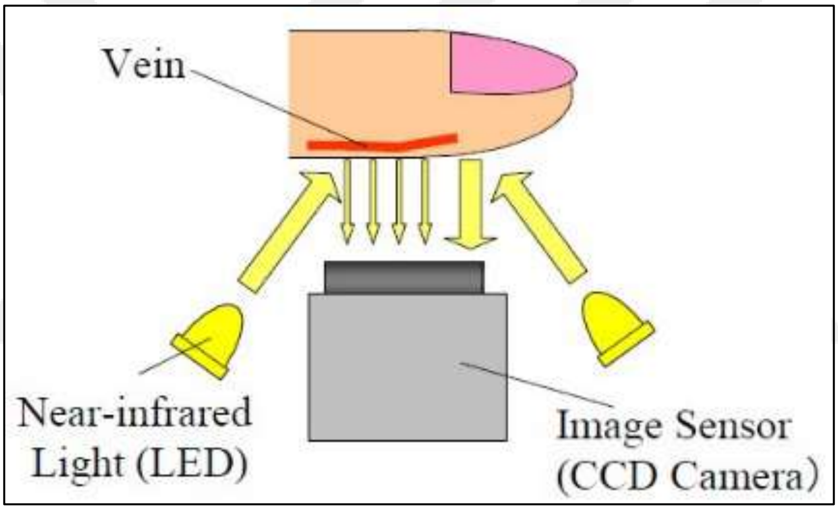


Figure 2.10: Light Reflection Method.

When light is shined on the finger, it reflects off the surface. Vein patterns can be distinguished because blood vessels absorb lighter than surrounding tissue, making veins appear as dark lines on a lighter background. This contrast is used to generate the image of the vein pattern.

Since the light source and the sensor are located on the same side, it is possible to design a more compact and clear capture device design because there is no physical barrier between the finger and the capture sensor, which makes the interaction more without any obstruction. As a result of its effectiveness, it is used in many biometric applications. Despite this, the image resulting from this method It requires many image processing techniques due to the low contrast between the vein pattern and other parts[45].

2.6.1.2 Light transmission method

In this method, the light source and the camera are placed on opposite sides of the hand. The light passes through the hand before being captured by the camera. The infrared light that penetrates the tissue and skin of the finger can be absorbed by the deoxygenated haemoglobin, resulting in the veins appearing dark in the image due to their ability to absorb light[45] see Figure 2.11).

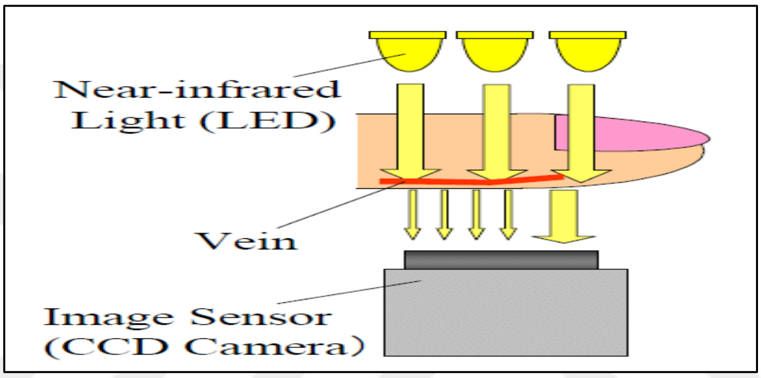


Figure 2.11: Light Transmission Method.

2.6.2 Advantages and Disadvantages of Vein Biometrics

When comparing the venous biometric fingerprint to other biometric methodologies, it becomes evident that the venous approach offers a plethora of advantages. Despite these merits, its adoption is less widespread compared to traditional fingerprinting, possibly due to inherent limitations in these techniques. In the subsequent section, we are going to explain the disadvantages and merits of vein fingerprinting[45].

i. Advantages

a. Uniqueness and Security: vein patterns are considered unique for everyone and cannot be repeated, even in twins. This uniqueness provides them with a high level of safety, in addition to the complexity of these patterns, which makes them difficult to fake.

b. Difficult to Forge: due to the presence of veins under the surface of the skin, which can only be seen by shining infrared rays, a fingerprint based on finger veins is not considered highly resilient against deep forgery and impersonation. These biometric features cannot be captured without the person's consent or the creation of parts that mimic veins, as they need to be completely visible when the finger is completely visible, and blood is moving in the vein[45].

c. Durability and Stability: the blood vessels often do not change significantly over time, which helps with the reliability of the system in the long term, in addition to making this flower more susceptible to external damage, such as injuries or skin diseases.

d. Hygiene and Contactless Operation: the venous image is usually taken in a non-contact manner, and this is considered important in limiting the spread of germs.

e. Less Affected by external factors: venous tissue is rarely affected by superficial wounds, dirt, or skin erosion, while fingerprints are affected by this.

ii. Disadvantages

a. High cost: Identifying a venous fingerprint requires special devices, equipment, and advanced software, which makes it more expensive compared to the method of identifying other identities.

b. Limited use on mobile devices: while fingerprint scanners and facial recognition technologies are readily available in mobile devices, venous fingerprinting technology may not be suitable or practical for integration into mobile devices due to the need for specialized scanners.

Even though the benefits have been talked about, the method based on recognizing finger veins has problems because of internal and external factors that could affect how well it works. But studies have shown that most of these problems can be solved by changing how the devices are set up and using certain treatment methods. In fact, many ideas and plans have been put forward to make it easier to recognize finger veins, showing that performance can be improved even though there are some problems.

2.7 IDENTIFICATION VS VERIFICATION

Identification is the process of identifying a person by comparing one of their biometric data (fingerprint, iris print, etc.) with a database or repository that includes a large set of pre-recorded biometric data. This process, which consists of one and many, includes many operations. Combined, which involves careful analysis of biometric data to ensure accuracy and efficiency. This technology is often used in criminal investigations[29].

Usually in identification systems, the stage after enrollment a person is verifying his identity, unlike verification systems, where a specific identifier is not required to achieve matching. Rather, biometric data templates are compared with all biometric data templates stored in the system. There are two types of identification systems: positive and negative Figure 2.2 [31].

a. Positive identification systems are designed to ensure that an individual's data is recorded in the database. This type of system is used to control buildings or access computer systems and others[31].

b. Negative identification systems are designed to verify the absence of biometric data for a person in the database. The expected result of this system is mismatch, such as ensuring that a specific person is not registered more than once in a specific system[31].

Verification is the process of verifying a person’s identity by comparing his biometric data now of verification with the data previously stored in the system. This process is known as one-to-one matching, where the biometric template of the person now of verification is compared with the biometric template of the same person in the system[31] Figure 2.3.

2.7.1 Approaches of Finger Veins Matching

Matching finger veins is a biometric technique that relies on the vein patterns found inside the fingers to determine a person’s identity. It is considered a safe method for identification because the pink pattern is unique for each person. There are many methods that can be relied upon to match finger veins. We will discuss some of these methods.

2.7.1.1 Minutiae-based method

The term "minute points" refers to the minute details in the finger veins, similar to those in a fingerprint, that can accurately identify individuals. These minutes encompass the locations where blood vessels terminate or diverge, forming unique features that guarantee precise identification see Figure 2.3. The importance of this lies in the use of minute points provides a high level of accuracy in identification and verification of identity, which reduces the possibility of error or fraud in a variety of applications, such as law enforcement, border control, and financial transactions. In recent years, advancements in technology have made it possible to capture and analyze these minute points in a more efficient and accurate manner. This has led to the development of biometric authentication systems that rely on finger vein recognition, in addition to other biometric factors such as facial recognition and iris scans. Such systems are becoming increasingly.

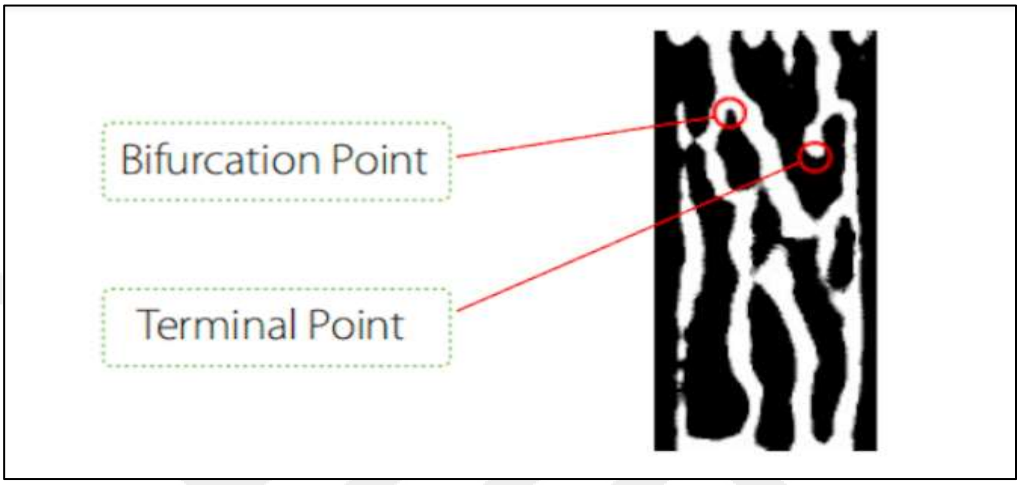


Figure 2.12: Terminal Points of Blood Vessels.

2.7.1.2 Vein line method

Vein lines Capture from Finger Gray Vein Image focus on taking the unique patterns of veins in the finger from sepia pictures and studying them. The topographical structure of the veins is better shown in these images. This means that details and features linked to the vein network are easier to see in grayscale images than in color images.

In other words, grayscale pictures of veins show their structure and small features in a way that makes it easier to understand their shapes and patterns. This makes it easier to study and use in biometric recognition and other similar tasks.

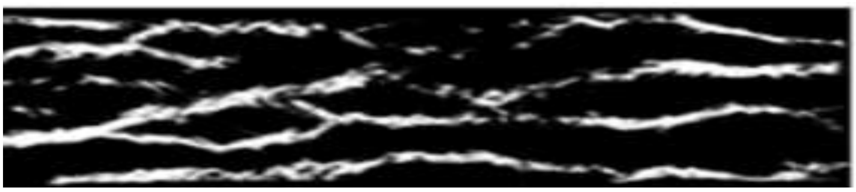


Figure 2.13: Vein Lines of Finger Watch used for Matching.

2.7.1.3 Vein texture characteristic

During the process of identifying the texture of the finger, which includes analyzing the image of the veins present in the finger with the aim of identifying the identity based on the unique pattern of the veins for each individual, the textural characteristics of the image are displayed, which represent the fine details that make up the texture of the image, such as the lines and patterns present in the image, where these characteristics are displayed in a form. Digital representations that use binary numbers, either zero or one. These codes are converted by comparing the grayscale of the existing pixels and the grayscale of the area.

2.8 RELATED WORK

Multimodal biometrics have received much attention because of their superior accuracy, security, and spoof resistance compared to systems operating in single-modal mode. Among the various biometric authentication techniques, fingerprint and vein recognition are two complementary approaches that are particularly successful. The fingerprint is analyzed based on ridge and valley patterns of an individual's finger, while vein recognition uses subcutaneous vein patterns captured through near-infrared photography. These features possess exclusive characteristics because fingerprints are external, and finger veins are internal attributes. Thus, their combination is resilient to changes. A variety of studies have focused on the fusion of fingerprint and vein biometrics. Early works considered the individual feature extraction and matching algorithms relevant to the specific pattern, followed by simple result-level fusion schemes. Recent works have moved to deep learning and, further, feature-level fusion techniques that aim to increase performance and reduce error rates.

Jeyalakshmi V, Pooja K, and Pethanatchi C[46] explored biometric identification using both fingerprint and finger vein modalities. Feature extraction techniques were applied along with two matching algorithms: ridge-based and minutiae-based matchings, to generate matching scores. Four fusion methodologies were utilized: holistic, non-linear, sum rule-based, and Dempster-Shafer theory, to combine these scores. The final decision was based on performance metrics and the ROC curve. The system was tested on the NUPT-FPV dataset, which contains 840 images. The results showed that the Equal Error Rate (EER) was 0% using Dempster-Shafer fusion, while it was 14% with other methods. Additionally, the False

Acceptance Rate (FAR) was 0% across all techniques, demonstrating the system's robustness and security.

Baratam Siddardha and S. Veluchamy [47]presented a biometric authentication technique that integrates two advanced methods: finger vein recognition and finger knuckle recognition. This technique combines the unique vein patterns inside the fingers with the features and shapes of the wrinkles on the knuckles to enhance the accuracy and security of personal identification. The paper describes the development of a fusion algorithm and a system for training and testing based on a large dataset. The proposed system aims to improve identification accuracy and minimize errors, such as false acceptance. It is anticipated that this system will be utilized in applications like access control and identity verification, contributing to enhanced security in the digital age.

Researchers Jian Guo, Jiaxiang Tu, Hengyi Ren, Chong Han, and Lijuan Sun[48] proposed a novel algorithm (FPV-CSAFM) to improve biometric recognition systems by fusing fingerprints and finger veins. They used a convolutional neural network (CNN) to extract features, and a novel fusion module (CSAFM) that dynamically adjusts the fusion weights according to the importance of channel and spatial information. Experiments on multiple datasets showed that the proposed system significantly outperformed traditional methods, enhancing the accuracy of multimodal biometric systems.

