Mohamed Khider University of Biskra
Faculty of Science and Technology
Department of Electrical Engineering

MASTER THESIS

Electrical Engineering
Telecommunication
Networks and Telecommunication

Réf. : Entrez la référence du document

Submitted and Defended by:
REZGUI ABDELMOUMEN ZAKI
KHERIF DJEMAI ISLAM EDDINE

On: Thursday, June 05, 2025

FACE AUTHENTICATION WITH FFT

Board of Examiners:

Dr.	MEDOUAKH Saadia	**MCB**	University of Biskra	**President**
Dr.	TOUMI ABIDA	**MCA**	University of Biskra	**Examiner**
Dr.	FEDIAS Meriem	**MCB**	University of Biskra	**Supervisor**

University year: 2024 - 2025

Mohamed Khider University of Biskra
Faculty of Science and Technology
Department of Electrical Engineering

MASTER THESIS

Electrical Engineering
Telecommunication
Networks and Telecommunication

Réf. : Entrez la référence du document

Submitted and Defended by:
REZGUI ABDELMOUMEN ZAKI
KHERIF DJEMAI ISLAM EDDINE

On: Thursday, June 05, 2025

FACE AUTHENTICATION WITH FFT

In: Thursday, June 05, 2025

Presented by:

REZGUI ABDELMOUMEN ZAKI
KHERIF DJEMAI ISLAM EDDINE

Favorable opinion of the supervisor:

Favorable opinion of the jury president

Stamp and signature

Acknowledgements

First and foremost, I would like to express my sincere gratitude to my supervisor, Miss Fidias Meriem, for their invaluable guidance, continuous support, and encouragement throughout the course of this project. Their expertise and insightful feedback greatly enriched this work.

I am also thankful to the faculty and staff of Mohamed Khider University – BISKRA , Faculty of Science and Technology , Department of Electrical Engineering , for providing a stimulating and supportive academic environment. Special thanks to my colleagues and friends for their helpful discussions, cooperation, and motivation.

Finally, I would like to thank my family for their unwavering love, patience, and moral support, which have been essential to my academic journey.....

Dedication

This work is humbly and gratefully dedicated to all the people who have been part of my journey, each contributing in their unique way to the person I have become and the work I present here.

To my beloved family my parents, who have been the foundation of my dreams, thank you for your unwavering support, unconditional love, and the countless sacrifices you have made to ensure I had the opportunities and encouragement to pursue my goals. Your belief in me has been my guiding light, and your patience during the most challenging times has been a source of strength and resilience.

To my siblings, who have inspired me with their determination, perseverance, and laughter, thank you for reminding me of the importance of balance and joy in life.

To my extended family, thank you for your encouragement and prayers, which have sustained me throughout this academic journey.

To my teachers and mentors, whose wisdom, guidance, and encouragement have helped me navigate the complexities of my field thank you for your dedication to imparting knowledge and fostering curiosity. Your passion for teaching and research has been a beacon, and your confidence in my abilities has motivated me to push beyond my limits.

To my friends and colleagues, who have stood by me through thick and thin, sharing in the joys and challenges, thank you for your companionship, support, and the countless hours of discussions, debates, and laughter that have enriched my academic and personal life. Your friendship has been a gift, and your insights have sharpened my understanding.

To all those who inspire innovation and growth in the field of technology and biometrics, your work has laid the foundation upon which this project stands. May this humble contribution add a small but meaningful step towards the advancement of knowledge.

Abstract

This thesis proposes a facial recognition system based exclusively on the Fast Fourier Transform (FFT) for feature extraction. To enhance the quality of facial inputs, the system incorporates key preprocessing steps including cropping, photonormalization, and resolution decimation. Evaluation is conducted on the XM2VTS database in accordance with the Lausanne Protocol, yielding a recognition accuracy of 70.88%. The results confirm that FFT-based spectral analysis offers a robust, computationally efficient, and practical approach for biometric authentication in real-world scenarios.

.

Contents

List of Figures

General Introduction

In the modern digital era, where the flow of information is constant and the protection of data is paramount, the need for secure and efficient authentication systems has grown tremendously. Traditional authentication methods, such as passwords, ID cards, or PIN codes, are no longer sufficient to guarantee optimal security, especially in contexts that require high-level identification accuracy. These conventional systems are often vulnerable to theft, duplication, and misuse. As a result, biometric authentication has emerged as a compelling alternative that offers a higher level of reliability by leveraging physiological or behavioral characteristics unique to each individual [37].

Among the various biometric techniques, facial recognition stands out due to its contactless nature, user-friendliness, and integration compatibility with existing imaging systems such as cameras and smartphones. A facial recognition system can be used in numerous sectors, including national security, financial services, healthcare, and smart access control systems. This project focuses specifically on facial authentication, with a detailed exploration of the application of spectral analysis methods—**Fast Fourier Transform (FFT)**[71], **Discrete Cosine Transform (DCT)**[57], and **Principal Component Analysis (PCA)**—to enhance recognition performance.

The objective of this final year project is to design and evaluate a facial authentication system that is both efficient and accurate. We aim to exploit the potential of frequency-based transformations to extract robust facial features that are invariant to noise, illumination changes, and minor occlusions. The project's structure follows a classical pipeline in biometric systems: preprocessing, feature extraction, and classification. Images are first normalized and standardized using techniques such as image cropping, resizing, and photonormalization. Feature extraction is carried out using FFT, DCT, and PCA, each offering a unique method for reducing dimensionality and emphasizing discriminative traits. Finally, similarity measures based on correlation are employed to compare extracted feature vectors and classify the input image [35].

To ensure consistent and reproducible evaluation, our experiments are based on the **XM2VTS database**, a benchmark multimodal dataset that provides multiple recordings of subjects under controlled environments. We adhere to the **Lausanne Protocol**, which defines the separation of training, evaluation, and testing datasets, while also providing a structured methodology for assessing the system's robustness against impostor attacks.

This thesis is organized into four chapters. The first chapter introduces biometric systems [35] and presents an overview of various facial recognition techniques. The second chapter is dedicated to the theoretical background of the FFT, DCT, and PCA algorithms. The third chapter discusses the system's architecture and implementation. Finally, the fourth chapter presents a detailed evaluation of the experimental results, along with comparisons and performance metrics such as FAR, FRR, and EER.

Through this project, we hope to contribute to the ongoing evolution of biometric authentication technologies and propose a reliable method for facial recognition based on well-established spectral analysis tools.

Chapter 1

Biometric Technologies

1.1 Introduction

Biometric systems have become an integral part of modern security and identification solutions. By utilizing unique physical or behavioral traits[29], these systems provide reliable and efficient methods for verifying identity. In this chapter, we explore the main aspects of biometric techniques, starting with the essential properties that make a biometric modality effective and reliable. We then examine the various areas where biometric systems are applied, showcasing their impact across different sectors. A comparison of the leading biometric technologies follows, highlighting their strengths and limitations [27]. Next, we delve into the main modules that constitute a biometric system, outlining how each component contributes to the overall functionality. Finally, we discuss the evaluation of biometric system performance, ensuring accuracy and security in real-world applications[41]. This comprehensive overview sets the stage for understanding the capabilities and challenges of biometric technologies, paving the way for their effective implementation.

1.2 The Main Biometric Techniques

1.2.1 Facial Recognition

1. **Definition and Principle:** Facial recognitionas shown in Figure 1.1 is a biometric technique that identifies or verifies a person by analyzing the unique features of their face. These features include the shape of the eyes, nose, mouth, and overall facial structure. This technology relies on the fact that every human face has distinct features that remain relatively constant over time [38].

- 2D Facial Recognition: Analyzes facial features from a 2D image, focusing on geometric relationships between facial landmarks.
- 3D Facial Recognition: Uses depth information from 3D sensors to capture facial contours and shapes, making it more robust to changes in lighting and head position.

2. **Application**

   - Security and surveillance (e.g., CCTV systems).
   - Mobile authentication (e.g., Face ID on smartphones).
   - Social media photo tagging (e.g., Facebook, Google Photos).

3. **Advantages and Challenges**

   - **Advantages:** Non-intrusive, contactless, and user-friendly. Can work from a distance and in real-time.
   - **Challenges:** Sensitive to variations in lighting, facial expressions, and head pose. Vulnerable to spoofing using photos or masks. Privacy concerns due to mass surveillance potential.

FIGURE 1.1: Facial Recognition [46]

1.2.2 Fingerprint Recognition

1. **Definition and Principle:** Fingerprint recognition as shown in Figure 1.2 identifies individuals by analyzing the unique patterns of ridges and valleys on their fingertips. These patterns are formed during fetal development and remain unchanged throughout a person's life [40].

2. **Applications**

   - Mobile device unlocking and payment authentication.
   - Law enforcement (criminal identification and background checks).
   - Access control systems in offices and secure facilities.

3. **Advantages and Challenges**

   - **Advantages:** High accuracy, mature technology with established standards, and relatively low cost.
   - **Challenges:** Affected by skin conditions (e.g., cuts, dryness). Vulnerable to spoofing using fake fingerprints.