Yihua Shi, Zheng Zhong, and Jinfeng Yang[49] developed a novel method to improve multimodal biometric identification using the WLGIGFs descriptor. They used Gabor filters to enhance fingerprint (FP), finger vein (FV), and finger knuckle print (FKP) images, and then encoded the features using LGBP. The maps were divided into small parts and described using an improved version of MRRID, with a Gaussian model applied to reduce the influence of finger pose changes. Experimental results demonstrated the superiority of the method in handling pose changes and achieving high accuracy on an expanded local database.

Choe Seong Ho, Song Chung Ja, and Park Dae Jin developed a multimodal 3D imaging device that can simultaneously verify fingerprint and finger veins. The device consists of a finger receiver unit (201) with a top cover (201a) that forms a finger mounting part, and a bottom cover (201b) that contains the electronic unit. The device features a scanning plate (250) that captures fingerprint and finger veins simultaneously and includes two parts: a fingerprint part (250a) and a finger vein part (250b), with a side wall (251) around the finger vein part, allowing an infrared light source (240) to be mounted underneath. The finger is placed on a designated area (252) that is equal in height to the fingerprint part (250a), enabling double-finger verification on parallel lines, providing higher efficiency and security in biometric verification.

Alshardan et al. (2024) [50]developed a multi-modal biometric identification system that fuses fingerprint and finger vein modalities using the power of artificial intelligence together with convolutional neural networks. The researchers have made use of the high-quality NUPT-FPV dataset to attain better accuracy and reliability by employing three CNN architectures, namely ResNet, VGGNet, and DenseNet. Image quality enhancement techniques such as CLAHE were employed to ensure that distinctive features are clearly extracted.It explored three fusion strategies, namely early fusion, late fusion, and score-level fusion, and achieved an appreciable accuracy of 97% with reduced error rates. This work represents very important advances in biometric recognition systems with practical applications in security and authentication that would open new avenues to more accurate and reliable biometric solutions.

3. THE PROPOSED APPROACH

The proposed system for verifying that a pensioner is still alive, based on double biometric authentication involving fingerprint and vein recognition, already provides a highly reliable way to ensure the identity of individuals and their current living situation. The proposed system runs on a web server with web technologies for the purpose of making the system available. The proposed system consists of three main stages: the enrolment phase, the verification request phase, and the verification phase see Figure 3.1.

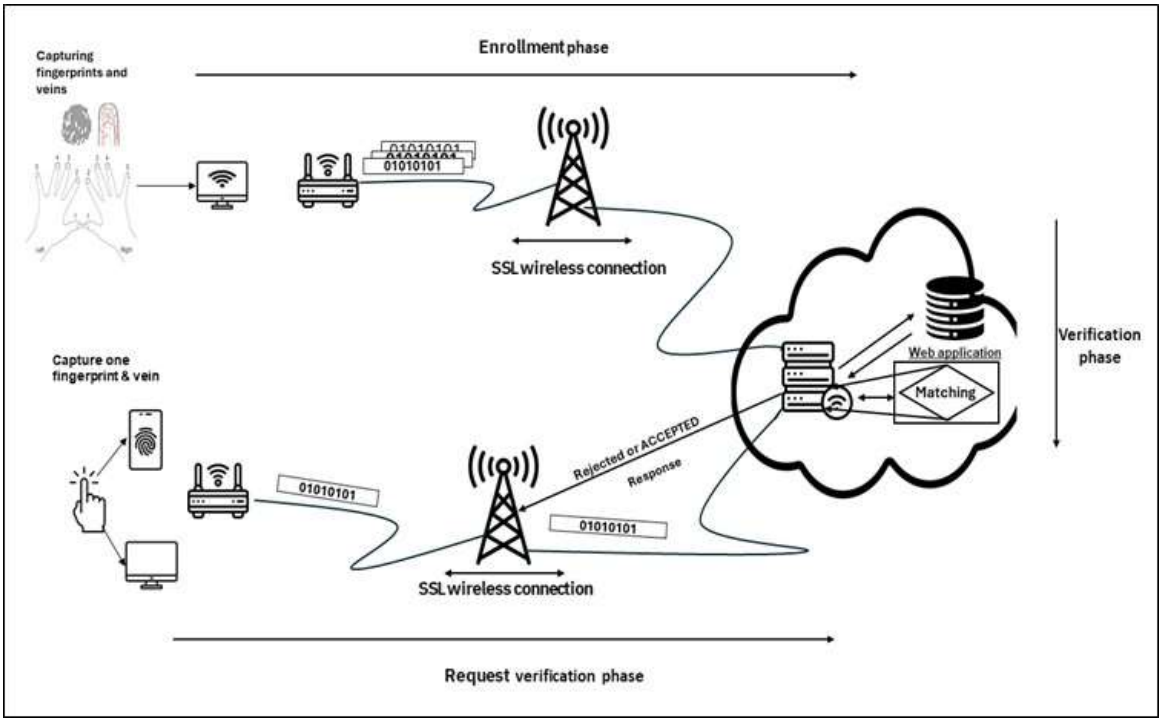


Figure 3.1: Diagram of Proposed System.

The enrollment phase begins with the pensioner presenting proof of pension, such as a pension ID or an identification document. All biometric and venous fingerprints are captured through a vein scanning device and fingerprint scanner connected to a computer. A local service is relied upon to operate the biometric data capture device and to connect with the interface. Through the proposed system, which will be designed using ASP.NET CORE and includes graphical interfaces to facilitate the process of capturing biometric data from the retiree during the biometric data capture phase. Afterward, the data is sent to the server using an encrypted HTTP protocol to ensure the security of the biometric data, moving to the second phase of this system.

When the biometric data arrives at the server, and is received from the system, the system performs some image processing operations on the biometric data to improve the image of the fingerprint, vein print, and some other processing, and thus extract its template and then save it in the database. Figure 3.2 shows the main operations of this process .

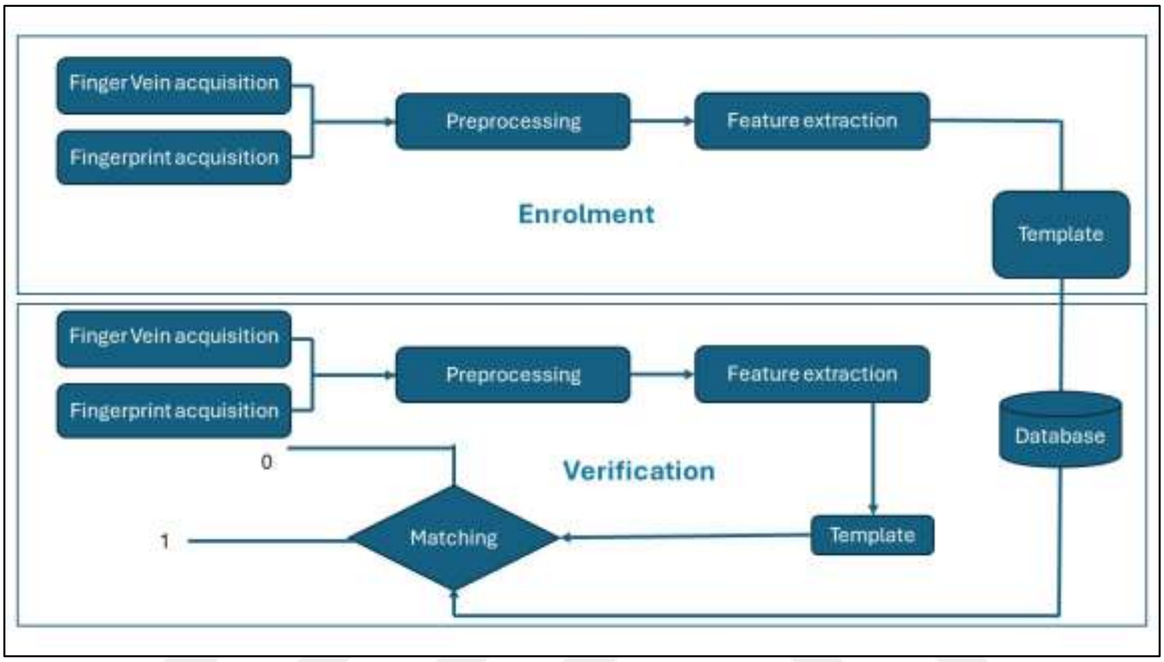


Figure 3.2: Flowchart of Main Operations of Biometric Verification Process.

3.1 ENROLLMENT PHASE

An important part of the biometric verification system is the registration phase, which is where the biometric data that will be used for future identification processes is first collected and stored. The following steps make up the main parts of this phase:

3.1.1 Capturing Fingerprint and Finger Vein Biometrics

The process begins with collecting biometric data from the user. In this system, fingerprints and vein patterns are captured from both hands. This is done using the FV1000 device see Figure 3.3, which is characterized by the ability to capture fingerprints and veins once see Table 3.1.

Figure 3.3: Finger and Vein Scanner Device.

Table 3.1: FV1000 Usb Finger Vein Scanner Features.

Feature	Description
Material	Optical
Effective Collection Area	13.24*15.7mm
Image Size	256*360 pixel / 240*320 pixel
Image Resolution	500dpi / 300dpi
Gray Level	256
Interface Socket	USB Type A
Communication	USB 2.0 / USB 1.1
Operating System	Windows / Linux / Android
Power Voltage	4.8V ~ 5.5V(USB)
Operating Environment	-20 °C ~ +50 °C; 90% r.h

a. Fingerprints scanning: The process involves scanning each finger to collect the precise patterns of ridges and valleys that constitute an individual's unique fingerprint.

b. Vein Patterns: The near-infrared light is used to capture the vein patterns, which are very resistant to change and challenging to counterfeit, to create a detailed map of the distinct vein structure beneath the skin.

3.1.2 Data Digitization

Once the biometric features are captured, the data is converted into a digital format by converting the image into a two-dimensional matrix and each pixel represents the specific brightness of the fingerprint at that point[51]. This involves encoding physical biometric characteristics into binary data that can be processed by computers. This step is necessary to ensure efficient data transfer and storage.

3.1.3 Secure Data Transmission

The digitized biometric data is sent to a distant server. In order to guarantee the confidentiality and reliability of this highly sensitive data, it is transmitted across a secure wireless connection employing SSL (Secure Sockets Layer). SSL employs encryption to safeguard data from interception or tampering while it is being transmitted.

3.1.4 Storage And Processing

Once the server is reached, the biometric data is stored in a database that is controlled by a web application. This database serves as a central storage for all registered biometric templates. The web application manages both the storing and processing of this data, guaranteeing proper formatting and indexing for efficient retrieval and matching in future verification procedures.

3.1.4.1 Preprocessing of fingerprint

Preprocessing is crucial in biometric recognition systems to ensure that the raw data is appropriate for precise and dependable feature extraction. Preprocessing methods often used include picture normalization, contrast correction, and filtering. These methods aid in reducing the impact of fluctuations in illumination, noise, and other environmental conditions that might impair the quality of biometric data. Preprocessing boosts the overall performance and resilience of the identification system by enhancing the quality of the pictures[52].

Image Enhancement

Fingerprint images taken on devices are usually poor in contrast and accuracy, and these two factors are important in the verification process[53]. The challenge lies in improving the accuracy of the images taken, as the contrast between the edges, valleys, and false points at the edges is improved through three steps.

a. Histogram Equalization: This step aims to widen the pixel value distribution to get a clear view of the image. This enhances the contrast in the image, making details clearer. The formula used for Histogram Equalization is:

$$\left\lfloor \frac{minCDF-(M*N)}{minCDF(i)-CDF} \times 255 = S(i) \right\rfloor \quad (3\text{-}1)$$

Where:

b. S(i): represents the intensity value of pixel iii in the output image

c. M×N is the total number of pixels in the image

d. CDF is the cumulative distribution function of pixel intensities in the image.

e. min CDF is the minimum value of the cumulative distribution function in the image

f. 255 is the maximum intensity value for a pixel in an 8-bit grayscale image

Table 3.2: Algorithm (3.1): Histogram Equalization.

Input: Original Image
Output: Equalized Image
Procedure: Step 0: Initialize variables Width ← original.Width Height ← original.Height equalizedImage ← new Bitmap(Width, Height) histogram ← array[256] of int (initialize all to 0)

Step 1: Calculate the histogram
For i ← 0 to Width - 1 do
For j ← 0 to Height - 1 do
pixel ← original.GetPixel(i, j)
histogram[pixel.R] ← histogram[pixel.R] + 1
End For
End For

Step 2: Calculate the cumulative distribution function (CDF)
cdf ← array[256] of int
[0]cdf[0] ← histogram
For i ← 1 to 255 do
cdf[i] ← cdf[i - 1] + histogram[i]
End For

Step 3: Find the minimum non-zero value in the CDF cdfMin ← FindFirstNonZero(cdf) scale ← 255.0 / (Width * Height - cdfMin)

Step 4: Apply the histogram equalization
 	
For i ← 0 to Width - 1 do
  For j ← 0 to Height - 1 do
    pixel ← original.GetPixel(i, j)
    newValue ← (cdf[pixel.R] - cdfMin) * scale
    newValue ← Clamp(newValue, 0, 255)
    newPixel ← Color.FromArgb(newValue, newValue, newValue)
    equalizedImage.SetPixel(i, j, newPixel)
  End For
End For

Table 3.2: Algorithm (3.1): Histogram Equalization “Table Continued”.

Step 5: Return the equalized image Return equalizedImage

Figure 3.4 Show a fingerprint image with its histogram before and after applying equalisation. It shows an increase in contrast in the fingerprint image after applying equalisation.

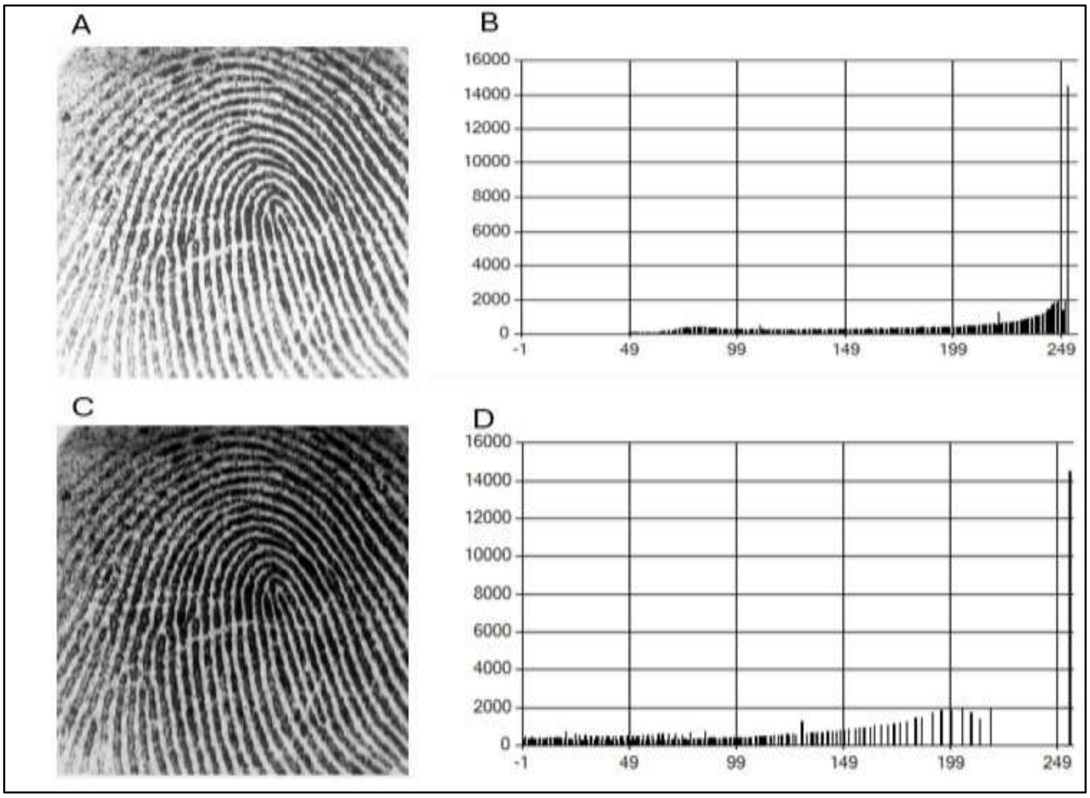


Figure 3.4: A: Original Fingerprint, B: Histogram of Original Fingerprint, C: Equalized Image, D: Histogram of Equalized Fingerprint.

a. Fast Fourier Transformation (FFT): using FFT as a powerful tool for analysing and enhancing digital images. The image can be divided into overlapping blocks with sizes that are powers of 2, such as 16x16 or 32x32 pixels, to obtain accurate directional information from these blocks. Applying the fast Fourier transform to each block allows obtaining the directional information of that block. If a block contains two or three parallel lines, the dominant frequencies of that block will express these lines. The FFT is calculated using the following equation:

$$f(u,v) = \frac{1}{MN}\sum_{U=0}^{N-1}\sum_{V=0}^{M-1} F(X,Y).e^{2\pi j(\frac{vy}{N}+\frac{ux}{M})} \tag{3-2}$$

Where f(u,v) is the frequency value at the frequencies u and v and f(x,y) is the pixel value at coordinates X and Yand j is the imaginary unit

To improve the representation of the masses according to their dominant frequencies, one can multiply the Fourier transform of the mass by its magnitude many times. This process effectively separates the parallel lines and enhances their sharpness. By squaring or cubing the Fourier transform expression, the outcomes can be enhanced; however, this may obscure subtle intricacies.

b. Binarization: In this process, the image is converted from grayscale to a binary image, where each pixel is represented in either black or white. There is usually a need for what is called a threshold, where the threshold represents a specific value. Each pixel in the image is compared to the threshold value[53],see equation.

$$f(u,v) = \begin{cases} 0, & if\ f(x,y) < T \\ 1, & if\ f(x,y) \geq T \end{cases} \tag{3-3}$$

Where f(x,y) is the pixel value at the location (x,y) in the original grayscale image, and f(u,v) is the pixel value in the resulting binary image and T represent threshold.

The pixel value is set to 0 (black), and if it is greater than the threshold, the pixel value is set to 1 (white).

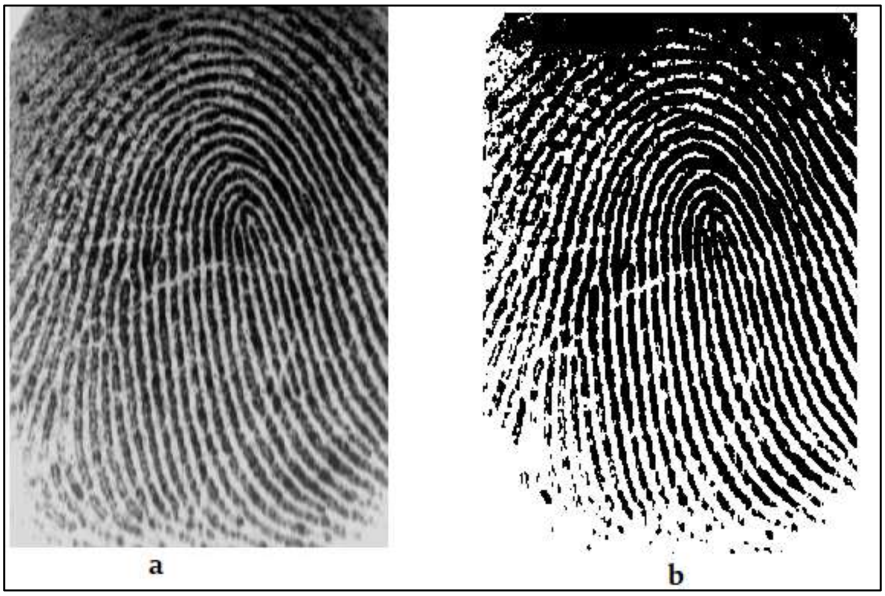


Figure 3.5: Binarization of Image. (a) Original Image. (b) Binarized Image.

Image Segmentation

The two basic steps in image segmentation include Ridge Flow Estimation and ROI Extraction.

a. Ridge Flow Estimation: the image is analysed to extract information about the local directions of the lines and textures in the image. The image is divided into small blocks with a size of 16 * 16 pixels[53], where each block is analysed separately to extract local information from it about the direction of the lines, and then the gradients are calculated in two directions x and y using the Soble filter. Or other filters, after which the local directions of each block are calculated using the arctangent function using the following formula

$$\theta = \tan^{-1}\frac{Y}{X} \tag{3-4}$$

Where θ is the direction angle of the lines the calculated angles are converted to a standard range usually between 0 and 180 degrees, which facilitates comparison and interpretation of trends between different masses.

b. Region of Interest (RIO): morphology operations are applied, specifically the opening and closing operations, to modify the structure of the image based on certain shapes to improve the quality of the image. in the case of opening, two successive operations are performed[53], which are erosion and then followed by expansion. this process aims to remove small noise and soften the edges of objects in the image, which leads to enlarging the image and getting rid of it. of peaks generated BY background noise. the closing process (close) involves dilation followed by erosion. this process is used to fill gaps and holes within objects, shrinking the image and filling in the gaps, thus making the objects more cohesive and continuous, FIGURE 3.6 show the impact of open -close operations on the image.

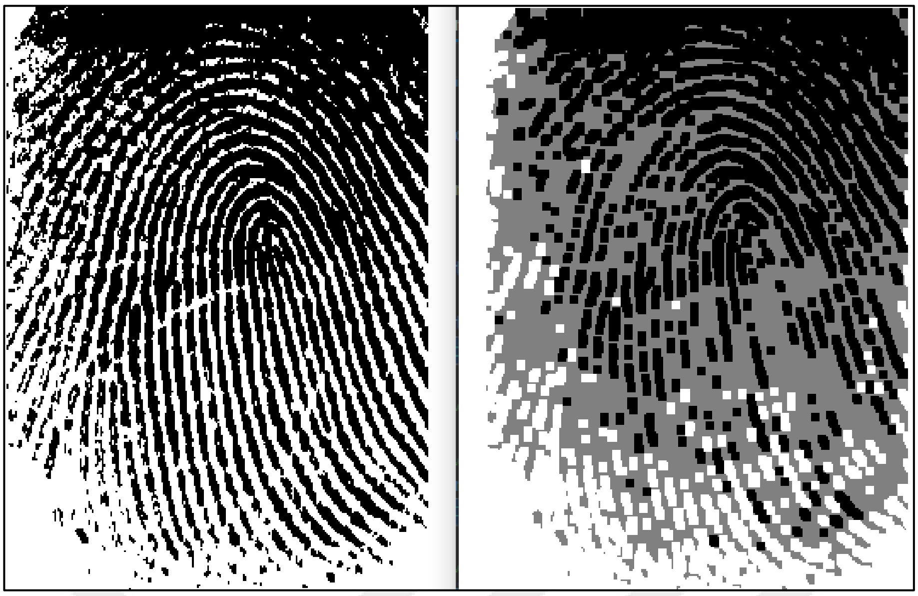


Figure 3.6: Fingerprint Before and After Applying Morphology Operations.

3.1.4.2 Fingerprint feature extraction

Ridge Thinning

In this process, the broad hills in the fingerprint image are transformed into thin lines consisting of one pixel in width without affecting their shape or direction. This process leads to simplifying the general structure of the fingerprint and facilitating the extraction and processing of distinctive points such as branch and end points[54]. Usually, several algorithms are used to implement the ridge thinning process, and one of these algorithms is the Zhang-Suen algorithm[55], Below table show the procedures of algorithm step by step, as it works to remove pixels that do not affect the basic structure of the edge. The process takes place in two stages. In each stage, the pixels are scanned, and the excess pixels are removed. Based on a set of rules.

Table 3.3: Algorithm (3.2): Ridge Thinning using the Zhang-Suen Algorithm.

Input: Original binary image
Output: Thinned image
Procedure: Initialize variables: Width ← original.Width Height ← original.Height thinnedImage ← new Bitmap(Width, Height) Repeat until no points are deleted: 1.1. For each pixel p(i, j) in the image: If the pixel satisfies the following conditions: (a): 2 ≤ Number of black neighbors (B(P1)) ≤ 6 (b): Number of transitions from white to black (A(P1)) = 1 (c): In odd iterations: P2 * P4 * P6 = 0, and in even iterations: P2 * P4 * P8 = 0 (d): In odd iterations: P4 * P6 * P8 = 0, and in even iterations: P2 * P6 * P8 = 0 If the conditions are met, delete the pixel p(i, j) 1.2. End for each pixel End repeat until no points are deleted

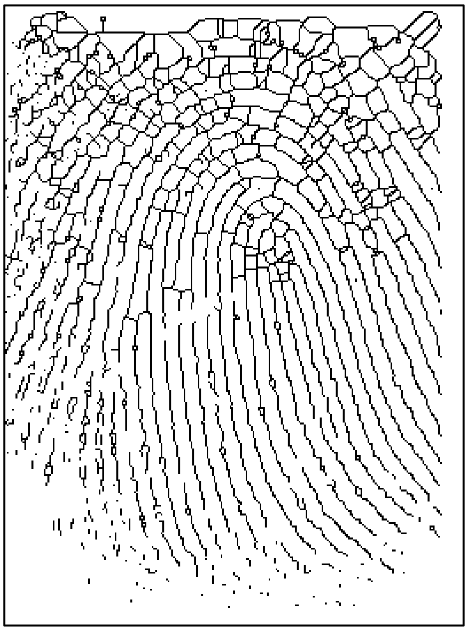


Figure 3.7: Ridge-Thinned Fingerprint.

Minutiae Marking

Classifying points of interest in a fingerprint image helps identify unique fingerprint patterns. Identifying and classifying points of interest in a fingerprint image involves two basic processes: distinguishing the ends of lines (ridges) and the bifurcations of lines (ridges). These two operations rely heavily on the concept of the crossing number[53]. the crossing number of each pixel is calculated using the flowing equation (3-5)

$$CN = \frac{1}{2}\sum_{i=1}^{8} |Pi - P(i+1) \quad P9 = P1 \tag{3-5}$$

Where Pi is the value for a pixel in the neighbourhood and eight neighboring pixels can get scanned in anticlockwise direction as follows Table 3.2.

Table 3.4: Neighbouring Pixel.

P4	P3	P2
P5	P	P1
P6	P7	P8

The values resulting from the transitions from the eight neighbors are collected, and then the transient count is calculated based on the previous equation, where if the calculated transient count value is equal to 1, the pixel is classified as the end of a line. If the calculated transient value is 3, the pixel is classified as a line bifurcation. Any other value of the transient number, the point is considered unmarked and is not classified as an important point. Table 3.8 show the fingerprint after applying cross number equation and mark the minutie.