FIGURE 1.2: Fingerprint Recognition [12]

1.2.3 Iris Recognition

1. **Definition and Principle:** Iris recognition as shown in Figure 1.3 uses the unique patterns in the colored ring surrounding the pupil to identify individuals. The iris has complex patterns of rings, furrows, and freckles that are unique to each person and remain stable throughout their lifetime [15].

2. **Applications**

   - Border control and immigration (e.g., Automated Passport Control).
   - High-security access control (e.g., data centers, research labs).
   - Financial transactions (e.g., ATMs with iris scanners).

3. **Advantages and Challenges**

   - **Advantages:** Extremely accurate and resistant to spoofing. Non-contact and hygienic.

- **Challenges:** Requires user cooperation and specialized infrared cameras. Affected by eye conditions (e.g., cataracts, contact

FIGURE 1.3: IRIS Recognition [54]

1.2.4 DNA Recognition

1. **Definition and Principle:** DNA recognition as shown in Figure 1.4 identifies individuals based on their unique genetic code. Every person (except identical twins) has a unique DNA sequence. DNA is extracted from biological samples such as hair, blood, or saliva and analyzed using techniques like PCR (Polymerase Chain Reaction)[11].

2. **Applications**

   - Criminal investigations and forensic science.
   - Paternity testing and familial relationships.
   - Identification of disaster victims.

3. **Advantages and Challenges**

   - **Advantages:** Highly accurate and reliable. Unique to each individual.
   - **Challenges:** Invasive collection process. Privacy and ethical concerns. Time-consuming analysis.

FIGURE 1.4: DNA Recognition[32]

1.2.5 Signature Recognition

1. **Definition and Principle:** Signature recognition as shown in Figure 1.5 verifies a person's identity by analyzing their handwritten signature. It examines the shape, speed, stroke order, and pressure of the signature. It can be either static (analyzing the image) or dynamic (analyzing the signing process)[51].

2. **Applications**

   - Document authentication (e.g., contracts, legal documents).
   - Banking and financial transactions.
   - Access control for secure systems.

3. **Advantages and Challenges**

   - **Advantages:** Non-intrusive and widely accepted.
   - **Challenges:** Signature variability due to mood, health, or aging. Vulnerable to skilled forgeries.

FIGURE 1.5: Signature Recognition[1]

1.2.6 Ear Recognition

1. Definition and Principle: Ear recognition as shown in Figure 1.6 identifies individuals by analyzing the unique shape and structure of their outer ear. The ear's anatomy remains relatively constant throughout a person's life, making it a reliable biometric trait [9].

2. **Applications**

   - Security and surveillance systems.
   - Mobile authentication (in development).

3. **Advantages and Challenges**

   - **Advantages:** Non-intrusive and stable over time.
   - **Challenges:** Affected by hairstyles, headwear, or ear accessories. Limited research and application compared to other biometrics.

FIGURE 1.6: Ear Recognition[17]

1.2.7 Hand Recognition

1. **Definition and Principle:** Hand recognition as shown in Figure 1.7 identifies individuals by analyzing the shape, size, and geometry of their hand, including finger length, width, and distances between knuckles. It can also include palm print recognition, analyzing the unique patterns on the palm [28].

   Applications

   - Access control in secured facilities.
   - Time and attendance tracking systems

   Advantages and Challenges

   - **Advantages:** Non-intrusive and user-friendly.
   - **Challenges:** Less accurate than other biometrics. Affected by hand positioning and pressure variations.

FIGURE 1.7: Hand Geometry Recognition [8]

1.2.8 Eye Recognition

1. **Definition and Principle:** Eye recognition as shown in Figure 1.8 includes two main techniques:

   - **Iris Recognition:** Analyzes the unique patterns in the colored ring surrounding the pupil [14].
   - **Retina Scanning:** Identifies individuals by analyzing the pattern of blood vessels in the retina at the back of the eye.

2. **Applications**

   - High-security access control.
   - Border control and immigration.
   - Financial transactions with high security.

3. **Advantages and Challenges**

   - **Advantages:** Extremely accurate and secure. Non-contact and hygienic.
   - **Challenges:** Requires specialized hardware. User cooperation needed. Affected by eye conditions (e.g., cataracts, contact lenses).

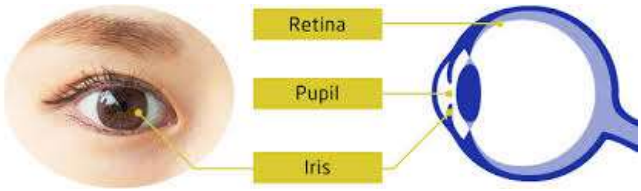

FIGURE 1.8: EYE Recognition [45]

1.2.9 Voice Recognition

1. **Definition and Principle:** Voice recognition as shown in Figure 4.3identifies individuals by analyzing their unique vocal characteristics, including pitch, tone, and speaking style. It can be text-dependent (specific phrases) or text-independent (any speech)[33].

2. **Applications**

   - Call center authentication and fraud prevention.
   - Voice-activated virtual assistants (e.g., Alexa, Google Assistant).
   - Secure voice communication systems.

3. **Advantages and Challenges**

   - **Advantages:** Hands-free and convenient. Can be used remotely.
   - **Challenges:** Affected by background noise and voice changes (e.g., illness). Vulnerable to spoofing using voice recordings.

FIGURE 1.9: Voice Recognition [62]

1.3 Comparison of Biometric Technologies

The International Biometric Group's evaluation framework assesses biometric systems through four key criteria: This comparison allows for selecting a technology based on the constraints related to the application. Figure 1.10 shows that there is no ideal method. The methods are divided into two main groups. The first group includes user-friendly methods (low effort required, non-intrusive, moderate cost) but is rather less effective. This group corresponds to methods based on behavioral biometrics (recognition of voice, signature, etc.) [28]. The other group contains more secure methods (intrusive methods and high costs, very good performance). It is therefore necessary to determine, on a case-by-case basis, the method that will best suit the situation for each problem. To do this, one must carefully study the required level of security, the budget that can be invested in the system, and how users may react. Currently, for the implementation of large biometric passport projects, the systems chosen by Europe seem to be a storage of the identity photo, fingerprints, and iris in digital form [67]. It should be noted that the choice of. The acceptance of biometric devices may also depend on local culture. Thus, in Asia, methods requiring physical contact such as fingerprints are rejected for hygiene reasons, while iris-based methods are very well accepted. Keystroke dynamics is one of the least effective biometric methods but is very interesting in terms of cost, effort required, and perceived level of intrusion. It is therefore suited for securing less sensitive areas where there is neither the desire nor the possibility to allocate very high budgets. In France, CLUSIF has also proposed a comparison (advantages/disadvantages) of the main biometric technologies[9].As shown in the following Table in the next page

TABLE 1.1: Advantages and Disadvantages of Different Biometric Technologies

Techniques	Advantages	Disadvantages
Fingerprints	Cost-effective, average ergonomics. Easy to implement. Small sensor size	Requires high-quality measurement devices. Medium user acceptance. Susceptible to attacks
Hand geometry	Highly ergonomic. Good user acceptance	Bulky system. Expensive. Can be affected by injuries or psychological factors
Face	Low cost, compact. Good user acceptance	Issues with twins, psychological factors. Religion, disguises. Vulnerable to attacks
Retina	High reliability and durability	Expensive. Low user acceptance. Difficult to install
Iris	High reliability	Very low user acceptance. Lighting constraints. Affected by emotional state
Voice	Easy to use. Ergonomic	Vulnerable to attacks. Affected by emotional state. Reliability issues
Signature	Ergonomic	Affected by emotional state. Reliability issues
Keystroke dynamics	Ergonomic	Affected by physical condition

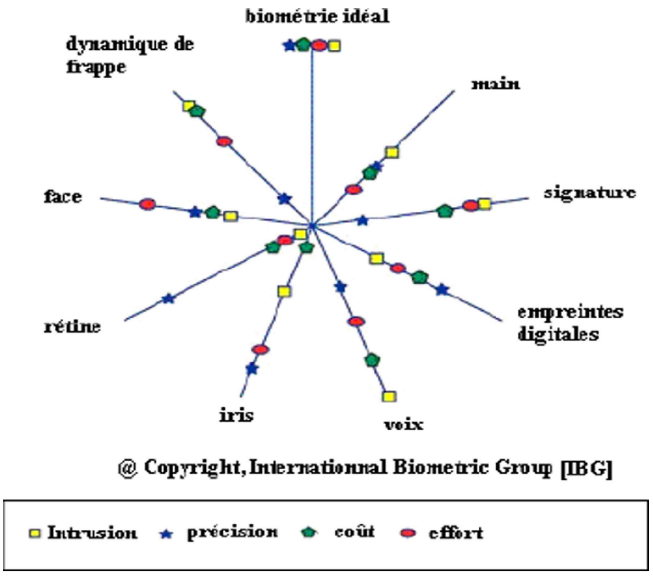

FIGURE 1.10: Comparison of Biometric Technologies[25]

For facial recognition, it is a common, popular, simple technique that has many advantages, such as the use of faces which are public data, the ability to integrate into existing surveillance systems, and it does not require expensive equipment. For this reason, facial recognition is the biometric technology. that will be used in our recognition system. In the following chapter, we briefly examine the main algorithms that have been developed over the last two decades to address the challenging problem of face identification or verification. We then describe in detail the algorithms we used in this thesis.