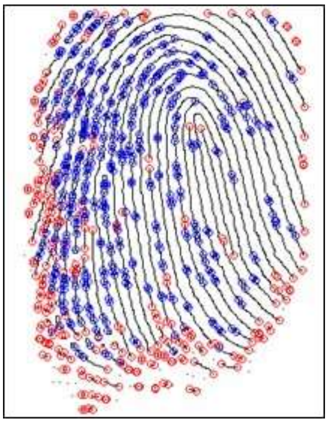


Figure 3.8: Minutiae Marking.

The Removal of False Minutiae

The image obtained after pre-processing is often not of good quality which can lead to errors in fingerprint recognition[53]. For example, if there are false points close to other real fingerprint points, the fingerprint may be incorrectly recognized. By removing these points, the accuracy of the system is greatly improved. Focusing only on the correct and important points in the fingerprint means that the system can recognize fingerprints in a more accurate and correct way. To eliminate these spurious details, the following steps are followed

a. Determine the distance between a bifurcation and a ridge ending. If this distance is less than D, it indicates that the minutiae points are located on the same ridge, allowing for the removal of both points. Here, D signifies the average interridge width, which is the average distance between two neighboring ridges.

b. Evaluate the distance between two bifurcations on a single ridge; if the distance is less than D, remove both bifurcations.

c. If two ridge endings are within D, share similar directions with slight angular variation, and meet the condition of having no terminations between them, they indicate false minutiae from a cracked ridge and should therefore be removed.

d. Remove two ridge ends in a narrow ridge with a distance less than D. This process offers the advantages of eliminating these false detail points by taking advantage of the ridge identifier to distinguish between true and false detail, strongly identified Across seven types. This reduction in spurious detail enhances computational efficiency, providing an additional benefit.

Figure 3.9: Finger Print After Remove Flase Minutiae

3.1.4.3 Preprocessing of finger vein

Pre-processing or a step that takes place after capturing an image of the vein is considered necessary because its goal is to identify the region of interest for feature extraction. The quality of the matching depends on the clarity of the finger veins. Usually, the image of the finger veins contains noise, blurring, and low contrast, which may be due to fluctuations in lighting or the device itself. This stage aims to solve these problems through the following two steps

Detection region of interest of finger

As we mentioned previously, the infrared radiation that is directed at the finger and is absorbed by the hemoglobin present in the veins makes these veins appear darker than the rest of the surrounding tissue[45].

At this stage, the finger's borders are detected, and its area is cropped, where the gaussian bluris is used. This mask is applied to the original image by element-wise multiplication. this means that each pixel in the image is affected by its corresponding value in the mask[56]. the expression of the Gaussian function of the traditional Canny edge detection algorithm is given by the formula:

$$\mathbf{G(x,y)} = \frac{\mathbf{1}}{\mathbf{2}\boldsymbol{x}\boldsymbol{\partial}^{\mathbf{2}}} \mathbf{exp}\left(\frac{\boldsymbol{x}^{\mathbf{2}} + \boldsymbol{y}^{\mathbf{2}}}{\mathbf{2}\boldsymbol{\sigma}^{\mathbf{2}}}\right) \tag{3-6}$$

Where $\boldsymbol{G(x,y)}$ is the value of the Gaussian function at the point (x,y), σ: Standard deviation of a Gaussian distribution, determining the spread of the distribution, 2π: A mathematical constant that represents the area of a circle in units of radius.

This filter helps reduce noise[57], which in turn can cause errors in the feature extraction or detection process, thus improving the matching process. See Figure 3.10.

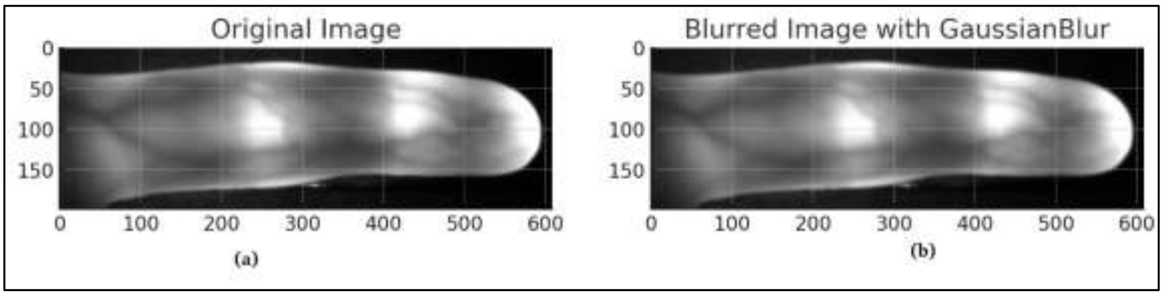


Figure 3.10: Captured Image a) Before Applying the Gaussian Bluris Filter b) After Applying Filter.

To calculate the magnitude and direction of the gradient in the second stage, Sobel filters are applied to calculate the partial derivative in the x and y directions based on different operations see Figure 3.11.

X – Direction Kernel

-1	0	1
-2	0	2
-1	0	1

Y – Direction Kernel

-1	-2	-1
0	0	0
1	2	1

Figure 3.11: Soble Filters.

The Sobel filter equation is applied in x direction by equation 3-7

$$G_X(i,j) = \sum_{l=-1}^{1} \sum_{K=-1}^{1} I(i+k, j+l) \,.\, S_x(k,l) \tag{3-7}$$

Where I(i,j) is the pixel value at the position (i,j) ,$S_x(k,l)$ is the value of the Sobel filter in the x direction at the position (k,l),G_x(i,j) is the value of the partial derivative in the x direction at the position I(i,j)

The Sobel filter equation is applied in y direction by equation 3-8

$$G_y(i,j) = \sum_{l=-1}^{1} \sum_{K=-1}^{1} I(i+k, j+l) \,.\, S_{xy}(k,l) \tag{3-8}$$

Where I(i,j) is the pixel value at the position (i,j) ,$S_y(k,l)$ is the value of the Sobel filter in the y direction at the position (k,l),G_x(i,j) is the value of the partial derivative in the y direction at the position I(i,j)

After applying these filters to the image, the Gradient Magnitude is calculated using the following equation[57]:

$$G(i,j) = \sqrt{{G_x}^2(i,j) + {G_y}^2(i,j)} \tag{3-9}$$

$$\theta(i,j) = \tan^{-1}\frac{G_y(i,j)}{G_x(i,j)} \tag{3-10}$$

After calculating Gradient Magnitude, we can calculate Gradient Direction using the following equation

After applying the previous procedures in image, we can see the result in the Figure 3.12.

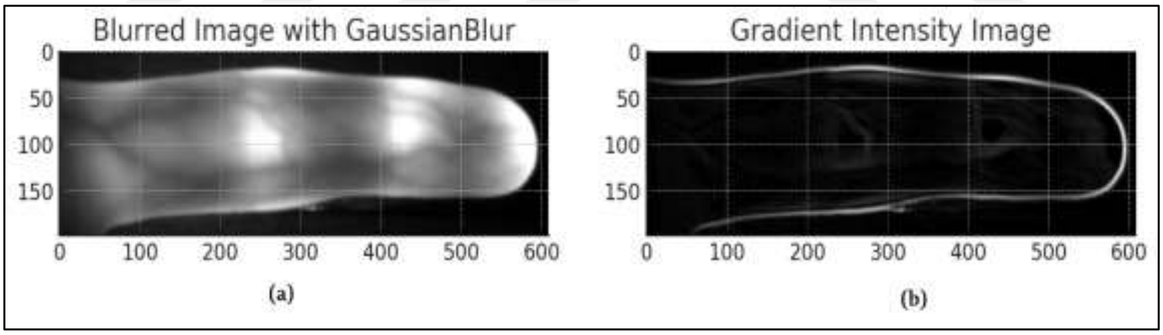


Figure 3.12: Finger Vein Image a) Orginal Image b) Gradient Intensity^.

We can see the result in the Figure 3.12 b we can see that the result looks good, but when we zoom in on the image, we find that some edges are thick and others are thin, so we need a step to reduce the thick margins, by Non-Maxima Suppression (NMS) The goal of this step is to reduce the number of points that are considered part of the edge and make the edges thinner and sharper, as the gradient of the target value is compared with the gradient values of the two neighbouring points in the direction of the gradient G1(i,j) and G2(i,j) [57].

Where:

If the gradient value of the target point G(i,j) is greater than the gradient values of the neighbouring points G1(i,j) and G2(i,j), then the target point is considered part of the edge and remains unchanged. If the gradient value of the target point is not greater than the neighbouring values, the gradient value of the target point is set to zero G(i,j)=0.see Figure 3.13.

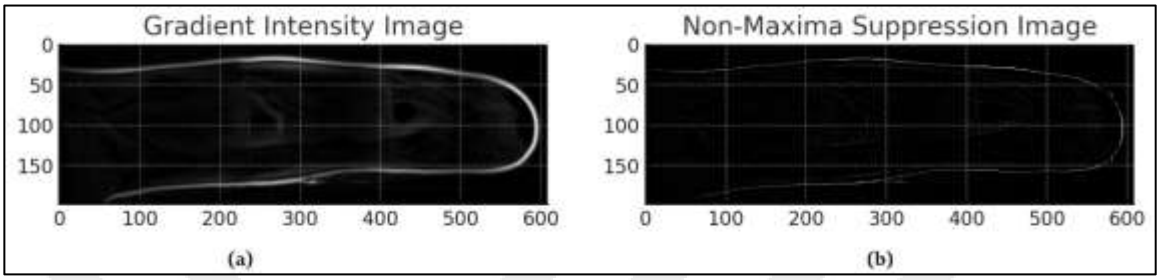


Figure 3.13: b) Finger Vein after Applying Non-Maxima Suppression.

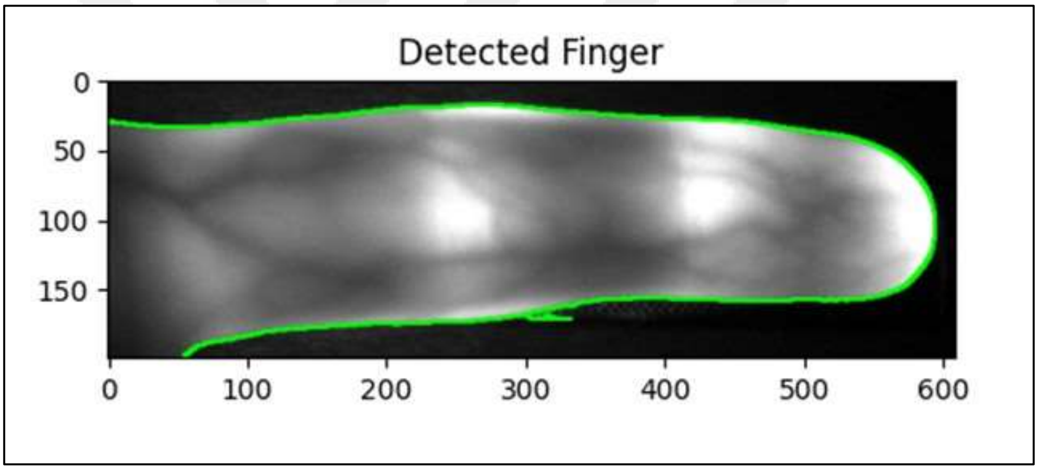


Figure 3.14: F: Finger Vein after Detect Boundary of Finger.

Vein Sharpening

In this step, the unsharp mask algorithm is used to highlight the vascular structure. The first step in the process is to create a blurry image and a non-sharp type of image. To find the edges, the non-sharp image is subtracted from the original image. To get a sharper image, there is a certain process involves several steps to achieve a sharper and more detailed image[58] see Figure 3.15.

a. Creating a Blurred and Unsharp Image: A blurred version of the original image is created and subtracted from the original image to create an unsharp image.

b. Edge Detection and Contrast Enhancement: To achieve a sharper image, the contrast is increased along the detected edges. This contrast adjustment helps in enhancing the visibility of the vascular structures, which may not be easily seen with the naked eye.

c. Pixel Intensity Adjustment: Pixel intensities are adjusted to improve contrast between different intensity ranges. This adjustment further enhances hidden visual details, improving overall image quality.

d. Use of Gaussian Filter: A Gaussian filter is employed to create the unsharp mask. This filter is particularly effective for gamma-enhanced finger vein images. The Gaussian filter is applied through convolution with a kernel mask. The standard deviation of the Gaussian filter[58], set to 4 during experiments, determines the extent of sharpening. Larger values affect a broader area, while smaller values are more localized.

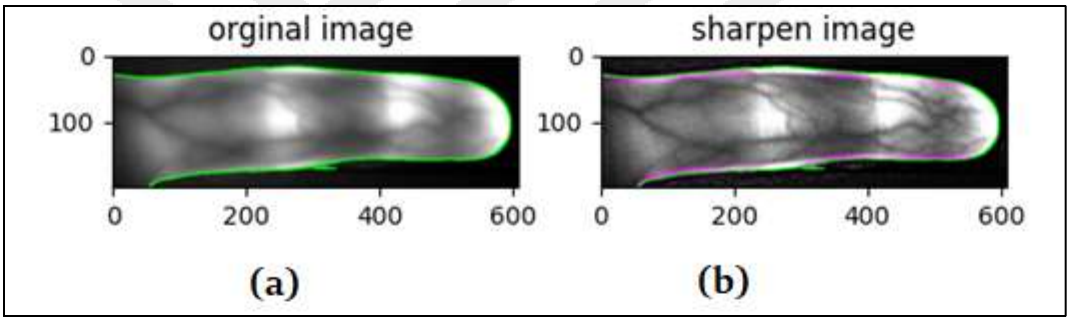


Figure 3.15: a) Orginal Finger Vien b) Sharpened Fingerivein İmage.

Dual Histogram Equalization

To modify the density distribution of pixel values, a histogram smoothing operation must be performed. By combining the power of fuzzy histogram with cumulative histogram smoothing, the use of double histogram smoothing is preferred. Fuzzy histogram is used to spread the pixel density evenly to increase the dynamic range of pixels and thus increase the contrast. cumulative histogram is performed before Gaussian histogram smoothing.

i. Cumulative histogram equation (CHE)**:** the cumulative histogram equation is used to improve the image by improving the contrast through a better distribution of brightness values[59],the following steps are applied to calculate the cumulative histogram equation[58]:

a. Calculate image histogram

b. Calculate the histogram of the cumulative distribution function (CDF) and calculate the histogram of the cumulative distribution function (CDF) where the new value is assigned to each grey value in the original image and the new value n is found by the formula equal to the histogram below.

$$C_k = \frac{L}{N} * S_r(k) - 1 \tag{3-11}$$

Where N: is the total number of pixels L: total number of possible intensity and $\boldsymbol{C_k}$ is the value of intensity that is mapped and k: an original intensity integer value such that k lies between 0 and L-1. levels

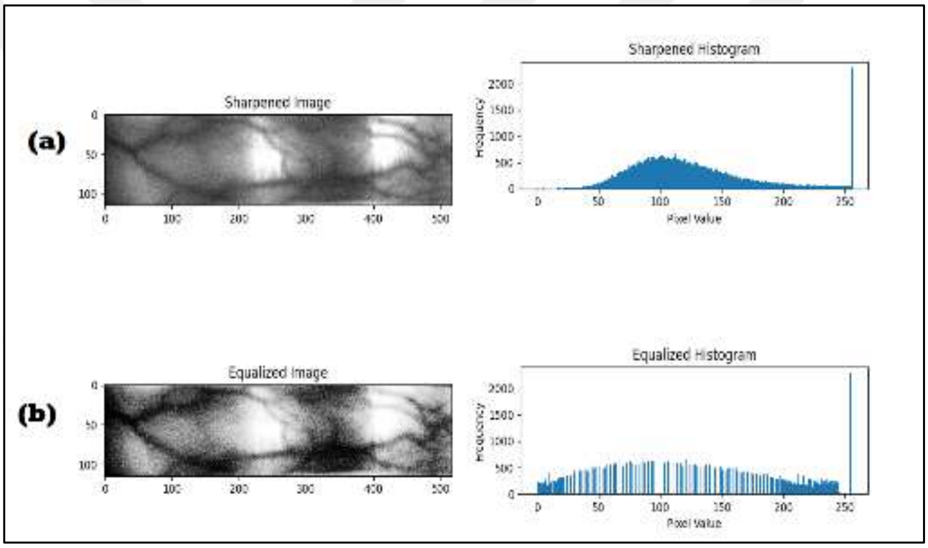


Figure 3.16: Finger Vein Histogram a) Before Applying Cumulative Histogram, b) After Applying Cumulative Histogram.

ii. Brightness Preserving Dynamic Fuzzy Histogram Equalization (BPDFHE): (BPDFHE) is used to improve the contrast of images. This technique effectively processes images by dealing with grey values in a fuzzy manner instead of the traditional precise values[60]. It is characterized by its ability to improve contrast while maintaining the original brightness of the image. the dynamic fuzzy Histogram Equalization can be calculating throw following operational stages:

a. Fuzzy histogram computation: fuzzy histogram is calculated by the equation:

$$h_f(i) = \sum_{x,y} \mu_{I(x,y)}(i) \tag{3-12}$$

where is the trigonometric membership function defined as follows:

$\mu_{I(x,y)}\ (i)$

$$\mu_{I(x,y)}(i) = \max\left(0,1 - \frac{|\, \mathrm{I}(x,y) - i \,|}{\boldsymbol{a}}\right) \tag{3-13}$$

Where is membership function value of the pixel at location (x, y) with respect to the grey level, max (0,·): is the function that takes the largest value between zero and the calculated value. This function ensures that the membership function is not negative and I(x,y) is the grey value of a pixel at location (x, y) in the image.

b. Partitioning of the histogram: in this step, the histogram is divided into multiple parts based on local maxima using the first and second derivatives of the fuzzy histogram:

c. Dynamic Histogram Equalization of the Partitions (DHE): at this stage, each part of the histogram is dynamically modified using the DHE technique. The goal of this process is to improve the contrast within each part of the histogram, while maintaining the distribution of grey values commensurate with the original image structure. This process involves two main stages: setting the dynamic range of each part, and the actual equalization of the histogram.

d. Normalization of Image Brightness: after dynamic equalization, a normalization process is applied to ensure that the average brightness of the resulting image matches the average brightness of the original image:

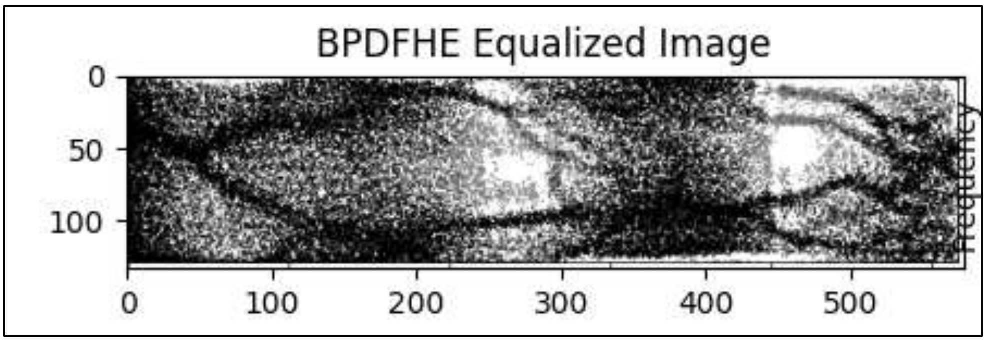


Figure 3.17: After Applying BPDFHE

Vein Edges Detection

In many image processing and computer vision applications, such as the recognition of finger vein patterns, edge detection is an essential first step. The canny algorithm is one of the most popular and successful edge detection techniques. This approach was created in 1986 by John F. Canny and finds edges by searching for the image's local gradient maxima[56]. The first stage in the procedure is applying a Gaussian filter to the image to smooth it out and remove noise. After that, the image's intensity gradients are computed. Then, non-maximum suppression is used to eliminate erroneous edge detection responses. Lastly, edges are found and linked using double thresholding and edge tracking via hysteresis. Applied to photographs of veins in the fingers see Figure 3.18.

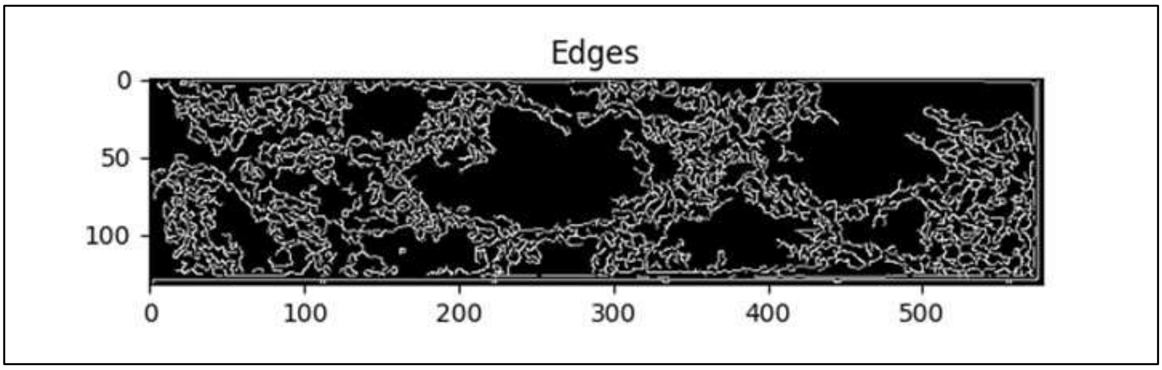


Figure 3.18: Edge Detection Using Canny Algorithm.

3.1.4.4 Feature extraction of finger vein

Feature extraction is the process by which a vein print image is converted into features. The set of features collected from the image is used in the matching process. Thus, feature extraction can make use of algorithms to identify and separate a specific part of the image[43], histogram of oriented gradient (HOG) feature extraction is widely used in difficult visual situations due to its ability to perform well in those cases. basic steps to extract HOG features[58]:

a. Divide the image into small cells: the image is divided into small sections called "cells".

b. Calculate the orientations of the edges in adjacent sections: edge orientations are calculated for each cell. For signed gradients, the histogram channels are evenly distributed between 0-360, and for unsigned gradients, they are distributed between 0-180.

c. Lighting effect correction: the illumination effect is corrected by adding the power scale to each local histogram on the larger connected sections.

d. Feature vector collection: The feature vector is finally assembled by considering all the dominant orientations of the computer gradients.

The above steps represent the unification of the clustered cells that form the HOG characteristic vector of the entire image [58]. The scaling and rotation process does not affect the algorithm because the algorithm only uses the key points to detect the extreme values in the space scale.

The HOG descriptor primarily consists of features related to the histograms of the slopes of object edges in an image. The HOG feature descriptor can be defined by the following equation.

$$H_{Hog} = [F_1, F_2, \dots F_k] \tag{3-14}$$

Where K is the total number of overlapping blocks in an image, F_j is the normalized block vector of j-th block

$$f_j = \left[h_{1,j}, h_{2,j}, \dots h_c * B,\ _i \right] \tag{3-15}$$

where c is the total number of cells in block, B is total number of bins in a cell, Figure 3.19 show sample image of size 32 x 32, this procedure can be demonstrated

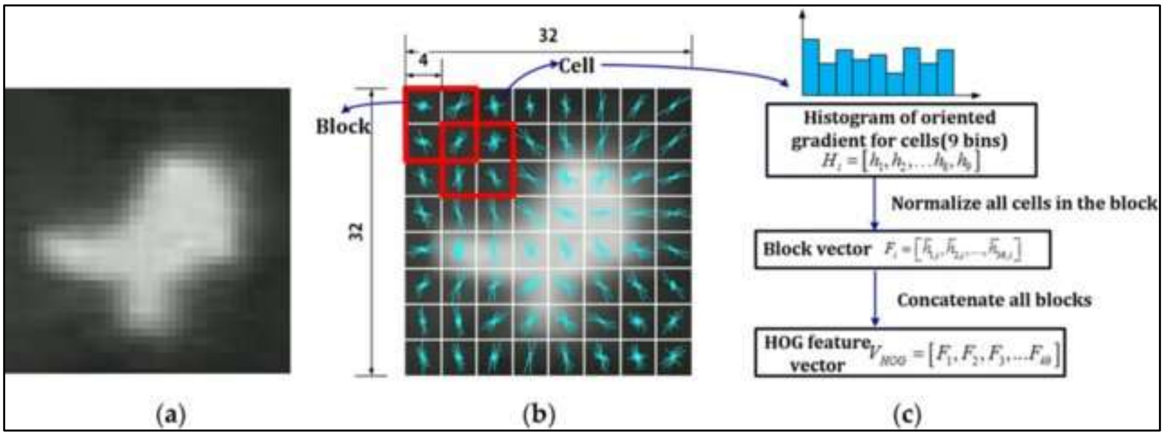


Figure 3.19: a) Original Image, b) Visualization of Gradient Orientations of all Cells (White Grids Represent cells, and Red Bounding Boxes Indicate Block Regions), c) Generating the Feature Vector. The Cell Size is 4 × 4 Pixels. The Local Histogram is Defined with 9 Orientations (bins). The Block Size is 2 × 2 Cells.

Then a sample of the image is chosen as a template used for comparison and measuring the similarity percentage.

3.2 FINGER VEIN VERIFICATION

At this stage, the similarity ratio of the finger vein template is measured using the cross-correlation coefficient. The cross-correlation coefficient is a statistical measure that assesses the similarity between two templates[61], in this case, the finger vein patterns. The correlation coefficient ρ is defined as:

$$\rho = \frac{\sigma_{LR}}{\sigma_L \, \sigma_R} \qquad (3\text{-}16)$$

Where ρ is the correlation coefficient is a measure of the degree of relationship between two images, σ_{LR} *is* the covariance between the left image and the right image, σ_L is standard deviation of left image, σ_R is standard deviation of left image.

When we say that the correlation coefficient between two images is ρ, we are talking about how similar or different these two images are based on some statistical property such as the mean and standard deviation. ρ is calculated by taking the covariance between the two images and dividing this covariance by the product of the standard deviation of each image.