1.4 Principal Properties of a Biometric Modality

1.4.1 Universality

Definition: Universality refers to the presence of the biometric characteristic in every individual within the target population. It ensures that the system can enroll and authenticate all users without exclusions [19].

Explanation: For a biometric modality to be practical, it must be universally available among all users. For example, fingerprints are generally universal, but some individuals may have worn fingerprints due to age or occupation. In contrast, iris patterns are more universally present but can be challenging to capture in cases of blindness or severe eye injuries.

Challenges: Universality may be compromised in cases of disability, injury, or illness. Therefore, alternative modalities might be required for inclusivity.

1.4.2 Distinctiveness

Distinctiveness **Definition:** Distinctiveness ensures that no two individuals have identical biometric characteristics, allowing the system to distinguish between different users[49].

Explanation: This property is crucial for accurate identification and authentication. For example, DNA and iris patterns offer high distinctiveness, whereas voice patterns might be less unique due to similarities among family members.

Challenges: In modalities like facial recognition, identical twins or family members with similar features can challenge distinctiveness. Advanced algorithms are often required to address these cases.

1.4.3 Stability

Definition: Stability refers to the consistency of the biometric characteristic over time. It should not change significantly due to age, health, or environmental factors[64].

Explanation: A stable biometric ensures that once enrolled, the user does not need frequent re-enrollment. For example, iris patterns and DNA remain stable throughout life, whereas voice or facial features can change due to aging, illness, or weight changes.

Challenges: Some modalities are affected by environmental or personal conditions—e.g., voice recognition is influenced by illness or emotional states, and fingerprints can be affected by cuts or abrasions.

1.4.4 Collectability

Definition: This property refers to the ease and convenience of acquiring the biometric data using available technology[64].

Explanation: A good biometric modality can be measured and digitized quickly and accurately. For example, facial recognition and fingerprint scanning are highly collectable, while DNA collection is more complex and invasive.

Challenges: Some modalities require specialized equipment or controlled environments for accurate data capture, such as retinal scanners needing precise alignment and lighting.

1.4.5 Acceptance

Definition: Acceptance refers to the level of user comfort and willingness to use the biometric modality. It is influenced by cultural, social, and psychological factors [64].

Explanation: If users are uncomfortable or perceive a modality as invasive, they may be reluctant to use the system. In contrast, non-intrusive methods like facial recognition or voice recognition typically have higher acceptance rates.

Challenges: Acceptance varies by culture and individual preference. For example, in some cultures, touching a sensor (e.g., for fingerprints) may be considered unhygienic.

1.4.6 Circumvention

Definition: This property measures the difficulty of fooling or bypassing the biometric system using fraudulent methods [64].

Explanation: A robust biometric modality should be resistant to spoofing attacks, such as using a photograph to bypass facial recognition or a recorded voice for voice authentication.

Challenges: Some modalities are more vulnerable to spoofing than others. For instance, 2D facial recognition is easier to deceive than 3D facial mapping, which uses depth information to verify liveness.

1.4.7 Performance

Definition: Performance evaluates the accuracy, speed, and robustness of the biometric system under various operational and environmental conditions [31].

Explanation: A high-performing system maintains low error rates, quick processing times, and reliable functionality regardless of lighting, noise, or other environmental changes.

Challenges: Performance can be affected by hardware quality, environmental conditions, and user behavior (e.g., varying facial expressions or voice modulation).

1.4.8 Balancing Properties for System Design

No biometric modality perfectly satisfies all these properties. Some modalities may exhibit them to varying degrees. Therefore, choosing the right one requires balancing these properties based on system requirements, application context, and user demographics [31].

1.4.9 Choosing the Right Biometric Modality

Choosing a biometric modality requires a trade-off between these properties. High-security applications may prioritize distinctiveness and circumvention resistance, while consumer applications may prioritize collectability and acceptance. Multimodal systems can also enhance security and user experience [49].

1.5 Application domain

1.5.1 Security and Access Control

Physical Access Control: Biometric systems are widely used for controlling access to secure areas such as offices, data centers, airports, and military facilities. Examples include fingerprint scanners, facial recognition systems, and iris scanners [68].

Logical Access Control: Biometrics are used to secure digital systems, including computers, mobile devices, and networks. This includes biometric login methods such as fingerprint and facial recognition for smartphones and laptops.Fiure 1.11 represent Security and Access Control

FIGURE 1.11: Security and Access Control[34]

Identification and Verification

Law Enforcement and Forensics: Biometrics play a crucial role in criminal identification, including fingerprint matching, facial recognition from surveillance footage, and DNA profiling [61].

Civil Identification: National ID systems, voter registration, and census data collection use biometrics to ensure accurate identification and reduce fraud. For example, many countries use biometric passports and national ID cards with embedded fingerprints or iris data.

1.5.2 Financial Services and Transactions

Payment Authentication: Biometric authentication methods like fingerprint or facial recognition are increasingly used for secure payment transactions, including mobile payments and ATMs [36].

Fraud Prevention: Biometrics help prevent identity theft and unauthorized access in banking and financial services by verifying the identity of users during online transactions Figure 1.12.

FIGURE 1.12: Financial Services and Transactions [24]

1.5.3 Healthcare and Medical Applications

Patient Identification: Biometrics ensure accurate patient identification, reducing medical errors and preventing identity fraud in healthcare services [36]. Access Control in Healthcare Facilities: Securing sensitive areas such as pharmacies, laboratories, and patient records using biometric authentication.

Remote Patient Monitoring: Biometrics, like voice recognition and facial recognition, are used for patient verification in telemedicine and remote healthcare services Figure 1.13.

FIGURE 1.13: Healthcare and Medical Applications [69]

1.5.4 Travel and Immigration

Border Control and Immigration: Biometrics are widely used at border crossings for identity verification, including e-passports with embedded biometric data (e.g., fingerprints or facial recognition) [36].

Airport Security: Automated border control gates and biometric boarding systems enhance security and streamline passenger flow using facial recognition or iris scanning Figure

FIGURE 1.14: Travel and Immigration [56]

1.5.5 Workforce Management

Attendance and Time Tracking: Organizations use biometric systems such as fingerprint or facial recognition for accurate employee attendance and time tracking, reducing time fraud [61].

Access Control: Securing restricted areas within organizations, ensuring only authorized personnel can enter sensitive zones.

1.5.6 Commercial Applications

Customer Experience and Personalization: Retailers use facial recognition for personalized marketing and customer engagement by recognizing returning customers and tailoring product recommendations.

Entertainment and Gaming: Biometric authentication is used for secure access to digital content, preventing piracy and ensuring age verification.

1.5.7 Mobile and Digital Authentication

Smartphones and Wearables: Biometric authentication, such as fingerprint scanners, facial recognition, and voice recognition, are commonly used for unlocking devices and authorizing app purchases.

App Security and Authentication: Biometric authentication provides secure access to apps and online services, replacing traditional passwords Figure 1.15 [68].

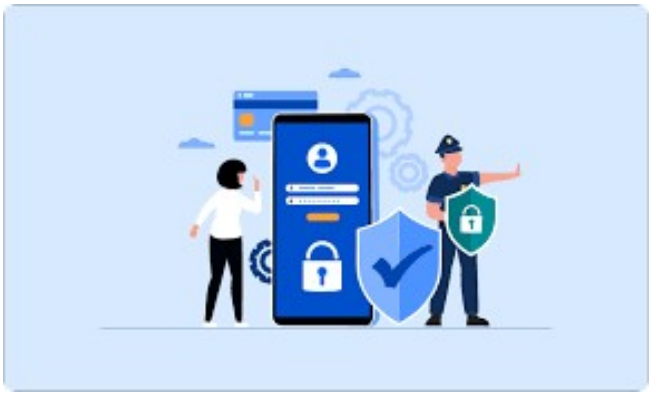

FIGURE 1.15: Mobile and Digital Authentication [55]

1.5.8 Education and Examination Security

Student Verification: Educational institutions use biometrics for student identification during examinations to prevent cheating and identity fraud .

Access Control: Securing access to educational facilities and resources, such as libraries and laboratories.

Biometrics are increasingly becoming an integral part of modern security systems, ensuring accurate identification, enhancing security, and improving user convenience across various sectors. As technology advances, the adoption of biometric solutions continues to grow, influencing everyday life and transforming how identity is managed Figure 1.16.

FIGURE 1.16: Education and Examination Security [53]

1.6 Main Modules of a Biometric System

1.6.1 Sensor Module

The sensor module is responsible for capturing the biometric data of an individual. It serves as the interface between the user and the biometric system. Depending on the type of biometric modality, different sensors are used, such as fingerprint scanners, cameras for facial recognition, or microphones for voice recognition [33].

Key Functions:

- Captures raw biometric data (e.g., image, voice, fingerprint pattern).
- Ensures quality of data capture to enhance accuracy and reliability.
- Preprocessing of data to reduce noise and enhance features.

1.6.2 Feature Extraction Module

This module processes the captured biometric data to extract distinctive features that can uniquely identify an individual. The extracted features are then converted into a digital template for further processing [26].

Key Functions:

- Identifies and extracts unique patterns or features (e.g., minutiae in fingerprints, iris patterns, or facial landmarks).
- Converts raw data into a mathematical representation or template.
- Ensures the template is compact and efficient for storage and matching.

1.6.3 Database Module

The database module securely stores the biometric templates of enrolled users. It maintains a collection of biometric records that are used during the matching process.

Key Functions:

- Stores biometric templates along with corresponding user identities.
- Ensures data integrity and security to prevent unauthorized access or modification.
- Manages the enrollment and deletion of user records.

1.6.4 Matching Module

The matching module compares the extracted features from the input biometric data with the stored templates in the database. It determines whether the input data matches any existing record [49].

Key Functions:

- Performs template matching using algorithms specific to the biometric modality.
- Computes a similarity score to quantify the match.
- Applies matching thresholds to determine acceptance or rejection.

1.6.5 Decision Module

The decision module makes the final authentication or identification decision based on the matching score. It compares the score to a predefined threshold to determine a match or mismatch.

Key Functions:

- Accepts or rejects the identity claim based on matching results.
- Handles false acceptance and false rejection rates to maintain system accuracy.
- Provides feedback to the user (e.g., access granted or denied).

1.6.6 User Interface Module

The user interface module facilitates interaction between the user and the biometric system. It provides prompts for biometric data capture, feedback on the authentication process, and results of the verification [49].

Key Functions:

- Guides users during the data capture process (e.g., positioning for facial recognition).
- Displays authentication outcomes.
- Ensures a user-friendly experience.

1.6.7 Security Module

This module is responsible for maintaining the security and privacy of biometric data. It implements encryption techniques to protect data during storage and transmission.

Key Functions:

- Encrypts biometric templates to prevent unauthorized access.
- Protects against spoofing and replay attacks.
- Ensures compliance with data protection regulations.

A biometric system is composed of multiple interconnected modules, each playing a crucial role in ensuring accurate and secure identification or authentication. From capturing raw biometric data to making the final decision, each module contributes to the system's overall performance. The efficiency, accuracy, and security of a biometric system depend on the effective integration and functioning of these modules.

1.7 Evaluation of the Performance of a Biometric System

To evaluate the performance of a biometric system, two primary types of errors are considered:

1.7.1 False Acceptance Rate (FAR)

The False Acceptance Rate (FAR) evaluates how often the system mistakenly recognizes two distinct biometric samples as originating from the same person [30]. FAR is calculated as:

$$\text{FAR} = \frac{\text{Number of Accepted Imposters}}{\text{Total Number of Imposter Access Attempts}}$$

FAR :False Acceptance Rate

1.7.2 False Rejection Rate (FRR)

The False Rejection Rate (FRR) measures the frequency with which the system incorrectly classifies two samples from the same individual as coming from different people [18].Figure 1.17 represent FAR and FRR Diagram FRR is calculated as:

$$\text{FRR} = \frac{\text{Number of Rejected Clients}}{\text{Total Number of Client Access Attempts}}$$

FRR:False Rejection Rate

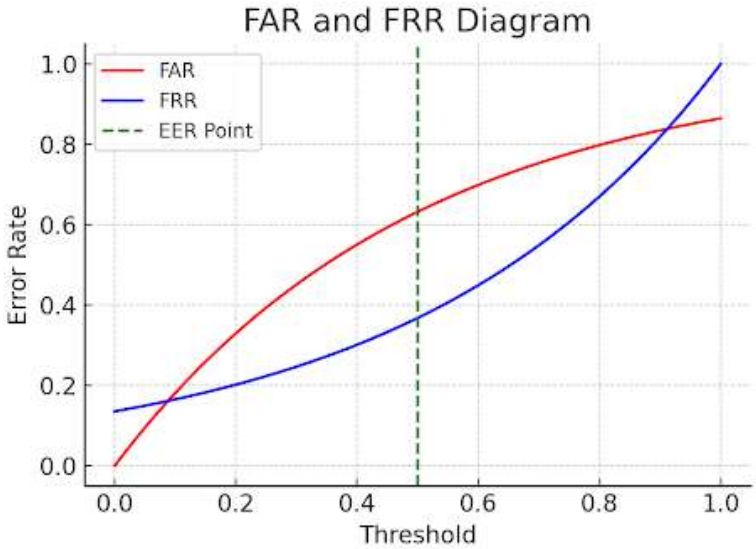

FIGURE 1.17: FAR and FRR Diagram [7]

1.7.3 Equal Error Rate (EER)

After calculating FAR and FRR, the Equal Error Rate (EER) is determined. It represents the point where FAR and FRR are equal, offering the optimal balance between

false acceptances and false rejections. EER is a key indicator for evaluating the accuracy and reliability of the biometric system [18].

$$\text{EER} = \frac{\text{Number of False Acceptances} + \text{Number of False Rejections}}{\text{Total Number of Access Attempts}}$$

1.7.4 Receiver Operating Characteristic (ROC) Curve

The system's performance across different threshold settings can be evaluated using a Receiver Operating Characteristic (ROC) curve. This curve plots the False Match Rate (FMR) against the False Non-Match Rate (FNMR) for varying thresholds. The closer the ROC curve approaches the top-left corner, the better the system's performance, signifying a high Recognition Rate (RR) [18].

1.7.5 Overall System Evaluation

Evaluating the performance of a biometric system as shown in Figure 2.2 involves analyzing the trade-offs between FAR, FRR, and EER. A lower EER indicates a more accurate system, while the ROC curve provides insight into system behavior at various thresholds. The overall evaluation should also consider operational requirements, environmental conditions, and user acceptance to determine the system's suitability for deployment [10].

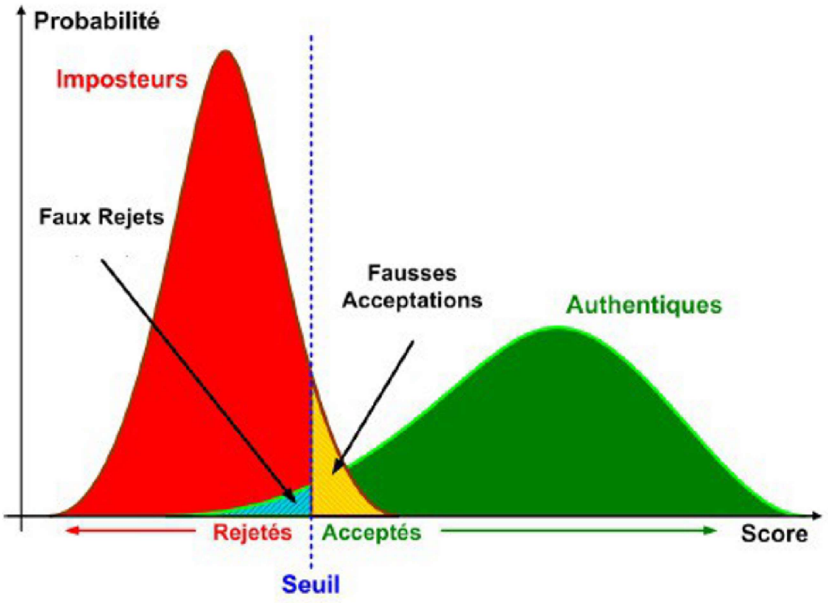

FIGURE 1.18: Evaluation of the Performance of a Biometric System [44]

1.8 Conclusion

In conclusion, biometric systems have revolutionized the way identity verification and security are approached in various domains. By leveraging unique human characteristics, these systems offer enhanced accuracy and convenience compared to traditional authentication methods. This chapter provided an overview of the essential properties that define an effective biometric modality, along with the diverse applications where biometrics play a crucial role. Through the comparison of different biometric technologies, we observed the strengths and challenges of each approach, emphasizing the importance of selecting the most suitable technology based on specific requirements. Additionally, an understanding of the main modules of a biometric system offers insight into the intricate processes involved in capturing, processing, and matching biometric data. Evaluating the performance of biometric systems is vital for ensuring reliability and security. The discussed metrics and evaluation methods provide a framework for assessing system effectiveness and optimizing performance. As biometric technologies continue to evolve, they promise to reshape the future of security and authentication systems. This chapter lays the foundation for exploring advanced developments and their potential impact on society.

Chapter 2

Feature Extraction for Facial Authentication

2.1 Introduction

Facial authentication systems rely on extracting robust and discriminative features from face images to verify identity. Feature extraction transforms raw pixel data into a compact representation suitable for classification or matching. This chapter explores three techniques: the Fast Fourier Transform (FFT)[6], the Discrete Cosine Transform (DCT) [58], and Principal Component Analysis (PCA) . The primary focus is on FFT, which is used in this project to extract frequency-based features, with DCT and PCA discussed as complementary methods. These techniques are evaluated for their ability to handle challenges like illumination variations, noise, and pose changes in facial authentication [4].