If the correlation coefficient ρ is normalized, it has a value between -1 and 1, where 1 indicates that the two images are perfectly similar, and -1 indicates that they are perfectly different[61]. The first step in finding the correlation coefficient is to find the mean of each of the two images, the right (R) and the left (L) throw the equations

$$\overline{g}_L = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} g_L(x_i, y_i)}{n.m}$$

$$\overline{g}_R = \frac{\sum_{i=1}^{n}\sum_{j=1}^{m} \mathrm{g_R}(x_i, y_i)}{n.m} \tag{3-17}$$

The standard deviation is then calculated using equation 3-16 for each image, which is a measure of how far the image values diverge from the mean. These calculations are necessary because they provide the basis for calculating the covariance between the two images, which is ultimately used to calculate the correlation coefficient.

$$\sigma_L = \sqrt{\frac{\sum_{a=1}^{z}\sum_{b=1}^{c}\left(g_l\,(x_i\,, y_i) - \bar{g_l}\,\right)^2}{n\,.\,m - 1}}$$

$$\sigma_R = \sqrt{\frac{\sum_{a=1}^{z}\sum_{b=1}^{c}\left(g_R\,(x_i\,, y_i) - \bar{g_R}\,\right)^2}{n\,.\,m - 1}} \tag{3-18}$$

To evaluate the accuracy of a biometric system, the receiver operating characteristic (ROC) curve and the equal error rate (EER) are used as the main criteria. These two indicators allow comparing the performance of different systems and determining the optimal threshold that achieves a balance between the two error rates. By analyzing the ROC curve, the relationship between the system sensitivity and the false alarm rate can be understood, while the equal error rate determines the point at which the two error rates are equal, which helps improve the performance of the biometric system.

3.3 FINGERPRINT VERIFICATION

In this method, feature point matching is used to compare the input fingerprint data with a previously stored fingerprint template. To facilitate the matching process, the extracted data is stored in the form of a matrix, where this matrix contains a number of rows equal to the number of feature points, and a number of columns equal to 4. These columns include information about each feature point, namely: the row index of each feature point, the column index of each point, the direction angle of each point, and finally the type of feature point. The number "1" is used to indicate the end points, and "3" to indicate the branch points. During the matching process, each feature point in the input fingerprint is compared with the feature point in the reference fingerprint. Reference points from both the template and the input fingerprint are selected to serve as reference points for their respective data sets. These reference points are used to convert the remaining points into polar coordinates.

To convert the points in the template from row and column coordinates to polar coordinates, the equation is used

$$\begin{pmatrix} r_k^T \\ \emptyset_k^T \\ \theta_k^T \end{pmatrix} = \begin{pmatrix} \sqrt{\left(row_t^k - row_{ref}^T\right)^2 + \left(col_T^k - col_{ref}^T\right)^2} \\ \tan^{-1}\left(\frac{row_t^k - row_{ref}^T}{col_T^k - col_{ref}^T}\right) \\ \theta_k^T - \theta_{ref}^T \end{pmatrix} \tag{3-19}$$

Where r_K^T represents the radial distance of the characteristic point k in the template, $\emptyset_K^T$ represents the radial angle of the characteristic point k, θ_K^T represents the direction angle of the landmark point k.

raw_k^T and col_k^T are the row and column coordinates of the landmark k, raw_{ref}^T and col_{ref}^T represent the row and column coordinates of the reference point used.

Vice versa, the fingerprint data is converted to polar coordinates.

$$\begin{pmatrix} r_m^I \\ \emptyset_m^I \\ \theta_m^I \end{pmatrix} = \begin{pmatrix} \sqrt{\left(row_m^I - row_{ref}^I\right)^2 + \left(col_m^I - col_{ref}^I\right)^2} \\ \tan^{-1}\left(\frac{row_m^I - row_{ref}^I}{col_m^I - col_{ref}^I}\right) + rotatevalues(k,m) \\ \theta_k^I - \theta_{ref}^I \end{pmatrix} \tag{3-20}$$

The rotation values (k, m) indicate the difference in orientation angles between Tk and Im. Tk and I_m correspond to the data extracted from all columns in row k and row m of the template and input matrices, respectively

4. RESULTE AND IMPLIMENTAITION

Fingerprint and vein patterns are among the most important biometric templates used for individual recognition, each facing similar challenges related to variations in biometric samples taken from the same person over time. Since biometric templates are inherently uncertain, the matching process is probabilistic, in contrast to the precise matching required in methods like passwords and codes.

To evaluate the performance of biometric systems such as fingerprint and finger vein recognition, one common approach is to use the confusion matrix is a powerful tool in classification tasks, providing a comprehensive view of the system's performance by showing the number of correct and incorrect classifications across different categories[62]. For biometric verification, the categories are typically divided into four possible outcomes:

a. True Positives (TP): Correct identification of a genuine user.

b. False Positives (FP): Incorrect acceptance of an imposter.

c. True Negatives (TN): Correct rejection of an imposter.

d. False Negatives (FN): Incorrect rejection of a legitimate user.

	Positive (1)	Negative (0)
Positive (1)	TP	FP
Negative (0)	FN	TN

Figure 4.1: Confusion Matrix**.**

Using this matrix, we can extract important metrics such as FAR, FRR, True Positive Rate (TPR), and False Positive Rate (FPR). These metrics are essential for understanding the trade-offs between false acceptance and false rejection in biometric systems.

TPR, also known as sensitivity, uses the percentage of actual positives (real users) that are correctly identified by the system. It is given by the equation (**4-1**:

$$TPR = \frac{TP}{TP + FN} \qquad (4\text{-}1)$$

In contrast, FPR measures the proportion of people who might be incorrectly accepted and is calculated by the equation (4-2)

$$FPR = \frac{FP}{FP + TN} \qquad (4\text{-}2)$$

The NUPT-FPV dataset[63] is used, which included samples of fingerprint and finger vein from 840 persons for two sessions, and each person had 10 fingerprint and vein samples taken during the two sessions see Table 4.1 illustrate the details of dataset.

Table 4.1: Statistical Description of the Proposed NUPT-FPV Dataset.

Data	**Subjects**	**Finger**	**Repetitions**	**Session**	**Size**	**Total**
Fingerprint	840	6	10	2	300*400	16800
Finger vein	840	6	10	2	300*400	16800

4.1 FINGERPRINT EVALUATION TEST

In the NUPT-FPV dataset, which consists of two fingerprint sessions, the 10 fingerprints of 840 individuals in the first session were compared with their fingerprints in the second session, Figure 4.2 shows the similarity score for each match, reflecting the degree of closeness between the two fingerprints. The higher the similarity score, the greater the likelihood that the two fingerprints are a match, providing an accurate indicator of potential matching.

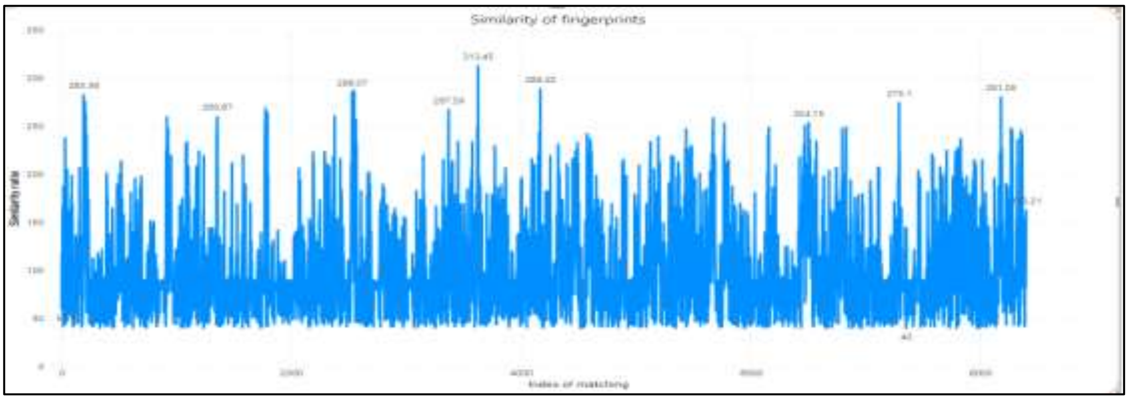


Figure 4.2: Finger print smilarty rate of NUPT-FPV.

When the user acceptance threshold was set at 50, the test results shown in Table 4.2 show a clear picture of the performance of the biometric system used. In terms of successful verification operations, the system achieved 7825 successful verification operations, which reflects a high level of efficiency in correctly identifying users who meet the required criteria. This large number of successful cases reflects the reliability of the system and its ability to verify with high accuracy, On the other hand, the results showed that there were 575 cases that were unable to pass the verification process successfully. This may be due to several factors, such as the quality of the entered biometric data or some limitations in the system itself that prevented some users from being accepted. This number of unsuccessful cases raises questions about the possibility of improving the system's performance, whether by improving the quality of the data or modifying the adopted threshold to achieve a better balance between security and ease of use.

Table 4.2: Details of the Fingerprint Vitrification Evaluation.

Biometric type	Successful Verification	Unsuccessful Verification	Total verification
Fingerprint	7825	575	8400

Another test was conducted to evaluate the False Acceptance Rate (FAR) on the second session, where each person's fingerprints were matched sequentially with the next person: the first person's fingerprints were matched with the second person's, the second people with the thirds, and so on. Since each folder (containing fingerprint data for each person) was only compared with the subsequent folder, the total number of folder comparisons in this second session was 839. As each folder contains 10 fingerprint images, 10 comparisons were made for each pair of folders. Therefore, the final count of matches was calculated by multiplying the number of folder comparisons by the number of images in each comparison. The highest similarity rate reached only 20 minutiae between fingerprints, which is relatively low and does not exceed the predefined threshold see Figure 4.3.

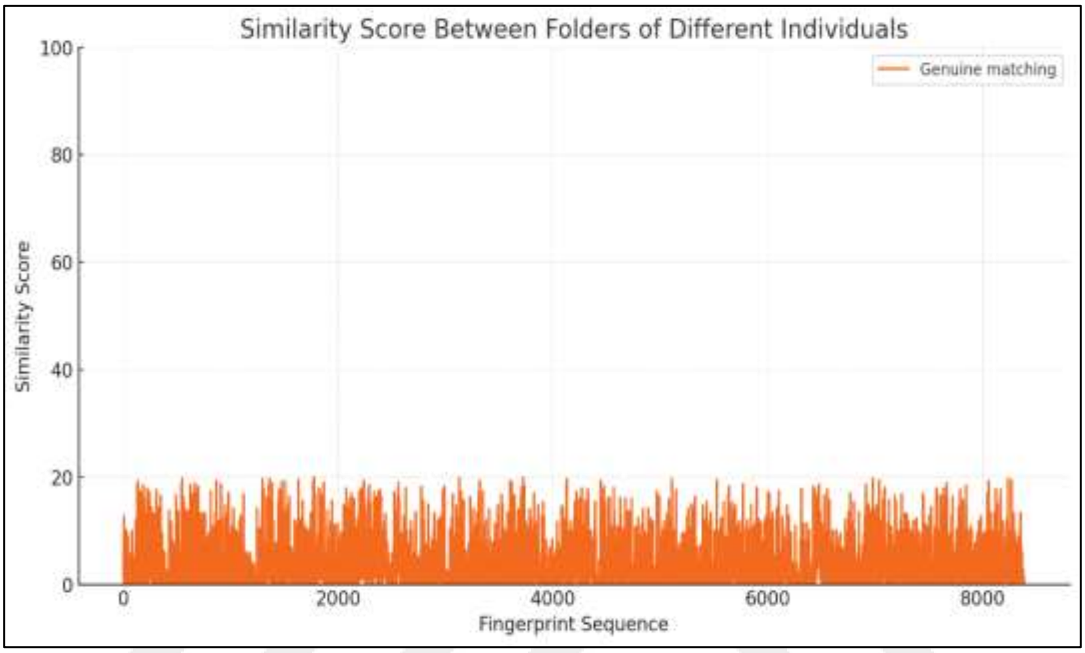


Figure 4.3: Similarity Score between Deferent Person Fingerprints.

Low similarity scores mean that individuals' fingerprints do not match or do not contain very similar features. This is important in the context of identifying individuals and verifying identity using fingerprint recognition systems, where similarity scores are expected to be low when comparing fingerprints from different individuals, which increases the accuracy of the system in avoiding false positives (false matches). Based on the results of the examinations, the confusion matrix can be drawn below figure

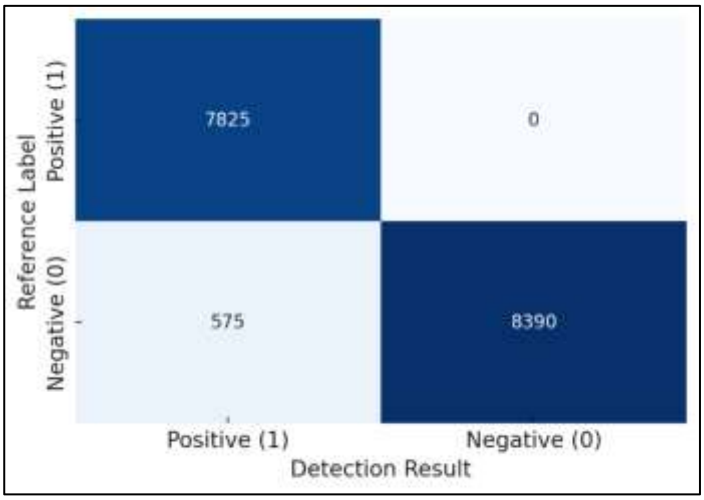


Figure 4.4: Confusion Matrix for Fingerprint Matching.

Next, the fingerprint model accuracy can be calculated as follows:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} = \frac{8390+7825}{7825+8390+0+575} \times 100 \ \cong 96.15\%$$

4.2 FINGER VEIN EVALUATION TEST

As with the fingerprint dataset NUPT-FPV, which consists of two finger vein sessions, the 10-finger vein of 840 individuals in the first session were compared to their fingerprints in the second session.