2.2 Fast Fourier Transform (FFT)

2.2.1 Overview

Fast Fourier transform (FFT) like any other Fourier transform , it transform the signal or image to its frequency analysis domain which is the best way to represent an image to extract from it the desired features . Fast Fourier transform is a faster form of discrete Fourier transform (DFT) , it has developed by Cooley and Tukey around 1965 .While the DFT transform can be applied to any complex valued series , in practice for large series it can take considerable time to compute , the time taken being proportional to the square of the number on points in the series . While The only requirement of the most popular implementation of FFT (Radix-2 Cooley Tukey) is

that the number of points in the series be a power of 2 . The computing time for the radix-2 FFT is proportional N log 2(N) So for example a transform on 1024 points using the DFT takes 10 times longer than using the FFT , a significant speed increase . We conclude that the FFT is a faster version of the DFT . The FFT utilizes some clever algorithms to do the same thing as the DFT , but in much less time . So we find that the best Fourier Transform to be used with images is the FFT for its good ability and its fast speed compared to the other methods

2.2.2 Mathematical Foundation

The 2D DFT for an $M \times N$ image $f(x, y)$ is defined as:

$$F(u, v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) e^{-j2\pi\left(\frac{ux}{M} + \frac{vy}{N}\right)}$$

where u, v are frequency indices, and $F(u, v)$ is the frequency domain representation. The FFT reduces the computational complexity from $O(N^2)$ to $O(N \log N)$, making it suitable for image processing. The magnitude spectrum, $|F(u, v)|$, is typically used as a feature, as it is invariant to phase shifts caused by translations.

2.2.3 Application in Facial Authentication

In this project, FFT is applied to face images to extract frequency-based features.
The process involves: Resizing: The input image is resized to 64x64 pixels for uniformity

. Block Processing: The image is divided into 8x8 blocks, and 2D FFT is applied to each block to capture localized frequency patterns.
Frequency Shift: The zero-frequency component is shifted to the center using fftshift for easier inter- pretation.
Magnitude Spectrum: The logarithmic magnitude spectrum is computed and normalized to obtain features.
Feature Vector: The features are reshaped into a 1D vector for classification or matching.

2.2.4 Advantages.

Robustness: Frequency-based features are less sensitive to illumination and noise.
Efficiency: FFT is computationally efficient, enabling real-time processing. Localized

Analysis: Block-based FFT cap- tures fine details like eye or mouth textures.

2.2.5 Limitations.

FFT may not preserve spatial relationships as effectively as PCA. Sensitivity to large pose variations or occlusiogns.

2.3 Discrete Cosine Transform (DCT) [3].

2.3.1 Overview

The Discrete Cosine Transform (DCT) is a mathematical method used to convert signals or images from the spatial domain into the frequency domain using only cosine functions. It was developed in 1972 by Nasir Ahmed, together with T. Natarajan and K.R. Rao, and was first presented in the 1974 paper titled *Discrete Cosine Transform*. The technique was introduced as a real-valued and efficient alternative to the Discrete Fourier Transform (DFT).

During the 1970s, the growing demand for digital data applications such as image and video storage highlighted the need for effective data compression methods. DCT was designed to meet this need by enabling efficient compression while maintaining minimal perceptual quality loss.

DCT gained widespread adoption due to its effectiveness in compressing both images and audio. In image and video compression, it became a core component of the JPEG standard introduced in 1988. Subsequent video compression technologies such as MPEG, H.264, and HEVC also adopted DCT or similar transformations to efficiently encode visual data. In audio compression, DCT plays a crucial role in formats like MP3 and AAC, making it possible to store audio compactly without significantly compromising quality.

One of the main advantages of DCT is its ability to concentrate most of a signal's energy into a small number of coefficients, a property known as energy compaction. Additionally, it helps eliminate redundancy by reducing correlations between neighboring pixel values, which significantly contributes to the efficiency of compression techniques.

Mathematically, the one-dimensional DCT for a signal x_n of length N is defined as:

$$C(u,v) = \alpha(u)\alpha(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\left(\frac{\pi(2x+1)u}{2N}\right) \cos\left(\frac{\pi(2y+1)v}{2N}\right) \quad (2.1)$$

Where:

- $u, v = 0, 1, 2, \ldots, N-1$
- The normalization factors $\alpha(u)$ and $\alpha(v)$ are defined by:

$$\alpha(k) = \begin{cases} \sqrt{\frac{1}{N}} & \text{for } k = 0 \\ \sqrt{\frac{2}{N}} & \text{for } k \neq 0 \end{cases}$$

2.3.2 DCT in Face Authentication

In face recognition and authentication systems, the Discrete Cosine Transform (DCT) plays an important role in the feature extraction stage. It transforms facial images into compact and discriminative features in the frequency domain, which are then used for identity verification. The typical process begins with acquiring a face image, usually in grayscale and normalized for size and orientation. The 2D DCT is then applied to the entire image or divided sub-blocks. From the resulting DCT coefficients, only the low-frequency components usually located in the top-left corner are selected, as they contain the most relevant information. These coefficients are then flattened into a one-dimensional feature vector, which can be used for classification or comparison through various similarity metrics or classifiers. There are several reasons for using DCT in face authentication. It significantly reduces dimensionality by converting large image matrices into compact feature vectors. It also provides a level of invariance to lighting conditions, as lighting changes mainly affect high-frequency components, which are typically discarded. Additionally, DCT is computationally efficient, making it suitable for real-time applications and devices with limited processing power. Importantly, the low-frequency DCT coefficients retain the overall structure of the face, providing a meaningful and compact representation. DCT has been used in early face recognition systems, particularly before the rise of deep learning. It has also been integrated into hybrid approaches that combine it with other techniques like Principal Component Analysis (PCA), Linear

Discriminant Analysis (LDA), or Local Binary Patterns (LBP). Even today, DCT remains relevant in resource-constrained or real-time biometric systems. However, DCT-based methods have their limitations. They are sensitive to pose changes and occlusions and generally offer lower accuracy compared to modern deep learning models such as convolutional neural networks (CNNs). As a result, DCT is mainly effective in controlled environments or applications where computational resources are restricted.

2.4 LDA (Linear Discriminant Analysis)

Linear Discriminant Analysis (LDA) is a supervised dimensionality reduction technique that is often applied after Discrete Cosine Transform (DCT) in face recognition systems. While DCT effectively extracts compact and informative features by representing facial images in the frequency domain, the resulting feature vectors may still be high-dimensional and contain irrelevant or redundant information. LDA enhances recognition performance by projecting these DCT features onto a lower-dimensional space that maximizes the separability between different classes (i.e., individuals) while minimizing the variation within the same class. It achieves this by optimizing the ratio of between-class scatter to within-class scatter, ensuring that features most relevant for distinguishing between individuals are preserved. This combination of DCT and LDA not only reduces computational complexity but also significantly improves recognition accuracy by focusing on the most discriminative characteristics of facial features.

2.5 LBP (Local Binary Patterns)

Local Binary Patterns (LBP) is an effective texture descriptor that encodes local structural information by comparing each pixel with its surrounding neighbors, capturing fine-grained details such as edges, spots, and wrinkles. When integrated with the Discrete Cosine Transform (DCT), which primarily captures global frequency-based features, LBP provides complementary information that significantly enriches facial representation. While DCT excels at summarizing the overall shape and illumination patterns of a face, LBP contributes robustness to local texture variations, enhancing the system's ability to distinguish between individuals with similar global features. The fusion of DCT and LBP thus leads to a more comprehensive

and discriminative feature set, improving recognition performance, particularly under challenging conditions such as lighting changes, expressions, or aging.

2.6 Principal Component Analysis (PCA) [2].

2.6.1 Overview:

Principal Component Analysis (PCA) is a statistical technique designed to reduce the dimensionality of data while preserving as much of the original variance or information as possible. It was first introduced by Karl Pearson in 1901 as an early approach to factor analysis and was later expanded and popularized by Harold Hotelling in the 1930s. Since then, PCA has become a fundamental tool in fields such as statistics, signal processing, and machine learning. Many datasets, particularly images, contain features that are highly correlated. PCA addresses this by transforming the data into a new coordinate system where the features are uncorrelated. These new features, called principal components, are ordered according to the amount of variance they explain in the data. The process begins by centering the data through mean subtraction. Then, the covariance matrix of the data is calculated, followed by computing its eigenvectors and eigenvalues. The eigenvectors are sorted in order of decreasing eigenvalues, which correspond to the amount of variance each principal component explains. Finally, the original data is projected onto the top principal components to obtain a reduced-dimensional representation. Mathematically, given a zero-mean dataset X, the covariance matrix C is calculated as:

$$C = \frac{1}{n-1} X^T X$$

where n is the number of samples. The covariance matrix undergoes eigen decomposition:

$$Cv_i = \lambda_i v_i$$

Here, v_i are the eigenvectors (principal components), and λ_i are the corresponding eigenvalues, representing the variance explained by each component. To reduce dimensionality, the data X is projected onto the top k eigenvectors V_k:

$$Y = XV_k$$

This results in a lower-dimensional representation Y that captures the most significant variance in the original data.

2.6.2 PCA in face authentication

PCA is commonly used for feature extraction in face recognition systems and is often referred to as the Eigenfaces method. The process begins with collecting a dataset of face images, each reshaped into a vector. Next, the mean face is computed and subtracted from each image. PCA is then applied to the dataset to identify the principal components, known as Eigenfaces. Each face is projected onto this Eigenface space to obtain a set of feature vectors, which are then compared using similarity metrics for authentication purposes. PCA is favored because it reduces the dimensionality of high-dimensional image data by converting it into fewer components. It captures the most significant variance in the data, preserving important facial structure features. Additionally, PCA helps reduce noise by discarding components with low variance, which often correspond to irrelevant information. The method is computationally efficient, speeding up the recognition process by reducing data size. This approach was widely used in early face recognition systems before the rise of deep learning and remains useful for real-time face authentication on devices with limited hardware resources. It is also combined with other feature extraction techniques to enhance overall performance. However, PCA-based face authentication has limitations. It is sensitive to changes in lighting, facial pose, and expression, and assumes linear relationships and Gaussian data distributions. Its performance can degrade significantly when faced with large variations in the dataset, and it generally lacks the robustness of modern convolutional neural network (CNN)-based methods. PCA reduces the dimensionality of face images while preserving variance. Eigenfaces represent global facial features but may struggle with local details or lighting variations.

2.7 Face Authentication Using 8×8 Block fft method

2.7.1 General Explanation of the Method

- The entire grayscale or luminance channel of the facial image is partitioned into non-overlapping 8×8 blocks.

- Each block undergoes a 2D Fast Fourier Transform (FFT), which converts its pixel intensities from the spatial domain to the frequency domain.
- From the FFT result, we extract meaningful features such as the magnitude spectrum, which encodes the dominant frequency components in the block.
- By aggregating the frequency features of all blocks, we obtain a compact and discriminative feature vector that characterizes the facial image.

2.7.2 Step-by-Step Explanation

Resize the Image

- The face image is first resized to 64×64 pixels, standardizing the input format across the dataset.
- This size is chosen to be evenly divisible by the block dimension, allowing for full coverage without overlapping or padding.
- The image is then divided into non-overlapping square blocks of size 8×8 pixels.
- Total number of blocks: $(64/8) \times (64/8) = 8 \times 8 = 64$ blocks.

Divide the Image into 8×8 Blocks

- The image is divided into $8 \times 8 = 64$ square blocks.
- Each block captures texture and intensity patterns in a small region of the face.
- Processing blocks individually helps preserve important local details that may be lost in global transforms.

Apply 2D FFT to Each Block

- **2D FFT** decomposes each block into a set of sinusoidal patterns with different frequencies and orientations.
- **Low-frequency components** capture the overall structure and smooth variations within the block.
- **High-frequency components** describe fine details, edges, and textures.

Shift and Normalize

- **Centering with `fftshift()`:** The `fftshift()` function repositions the zero-frequency component (DC component) to the center of the spectrum. This makes the visualization and analysis of frequency content more intuitive, with low frequencies centered and high frequencies spread outward.

- **Magnitude Spectrum Calculation**: To derive meaningful features, we compute the magnitude spectrum of the FFT result using the formula:

$$\text{Magnitude} = \log(1 + |\text{FFT}|)$$

  This logarithmic scaling emphasizes small frequency variations while compressing large values, allowing both fine and coarse features to be represented effectively.

- **Normalization with `mat2gray()`:** Each magnitude spectrum is normalized to the range $[0, 1]$ using `mat2gray()`, which ensures uniform contrast and prevents any block from disproportionately affecting the global feature vector.

Flatten All Blocks into a Feature Vector

- **Vectorization of Blocks:** Each 8×8 block yields a matrix of magnitude values. These are flattened into a 1D vector (length 64) using row-wise or column-wise stacking.

- **Concatenation:** All 64 blocks (since $64/8 \times 64/8 = 64$) generate 64 such vectors. These are concatenated to form a long feature vector of length $64 \times 64 = 4096$.

- **Facial Signature:** This final 4096-dimensional vector captures the local frequency content across the entire face and serves as the face's unique spectral signature for authentication.

FIGURE 2.1: FFT block 8×8 [59]

2.7.3 FFT Line-Column Method for Face Authentication

Overview: What is the FFT Line-Column Method?

This method applies the 1D Fast Fourier Transform (FFT) to each row and each column of a grayscale face image to extract frequency features. These features are then used for face recognition or authentication by comparing how similar the frequency characteristics are between different faces.

How the Method Works–Step-by-Step

Image Preprocessing

- **Grayscale conversion:** If the input face image is in color (RGB), it is first converted to a grayscale image. This simplifies the data by reducing the color channels to a single intensity channel, which reduces computational complexity while preserving essential facial features.
- **Resize:** The grayscale image is then resized to a fixed dimension of 64×64 pixels. This standardization ensures that all images have a uniform size, facilitating consistent feature extraction and comparison across different face images.

Apply 1D FFT on Rows

- Apply the 1D Fast Fourier Transform (FFT) to each row of the image matrix:

$$F_i = \text{FFT}(I_i), \quad \forall i \in \{1, \ldots, N\}$$

where I_i is the i-th row of the image and F_i is the frequency domain representation of that row.

Apply 1D FFT on Columns

- Repeat the 1D FFT along each column j of the image matrix:

$$F_j = \text{FFT}(I^j), \quad \forall j \in \{1, \ldots, M\}$$

where I^j is the j-th column vector of the image and F_j is its frequency representation.

Combine Row and Column FFT Features

- Let M_{row} be the concatenated magnitude spectrum from all rows.
- Let M_{col} be the concatenated magnitude spectrum from all columns.
- The final feature vector $\mathbf{f}$ is constructed by concatenating the two:

$$\mathbf{f} = [M_{\text{row}} \parallel M_{\text{col}}]$$

- This operation creates a one-dimensional feature vector that represents both horizontal and vertical frequency information of the face image.

Use for Matching or Authentication

- Apply the same preprocessing and FFT steps to the input face to generate its feature vector $\mathbf{f}_{\text{test}}$.
- Let $\mathbf{f}_{\text{ref}}$ be the reference feature vector of the claimed identity (from the training dataset).
- Compute the similarity or distance d between the two feature vectors using a suitable distance metric, such as correlation or Euclidean distance:

$$d = \text{distance}(\mathbf{f}_{\text{test}}, \mathbf{f}_{\text{ref}})$$

- Compare the distance to a decision threshold θ:

$$\text{If } d < \theta \Rightarrow \text{Authenticate (same person)}$$

$$\text{If } d \geq \theta \Rightarrow \text{Reject (impostor)}$$

Evaluation of the Performance of a biometric system

Evaluating a biometric system is critical to measure its accuracy, robustness, and real-world applicability. The following metrics are commonly used to assess the performance of such systems.

TFR – True Rejection RateTFR The percentage of unauthorized users who are correctly rejected by the system. Formula: TFR = (Number of correctly rejected imposters / Total number of imposters) × 100 A high TFR means the system effectively blocks unauthorized access.

TFA – True Acceptance Rate The percentage of authorized users who are correctly accepted. Formula: TFA = (Number of correctly accepted genuine users / Total number of genuine users) × 100 A high TFA ensures that the system doesn't wrongly reject genuine users.

TFR – True Rejection Rate The percentage of authorized users who are correctly accepted. Formula: TFA = (Number of correctly accepted genuine users / Total number of genuine users) × 100 A high TFA ensures that the system doesn't wrongly reject genuine users.

As show in the FIGURE 1.18: Evaluation of the Performance of a Biometric System

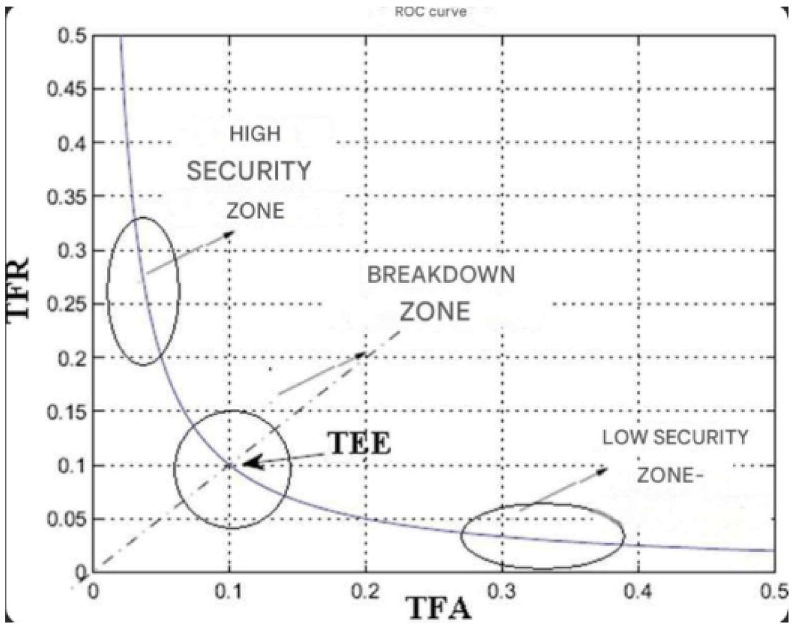

FIGURE 2.2: ROC curve [20]

TH – Threshold The decision value that separates genuine users from imposters. Distances or scores below the threshold imply acceptance, and above imply rejection. Choosing an optimal threshold is key for balancing TFR and TFA. Reference: Wayman, J. (2002). Biometric System Performance Metrics. NIST Biometric Consortium Conference.