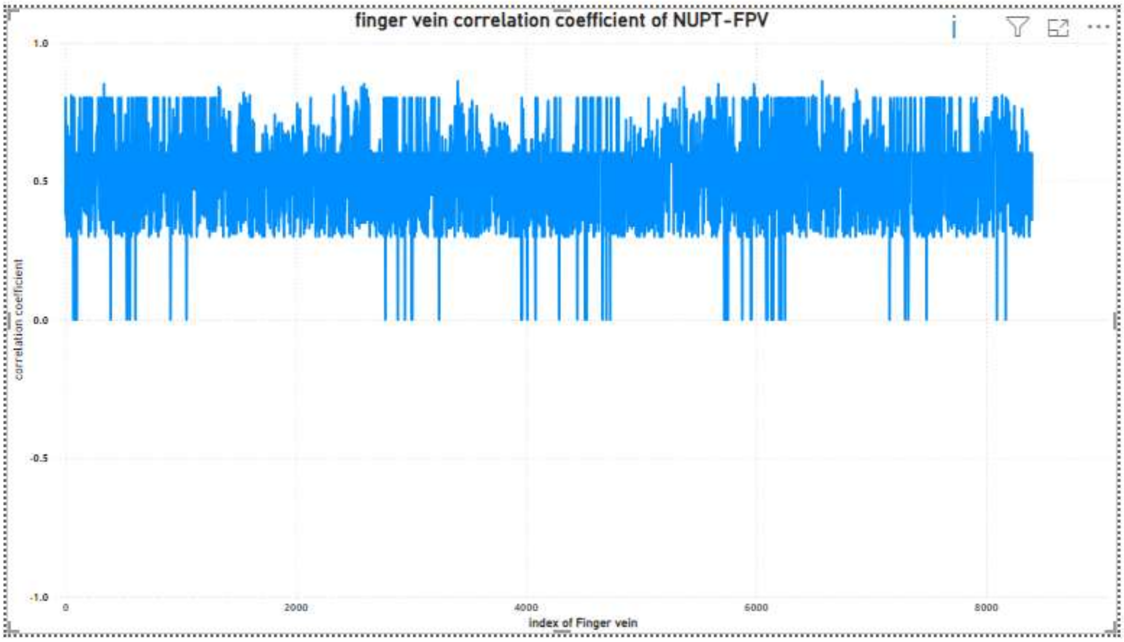


Figure 4.5: Finger Vein Matching Score Using Correlation Coefficient.

When the acceptance threshold was set at 0.5, the test results shown in Table 4.3 provide a clear view of the performance of the utilized biometric vein recognition system. The system successfully verified 6812 instances, indicating a high level of accuracy in correctly identifying users who met the required criteria. This substantial number of successful matches reflects the system's reliability and strong ability to accurately verify identities.

However, the results also revealed 1588 instances where the system failed to verify users successfully. These unsuccessful cases could stem from various factors, such as the quality of the biometric data or inherent limitations within the system itself, which may have impacted certain users' ability to be verified. The presence of these unsuccessful cases highlights areas where the system's performance could potentially be improved, such as by enhancing data quality or adjusting the threshold to achieve a more optimal balance between security and usability.

Table 4.3: Details of the Finger Vein Vitrification Evaluation.

Biometric type	Successful Verification	Unsuccessful Verification	Total verification
Finger vein	6812	1588	8400

The false positive rate (FP) was evaluated by comparing each person's finger vein patterns with the next person in the sequence. The comparison was performed between the first person and the second person, then the second person and the third person, and so on. Since each folder was only compared with the next folder, the total number of comparisons between folders in this session was 839.Each folder contained 10 finger vein images, which means that 10 comparisons were performed for each pair of folders. Therefore, the total number of comparisons was calculated by multiplying the number of comparisons between folders by the number of images in each comparison. The highest value recorded during this test was 0 (i.e. no match between vein images was recorded), which means that the system did not record any FPR during this session. This indicates that the system is effective in preventing false acceptance between different finger vein patterns.

The confusion matrix in finger vein verification can be represented as in the figure.

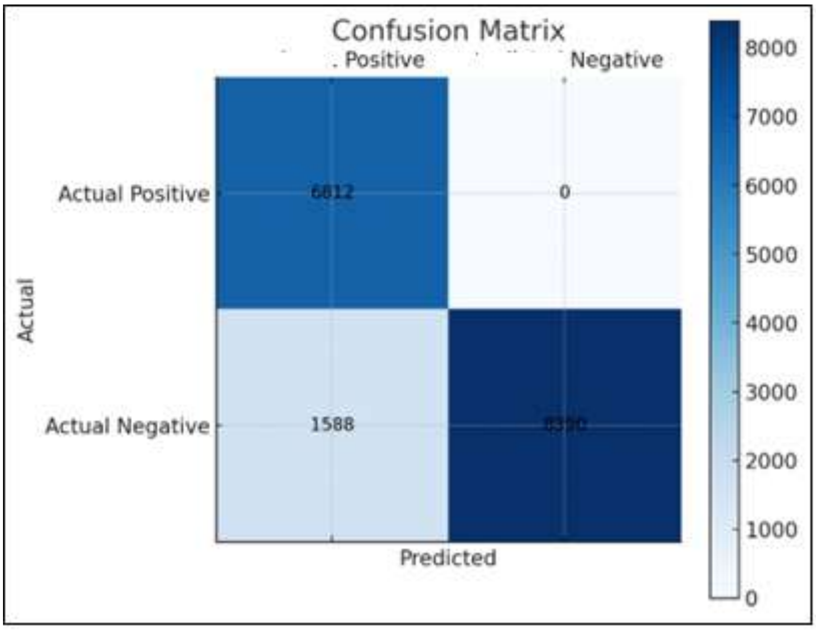


Figure 4.6: Confusion Matrix for Finger Vein Matching Model.

Next, the fingerprint model accuracy can be calculated as follows:

$$\text{Accuracy} = \frac{TP+TN}{TP+TN+FP+FN} = \frac{6812+8390}{6812+8390+0+1588} \times 100 \cong 90.54\% \qquad (4.3)$$

4.3 SYSTEM IMPLEMENTATION

The system being developed aims to simulate the process of verifying the life status of retirees using fingerprint and vein recognition technologies. This verification process can be executed through mobile phones or tablets, but the actual verification must occur on the servers to ensure secure processing.

The system comprises a database that contains essential information about the pensioner, which can be expanded as needed. The system is built using the .NET 5 framework and features a desktop-based user interface.

The system operates in two main phases:

a. The first phase involves enrolment the retiree's biometric data, including fingerprints and vein patterns from all ten fingers. These biometrics are securely stored in the database for future verification see Figure 4.7.

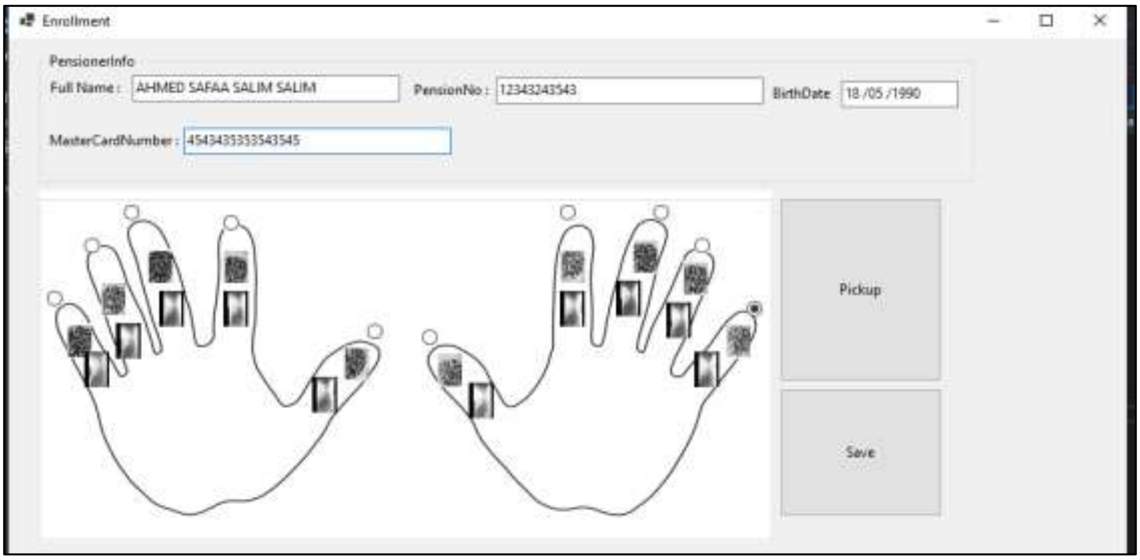


Figure 4.7: Enrolment form to Obtain Pensioner Biometric Data.

b. The second phase involves the verification process, where the stored biometrics are compared with the real-time data collected during the verification request see finger

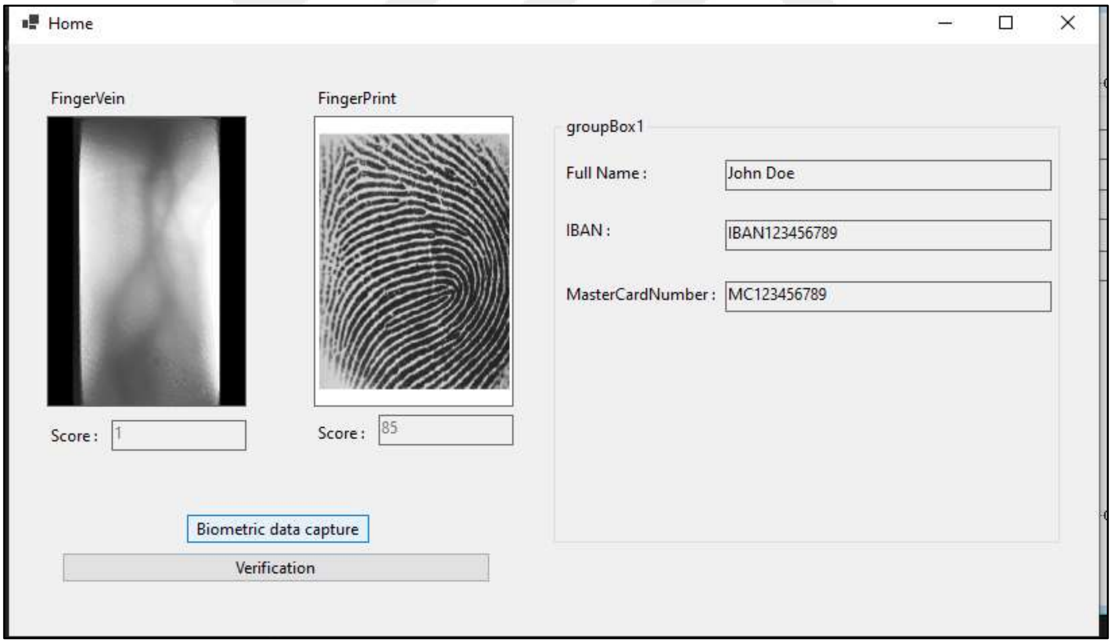


Figure 4.8: Verification Interface Used to Match Fingerprints and Veins in Real Time with Previously Stored Data.

This system provides a reliable method for periodically verifying the life status of retirees, ensuring the protection of their rights and the continuous and secure disbursement of their benefits.

5. CONCLUSION AND FUTURE WORK

Based on the results of the biometric authentication system developed using fingerprint and vein print, it can be concluded that the system showed generally acceptable effectiveness, with an overall success rate of approximately 87.07%. This indicates that using the two methods together enhances the accuracy of the authentication and increases the reliability of the system compared to using each method alone. The data showed that fingerprint achieved a slightly higher matching rate than finger vein, suggesting that vein print may be more effective in certain contexts or with a certain group of individuals. However, the integration of the two methods helped improve the overall performance of the system, reducing the possibility of error and increasing the security of the system, this is a positive result, but it opens the way for future improvements and developments that could further increase the effectiveness of the system. For example, the algorithms used in data matching could be improved to make them more accurate and faster, by taking advantage of modern technologies such as machine learning and deep neural networks. Additional biometric features such as face or iris recognition can also be incorporated to increase the accuracy of the system and reduce the chances of error, taking into account that incorporating multiple features can increase the complexity and cost of the system, In addition, it is important to improve data processing under changing conditions such as lighting changes, skin colour variations, and head or hand movement during the verification process. These improvements can make the system more flexible and effective in real-world operational environments where these challenges are common. Another important aspect to consider is testing the system in real field environments with large and diverse data sets to ensure its performance and effectiveness in real-world operational conditions. The application of the system in other areas, such as security and government systems or banking systems, can also be considered, where a reliable biometric verification system can provide a high level of security and reliability. In addition, it is useful to conduct a cost-benefit analysis of the system in different contexts, with the aim of improving the economic effectiveness of the system and ensuring that it is practical for daily use.

Finally, the focus should also be on the user experience and assessing the level of user satisfaction with the current system. Understanding and analysing their feedback can go a long way in identifying areas for improvement, leading to a more efficient and user-friendly system. In conclusion, these actions and future steps will help enhance the system and increase its effectiveness, making it a reliable and secure option for biometric verification.