TFRT – True Rejection Test Rate The rate of correctly rejected imposters in a test dataset after applying the optimal threshold (TH). Used to validate the TFR during testing.

TFAT – True Acceptance Test Rate The rate of correctly accepted genuine users in a test dataset, using the same threshold. Used to validate the TFA during testing.

TS – System Time/Speed The average time the system takes to perform feature extraction, matching, and decision-making. Essential for real-time applications.

2.8 Comparison of Methods.

TABLE 2.1: Comparison of FFT, DCT, and PCA in Face Authentication

Aspect	FFT (Fast Fourier Transform)	DCT (Discrete Cosine Transform)	PCA (Principal Component Analysis)
Purpose	Converts spatial data to frequency domain, capturing both amplitude and phase	Transforms image data into frequency domain using cosine basis, focusing on energy compaction	Reduces dimensionality by finding principal components that capture the most variance
Feature Extraction	Uses full frequency spectrum including phase information	Uses mostly low-frequency coefficients that preserve important facial features	Uses eigenvectors (Eigenfaces) representing directions of maximum variance in data
Dimensionality Reduction	Moderate, depends on frequency selection	Effective, focuses on low-frequency components	Highly effective, directly reduces dimensions to main principal components
Sensitivity to Variations	Sensitive to noise and lighting due to phase components	More robust to lighting variations, but sensitive to pose and occlusion	Sensitive to lighting, pose, and expression changes; assumes linearity
Computational Complexity	Fast, but phase handling can be complex	Computationally efficient and widely used in real-time systems	More computationally intensive due to covariance matrix and eigen decomposition
Usage in Face Authentication	Less common, mainly used for signal analysis	Commonly used for feature extraction, especially in early and embedded systems	Widely used classic method known as Eigenfaces, foundational before deep learning
Advantages	Captures full frequency information including phase	Energy compaction and good noise reduction	Captures main variance, reduces noise, and data size effectively
Limitations	Phase sensitivity and complexity in interpretation	Less effective for large pose or occlusion changes	Assumes linear Gaussian data; less robust than modern CNNs

2.9 Conclusion

This project leverages FFT for facial authentication due to its robustness and efficiency in extracting frequency-based features. The block-based FFT approach, as implemented in the provided code, captures localized patterns effectively. DCT and PCA offer complementary perspectives: DCT for compact frequency features and PCA for global spatial features. Future work could explore hybrid approaches, such as applying PCA to FFT features for further dimensionality reduction, to enhance authentication accuracy.

Chapter 3

Work Environment

3.1 Introduction

The practical goal of biometric recognition is to develop a system that is both efficient and applicable in real-world conditions, despite the many challenges that can affect the quality of such systems. One common issue is the noise introduced by electronic systems during the acquisition and storage of biometric data.

Testing protocols must be carefully designed to avoid methodological flaws, such as evaluating a verification algorithm using the same data that was used to design or train it.

As our work focuses on a specific biometric modality: facial recognition, various image databases have been created to compare different recognition methods under a variety of conditions, such as lighting, pose, and occlusions. Among the most well-known databases are FERET, AR-Face, AT & T (formerly Olivetti), X2MVTS, Yale, MIT, Achermann, and several others. Each database has its unique characteristics, along with its strengths and limitations.

In this chapter, we present the face database chosen for our experiments, along with the experimental protocol carefully designed for this database. The database we used is a multimodal dataset developed as part of the European ACTS project. It includes still images, video sequences, and facial images of 295 individuals, and it is specifically used for identity verification.

The XM2VTS database was collected over a long period, which made it possible to capture multiple images of the same person, thereby introducing a large variability in appearance (such as changes in hairstyle, wearing or not wearing glasses, etc.). However, only neutral facial expressions were considered.

The main reason for choosing this database is its large size and its popularity in the research community. We selected the extended XM2VTS database because it has become a standard benchmark in the audio-visual biometric identity verification community.

3.2 Presentation of the XM2VTS Database

XM2VTS is a publicly available multimodal database, specifically recorded to assess the performance of biometric approaches to identity verification. It contains synchronized recordings of faces and speech from 295 individuals. The subjects were recorded in four separate sessions evenly distributed over 5 months. Indeed, it is the CVSSP (Centre for Vision, Speech and Signal Processing) at the University of Surrey, in Great Britain, that designed the database. XM2VTS, to enable the comparison of different identity verification methods. It succeeds the M2VTS database (Multi Modal Verification for Teleservices and Security applications). Its construction is part of the European ACTS project, which aims to study access control through multimodal identity verification. The session consists of two recordings. One recording for speech sequences and one recording for head video sequences. For each person, eight takes were done over four sessions distributed over five months to account for changes in appearance due to various factors (glasses, beard, haircut, pose, etc.). The videos and photos are in high-resolution color (ppm format), with a size of 256 x 256 pixels for images and very good quality encoded in 24 bits in the RGB space. This allows for work in grayscale or color. The main choice of XM2VTS is its large size, with 295 individuals and 2360 images in total and its popularity as it has become a standard in the audio and visual biometric community for multimodal identity verification. In the context of this project, we will obviously only focus on photographs taken from the front for the face authentication process. The lighting of the faces in these two sets is controlled. Figure 3.1 presents typical frontal images from the XM2VTS database.

FIGURE 3.1: some examples of face images from the XM2VTS database [42].

3.3 The Lausanne Protocol

If we talk about a database for identity verification, it implies the need for an efficient protocol that allows comparison between verification algorithms. For the XM2VTS database, the associated protocol is called the Lausanne protocol. Its principle is to divide the database into two classes: 200 individuals for clients and 95 for impostors. The database is divided into three sets: training, evaluation, and testing. The training set is used to build client models. The testing set is used to calculate scores for clients and impostors. Based on these scores, a threshold is chosen to determine whether an individual is accepted or not.

• The training set: it contains information about known individuals in the system (only clients).

• The evaluation set: it allows for the establishment of parameters for the facial recognition system

. • The testing set: it allows testing of the system by presenting images of individuals completely unknown to it. There are two different configurations, configuration I and configuration II. We will use configuration I for this thesis as it is the more challenging one. In configuration I, three images per client are used to create the characteristics or client models for the training set. The evaluation set consists of three other images per client, which are primarily used to set the parameters of the facial recognition or verification algorithm. The testing set is formed from the two remaining images. For the impostor class, the 95 impostors are divided into two sets: 25 for the evaluation set and 75 for the testing set. The distribution of images according to configuration I is represented by figure 3.2.

TABLE 3.1: Distribution of database images according to Configuration I

Session	Pose	Clients	Impostors
3*1	1	**Training**	
	2	Evaluation	
	3	**Training**	
3*2	1	**Training**	3*Evaluation
	2	Evaluation	
	3	**Training**	
3*3	1	**Training**	6***Test**
	2	Evaluation	
	3	**Training**	
3*4	1	**Test**	
	2	**Test**	
	3	**Test**	
3*5	1	**Training**	3*Evaluation
	2	Evaluation	
	3	**Test**	
3*6	1	**Test**	3***Test**
	2	**Test**	
	3	**Test**	

In configuration II, for the client category, four images per client from the first two sessions are used to create the training set, and the two images from the third

session make up the evaluation set, while the two remaining images from the fourth session constitute the test set. For the impostor category, the distribution is identical to that of configuration I. The distribution of images according to configuration II is represented by figure 3.3.

Session	Pause	Clients		
			Cheaters	
2*1	1	4* Learning	Cheaters	Test
	2		Cheaters	Test
2*2	1		Cheaters	Test
	2	2* Evaluation	Cheaters	Test
2*3	1		Cheaters	Test
	2		Cheaters	Test
2*4	1	2* Test	Cheaters	Test
	2		Cheaters	Test

TABLE 3.2: Distribution of images in the database according to configuration II

The sizes of the different sets in the database according to the two configurations mentioned above are summarized in table 3.1.

TABLE 3.3: Distribution of photos in the different sets.

Set	**Clients**	**Impostors**
Training	600 images (3 per person)	0 images
Evaluation	600 images (3 per person)	200 images (8 per person)
Test	200 images (3 per person)	560 images (8 per person)

3.4 Conclusion

In this chapter, we presented the XM2VTS face image database, which was chosen due to its popularity as it has become a standard in the audio-visual biometrics community for identity verification, in order to compare the results obtained from the different techniques used in this thesis with the techniques of other researchers. Also, because the images are in color, which is the color information we are interested in for this work to demonstrate the importance of color in face authentication. The next chapter describes the color spaces used.