REFERENCES

[1] "Life Certificate - Lebensbescheinigung - Federal Foreign Office." Accessed: Nov. 15, 2023. [Online]. Available: https://www.germany.info/us-en/service/07-Pension/life-certificate/917848

[2] "Life Certificate for pensioners: How super senior citizens can submit Jeevan Praman Patra via face authentication | Mint." Accessed: Nov. 15, 2023. [Online]. Available: https://www.livemint.com/money/personal-finance/life-certificate-for-pensioners-how-super-senior-citizens-can-submit-jeevan-praman-patra-via-face-authentication-11696494966440.html

[3] "Consulate General of India, Chicago, USA : Life Certificate." Accessed: Nov. 15, 2023. [Online]. Available: https://www.cgichicago.gov.in/page/life-certificate/

[4] "FAQ: Notarizing Proof Of Life documents | NNA." Accessed: Nov. 15, 2023. [Online]. Available: https://www.nationalnotary.org/notary-bulletin/blog/2017/08/faq-notarizing-proof-of-life-documents

[5] "Embassy of India, Washington D C, USA." Accessed: Nov. 15, 2023. [Online]. Available: https://www.indianembassyusa.gov.in/extra?id=8

[6] "What is a life certificate?" Accessed: Nov. 15, 2023. [Online]. Available: https://www.wypf.org.uk/pensioner/all-about-my-pension/what-is-a-life-certificate/

[7] J. Banks and Z. Oldfield, "Understanding Pensions: Cognitive Function, Numerical Ability and Retirement Saving*," *Fisc Stud*, vol. 28, no. 2, pp. 143–170, Jun. 2007, doi: 10.1111/J.1475-5890.2007.00052.X.

[8] T. N. Friemel, "The digital divide has grown old: Determinants of a digital divide among seniors," *New Media Soc*, vol. 18, no. 2, pp. 313–331, Jun. 2014, doi: 10.1177/1461444814538648.

[9] A. Hope, T. Schwaba, and A. M. Piper, "Understanding digital and material social communications for older adults," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2014, pp. 3903–3912.

[10] S. Behncke, “Does retirement trigger ill health?,” *Health Econ*, vol. 21, no. 3, pp. 282–300, 2012.

[11] D. Dave, I. Rashad, and J. Spasojevic, “The effects of retirement on physical and mental health outcomes,” *South Econ J*, vol. 75, no. 2, pp. 497–523, 2008.

[12] A. Lusardi and O. S. Mitchell, “Financial literacy and retirement planning: New evidence from the Rand American Life Panel,” *Michigan Retirement Research Center Research Paper No. WP*, vol. 157, 2007.

[13] C. J. Dede and J. Richards, *The 60-year curriculum: New models for lifelong learning in the digital economy*. Routledge, 2020.

[14] S. Lissitsa and S. Chachashvili-Bolotin, “Does the wind of change blow in late adulthood? Adoption of ICT by senior citizens during the past decade,” *Poetics*, vol. 52, pp. 44–63, 2015.

[15] “Digital Life Certificate App - UX Case Study | by Venkatakrishnan M | Medium.” Accessed: Nov. 27, 2023. [Online]. Available: https://medium.com/@venkatkrishnan370/digital-life-certificate-app-ux-case-study-adaec27dfec5

[16] “Requirements for organizing life certificates of all kinds - Consulate General of the Republic of Iraq in Detroit.” Accessed: Nov. 27, 2023. [Online]. Available: https://mofa.gov.iq/detroit/?page_id=398

[17] “BBVA Mexico allows its pensioner customers to provide proof of life from home thanks to Veridas voice biometrics | Veridas,” Marta Morrás. Accessed: Nov. 28, 2023. [Online]. Available: https://veridas.com/en/bbva-mexico-allows-pensioner-customers-provide-proof-of-life-from-home/

[18] “PTAD I am alive Verification Process | www.ptad.gov.ng - ZamCash.” Accessed: Nov. 29, 2023. [Online]. Available: https://zamcash.com.ng/ptad-i-am-alive-verification-process/

[19] “FG gives pensioners 6 months’ notice to confirm their aliveness – Nigerian Observer.” Accessed: Nov. 29, 2023. [Online]. Available:

https://nigerianobservernews.com/2023/04/fg-gives-pensioners-6-months-notice-to-confirm-their-aliveness/

[20] "Pensioners' biometric verification twice a year: SBP - Business - DAWN.COM." Accessed: Nov. 29, 2023. [Online]. Available: https://www.dawn.com/news/1605000

[21] "NADRA Launches New Verification Method For Old Citizens." Accessed: Nov. 29, 2023. [Online]. Available: https://propakistani.pk/2023/01/17/nadra-launches-new-verification-method-for-old-citizens/

[22] "Pensioners' biometric verification twice a year: SBP - Business - DAWN.COM." Accessed: Nov. 29, 2023. [Online]. Available: https://www.dawn.com/news/1605000

[23] R. Sharma, "Digital Life Certificate: Facilitating Pension Disbursement in India," *SCMS Journal of Indian Management*, vol. 14, no. 3, pp. 87–92, 2017.

[24] "'Proof of life' certificates required for overseas pensioners - Armstrong Dawson." Accessed: Dec. 01, 2023. [Online]. Available: https://armstrongdawson.com.au/proof-life-certificates-required-overseas-pensioners/

[25] "Proof of Life Certificate form (AUS061) - Services Australia." Accessed: Dec. 01, 2023. [Online]. Available: https://www.servicesaustralia.gov.au/aus061

[26] "Life existence verification." Accessed: Dec. 01, 2023. [Online]. Available: https://www.inps.it/en/en.information-english.pensions.payment-of-pensions.life-existence-verification.html

[27] "Brazil to trial biometric pension benefits app with 10,000 retired civil servants | Biometric Update." Accessed: Dec. 01, 2023. [Online]. Available: https://www.biometricupdate.com/202012/brazil-to-trial-biometric-pension-benefits-app-with-10000-retired-civil-servants

[28] S. Dargan and M. Kumar, "A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities," *Expert Syst Appl*, vol. 143, p. 113114, 2020.

[29] B. Vidyapeeth, “A Comparative Study of Biometric Technologies with Reference to Human Interface K P Tripathi Lecturer (MCA Programme),” 2011.

[30] “How Biometrics Works | HowStuffWorks.” Accessed: Dec. 12, 2023. [Online]. Available: https://science.howstuffworks.com/biometrics.htm

[31] J. R. Vacca, *Biometric Technologies and Verification Systems*. Elsevier Science, 2007. [Online]. Available: https://books.google.com.tr/books?id=Pwv_4mnIRFEC

[32] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, “Handbook of Fingerprint Recognition,” *Handbook of Fingerprint Recognition*, 2009, doi: 10.1007/978-1-84882-254-2.

[33] J.-W. Wang, “Evolutionary optimization approach for fingerprint classifications,” in *Proceedings of the World Congress on Engineering, London, UK*, 2011.

[34] U. S. D. Justice and N. Justice, *The Fingerprint Sourcebook*. CreateSpace Independent Publishing Platform, 2012. [Online]. Available: https://books.google.com.tr/books?id=Z8dyLwEACAAJ

[35] Dimple Parekh, “Fingerprint Classification: A Fusion Scheme: Parekh, Dimple: 9783846520826: Amazon.com: Books.” Accessed: Dec. 22, 2023. [Online]. Available: https://www.amazon.com/Fingerprint-Classification-Fusion-Dimple-Parekh/dp/3846520829

[36] R. Sanchez-Reillo and C. Sanchez-Avila, “Fingerprint verification using smart cards for access control systems,” pp. 250–253, Nov. 2002, doi: 10.1109/.2001.962840.

[37] S. A. COLE and S. A. Cole, *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Harvard University Press, 2009. [Online]. Available: https://books.google.com.tr/books?id=3CYqtVk6oI8C

[38] H. B. Kekr, S. D. Thepade, and D. Parekh, “Comparison of Fingerprint Classification using KFCG Algorithm with various window sizes and codebook sizes,” *Int J Comput Appl*, vol. 46, no. 17, pp. 21–24, 2012.

[39] K. Nagati, *Contribution To The Solution Of Fingerprint Identification Problem: Fingerprints Classification and Identification A Statistical, Structural and Artificial Neural Networks Approach*. LAP Lambert Academic Publishing, 2012.

[40] C. Champod, C. J. Lennard, P. Margot, and M. Stoilovic, *Fingerprints and other ridge skin impressions*. CRC press, 2004.

[41] Y. Yao, G. L. Marcialis, M. Pontil, P. Frasconi, and F. Roli, "Combining flat and structured representations for fingerprint classification with recursive neural networks and support vector machines," *Pattern Recognit*, vol. 36, no. 2, pp. 397–406, 2003, doi: https://doi.org/10.1016/S0031-3203(02)00039-0.

[42] Ł. Więcław, "A minutiae-based matching algorithms in fingerprint recognition systems," *Journal of medical informatics & technologies*, vol. 13, 2009.

[43] H. Kolivand, S. Asadianfam, K. A. Akintoye, and M. S. Rahim, "Finger vein recognition techniques: a comprehensive review," *Multimed Tools Appl*, pp. 1–35, 2023.

[44] "Vein pattern recognition | Recogtech." Accessed: Feb. 25, 2024. [Online]. Available: https://recogtech.com/en/insights-en/how-does-vein-pattern-recognition-work/

[45] G. K. Kyeremeh *et al.*, "Finger vein Recognition," in *2022 International Telecommunications Conference (ITC-Egypt)*, 2022, pp. 1–5. doi: 10.1109/ITC-Egypt55520.2022.9855699.

[46] J. Vijayarajan, "Multi-Biometric System Based On The Fusion Of Fingerprint And Finger-Vein," *ELCVIA Electronic Letters on Computer Vision and Image Analysis*, vol. 23, no. 1, pp. 32–46, 2024.

[47] B. Siddardha and S. Veluchamy, "Hand -Based Multimodal Biometric Authentication System," in *2024 2nd International Conference on Artificial Intelligence and Machine Learning Applications Theme: Healthcare and Internet of Things (AIMLA)*, 2024, pp. 1–5. doi: 10.1109/AIMLA59606.2024.10531351.

[48] J. Guo, J. Tu, H. Ren, C. Han, and L. Sun, “Finger multimodal feature fusion and recognition based on channel spatial attention,” *arXiv preprint arXiv:2209.02368*, 2022.

[49] Y. Shi, Z. Zhong, and J. Yang, “A New Finger Feature Fusion Method Based on Local Gabor Binary Pattern,” in *Biometric Recognition*, Z. You, J. Zhou, Y. Wang, Z. Sun, S. Shan, W. Zheng, J. Feng, and Q. Zhao, Eds., Cham: Springer International Publishing, 2016, pp. 317–325.

[50] A. Alshardan *et al.*, “Multimodal biometric identification: leveraging convolutional neural network (CNN) architectures and fusion techniques with fingerprint and finger vein data,” *PeerJ Comput Sci*, vol. 10, p. e2440, 2024.

[51] S. E. Umbaugh, *Digital Image Processing and Analysis: Digital Image Enhancement, Restoration and Compression*. CRC Press, 2022. [Online]. Available: https://books.google.com.tr/books?id=5QGeEAAAQBAJ

[52] S. Krig, “Image Pre-Processing,” in *Computer Vision Metrics: Survey, Taxonomy, and Analysis*, S. Krig, Ed., Berkeley, CA: Apress, 2014, pp. 39–83. doi: 10.1007/978-1-4302-5930-5_2.

[53] K. Nirmalakumari, H. Rajaguru, and P. Rajkumar, “Efficient Minutiae Matching Algorithm for Fingerprint Recognition,” in *2019 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2019, pp. 1–5. doi: 10.1109/ICACCE46606.2019.9079971.

[54] K. A. P. Perichappan and S. Sasubilli, “Accurate fingerprint enhancement and identification using minutiae extraction,” *Journal of Computer and Communications*, vol. 5, no. 14, pp. 28–38, 2017.

[55] N. P. Khanyile, J.-R. Tapamo, and E. Dube, “A comparative study of fingerprint thinning algorithms,” 2011.

[56] K. Liu, K. Xiao, and H. Xiong, “An Image Edge Detection Algorithm Based on Improved Canny,” in *Proceedings of the 2017 5th International Conference on*

Machinery, Materials and Computing Technology (ICMMCT 2017), Atlantis Press, Apr. 2017, pp. 533–537. doi: 10.2991/icmmct-17.2017.114.

[57] Timothy Malche, "Edge Detection in Image Processing: An Introduction." Accessed: Jul. 21, 2024. [Online]. Available: https://blog.roboflow.com/edge-detection/

[58] S. S. Jumaa and K. Zidan, "Finger vein recognition using two parallel enhancement ppproachs based fuzzy histogram equalization," *Periodicals of Engineering and Natural Sciences*, vol. 7, no. 1, pp. 514–529, 2019.

[59] P. Garg and T. Jain, "A Comparative Study on Histogram Equalization and Cumulative Histogram Equalization," *International Journal of New Technology and Research*, vol. 3, no. 9, 2017.

[60] D. Sheet, H. Garud, A. Suveer, M. Mahadevappa, and J. Chatterjee, "Brightness Preserving Dynamic Fuzzy Histogram Equalization," 2010.

[61] A. P. Vega, C. M. Travieso, and J. B. Alonso, "Biometric personal identification system based on patterns created by finger veins," in *3rd IEEE International Work-Conference on Bioinspired Intelligence*, 2014, pp. 65–70. doi: 10.1109/IWOBI.2014.6913940.

[62] A. Arias-Duart, E. Mariotti, D. Garcia-Gasulla, and J. M. Alonso-Moral, "A confusion matrix for evaluating feature attribution methods," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2023, pp. 3709–3714.

[63] H. Ren, L. Sun, J. Guo, and C. Han, "A Dataset and Benchmark for Multimodal Biometric Recognition Based on Fingerprint and Finger Vein," *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 2030–2043, 2022, doi: 10.1109/TIFS.2022.3175599.