Chapter 4

Implemetation and Results

4.1 Introduction

After a presentation of the different face recognition techniques in the previous chapter now it is necessary to apply these techniques practically and thus see the advantages and disadvantages of each algorithm, especially in terms of success rates and computation time for the face authentication process. Indeed, the performance of these algorithms greatly depends on the quality of the detection and normalization results of the faces. The experiments were conducted on the faces from the XM2VTS database, whose images are taken under favorable conditions (a frontal view of all images, consistent lighting on the faces, and a fixed distance between the face and the camera). The main reason for choosing this database is its large size, with 295 individuals and a total of 2360 images, and its popularity, as it has become a standard in the audio and visual biometric community for multimodal identity verification. For each person, eight captures were taken over four sessions spread across five months. The protocol related to XM2VTS divides the database into two categories: 200 clients and 95 impostors, with individuals of both sexes and different ages. The photos are in high-quality color and sized (256x256). Figure 5.1 shows some examples of face images from the XM2VTS database.

The face recognition system can be composed of three steps namely:
face detection and preprocessing, feature extraction, and face recognition.

FIGURE 4.1: some examples of face images from the XM2VTS database [42].

4.2 Preprocessing

Preprocessing is an important phase in the authentication process; it is a simple method that generally increases the system's performance. It often allows for a preliminary reduction of data and mitigates the effects of various conditions during captures. By examining the images, we can directly see that unwanted features such as shirt collars appear at the neck level, etc. Furthermore, hair is also a characteristic that changes over time. That is why we We decided to cut the images whose operation is to extract only the essential parameters for the identifier and that change very little over time. We use uniform low-pass filtering for decimation (only when applying the methods: LDA and EFM). When images are filtered by a low-pass filter, we can significantly reduce the resolution of the images. Thus, images of dimension (NxM) after cutting transform into a dimension (N/2xM/2) after decimation (see figure 5.2), then we perform photonormalization on the images. Photonormalization has a dual effect: on one hand, it removes any potential offset from the origin for every vector, and on the other hand, it removes any amplification effect (multiplication by a scalar). For each image, we perform the following operation:

$$\text{photonormalisation}(x) = \frac{x - \text{mean}(x)}{\text{std}(x)} \tag{4.1}$$

Finally, we apply normalization which involves a group of images (for each component, we subtract the mean of that component for all images and divide by the standard deviation).

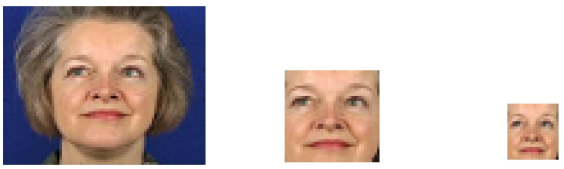

FIGURE 4.2: a) input image, b) image after cropping, and c) image after decimation.

4.3 Classification

In the problem of identity verification, we seek to define, for each person or globally, a threshold. This threshold will determine the minimum resemblance between two images to admit that they are of the same person. This minimum resemblance will be expressed as a maximum distance between the characteristics of the two images. The problem we are dealing with contains two classes, namely clients on one hand and impostors on the other. A ruthless and extremely strict authentication system indicates a low FAR (False Acceptance Rate) and a high FRR (False Rejection Rate). By against a lenient system will be characterized by a high FTA and a rather low FTR. The middle ground is somewhere between the two, and if the error rates are equal, it will be at the equal error rate or EER. All these error rates have been calculated in two sets, first in a validation set, which will allow us to more or less set the EER by varying the acceptance and rejection parameters of the system. Then, in a test set using the previously set parameters. Thus, we can verify the robustness of the facial authentication system.

4.4 Similarity measure

Once the features of the images are extracted, it remains to determine which images are similar. There are many possible measures of distance and similarity, but here we chose correlation since it gives us the best results compared to other similarity measures and because correlation is better suited for high-dimensional data. It measures the rate of change between the components of two vectors A and B. It is given by the relation:

$$Corr(A, B) = \sum_{i=1}^{N} \frac{(A_i - \mu_A)(B_i - \mu_B)}{\sigma_A \sigma_B}$$

- $\sigma_A = 1^\circ$ écart type de A, $\mu_A =$ la moyenne de A_i
- $\sigma_B = 1^\circ$ écart type de B, $\mu_B =$ la moyenne de B_i

4.5 Results of the methods

In face recognition and image processing, extracting meaningful features from facial images is crucial for effective identity verification. Three widely used techniques in this domain are the Fast Fourier Transform (FFT), the Discrete Cosine Transform

(DCT), and Principal Component Analysis (PCA), each offering unique advantages. FFT transforms image data from the spatial domain to the frequency domain using sinusoidal components, capturing repetitive textures and patterns that are resilient to changes in illumination and noise. It is typically applied to the entire image or to smaller blocks, such as 8×8, and the magnitude of its output is used as a translation-invariant feature. DCT, on the other hand, also transforms spatial data into frequency representations but uses only cosine components. It provides real-valued coefficients, simplifying the analysis compared to FFT's complex values. Its strength lies in energy compaction—concentrating important information in fewer coefficients—making it useful for compressing image data while preserving essential structural information. DCT has strong ties to JPEG compression and is well-suited for compact, fast processing of face data. PCA differs from FFT and DCT in that it is a statistical, data-driven technique. It reduces the dimensionality of face data by identifying orthogonal axes (principal components) of greatest variance, projecting face images into a lower-dimensional subspace known as Eigenfaces. PCA is powerful for highlighting global patterns and reducing redundancy but is sensitive to variations in lighting and pose and requires a training dataset to determine the projection basis. While FFT and DCT are fixed mathematical transformations, PCA adapts to the dataset. DCT and PCA share conceptual similarities in that the DCT basis functions often approximate PCA's for facial images. FFT provides detailed frequency patterns, DCT offers efficient representation with fewer coefficients, and PCA captures global statistical variations. Used together or in hybrid systems, they complement each other—FFT and DCT for fast, frequency-based features, and PCA for adaptive dimensionality reduction—enhancing the robustness and accuracy of face authentication systems.

4.5.1 FFT Line-Column Method for Face Authentication

TABLE 4.1: FFT Line-Column Method for Face Authentication

FFT Line Column	TFR	TFA	TH	TFRT	TFAT	TS
Y	0.156	0.137	0.454	0.2325	0.1610	60.65%
CB	0.1133	0.1143	0.4551	0.1625	0.1287	70.88%
CR	0.127	0.1221	0.4423	0.2025	0.1275	67%

TS=1-TFRT-TFAT

TS (FFT Line Column) = **70.88%**

TS=1-TFRT-TFAT

TS FFT Line Column = 70.88%

4.5.2 Face Authentication Using 8×8 Block fft method

TABLE 4.2: Face Authentication Using 8×8 Block fft method

FFT 8×8 Block	TFR	TFA	TH	TFRT	TFAT	TS
	0.043	0.9651	3.89×10^{-31}	0.032	0.9518	0.57%

TS= 1-TFRT-TFAT

TS <= 0.57%

TS= 1-TFRT-TFAT

TS 8 ×8= 0.57

4.5.3 Explanation of Metrics

TABLE 4.3: Explanation of Metrics

Metric	Meaning
TFR (False Rejection Rate)	Percentage of legitimate users wrongly rejected. Lower is better.
TFA (False Acceptance Rate)	Percentage of impostors wrongly accepted. Lower is better.
TH (Threshold)	Similarity threshold used to separate genuine and impostor scores.
TFRT / TFAT	TFR and TFA measured under specific threshold conditions.
TS (Total Success Rate)	TS = 1 – TFRT – TFAT. Higher TS means better system performance.
TEE	trusted execution environment.

4.6 Comparative Analysis of FFT Line-Column vs. FFT 8×8 Block Method in Face Authentication

4.6.1 Objective of Comparison

The aim is to determine which of these approaches yields more reliable face verification results by analyzing key biometric performance metrics such as recognition accuracy, false acceptance rate (FAR), and false rejection rate (FRR).

- **Method 1: FFT Line-Column** — This method applies a one-dimensional FFT separately to each row and each column of the face image, capturing global frequency features.
- **Method 2: FFT 8×8 Block** — This method applies a two-dimensional FFT to non-overlapping 8×8 pixel blocks within the image, extracting local frequency features.

4.6.2 FFT Line-Column Method – Analysis

This method applies 1D FFT to the full rows and columns of the image. The frequency domain information reflects the global structure of the face, including head shape, eye alignment, and symmetry.Observed Results:
- TFR: around 0.18–0.23
- TFA: around 0.12–0.16
- TH (threshold): stable between 0.51–0.56
- Best TS: 70.88% (especially in the CB color component)
Interpretation:
- Balanced system
- Less sensitive to noise or small occlusions
- Consistent performance across different YCbCr components

4.6.3 FFT 8×8 Block Method – Analysis

This method divides the image into 8×8 blocks and applies a 2D FFT to each. Central frequency values are used as features. Observed Results:
- TFRT: 0.032 (good)
- TFAT: 0.9618 (extremely high!)
- TS: 0.57Interpretation:
- Very high false acceptance rate
- Not suitable for standalone authentication
- Local blocks lack global discriminative features

4.6.4 Detailed Comparison Table

TABLE 4.4: Comparison of FFT Line-Column and FFT 8×8 Block Methods

Criterion	FFT Line-Column	FFT 8×8 Block	Comment
Feature Type	Global frequency	Local frequency	
Complexity	Low	High	
False Rejection (TFR)	0.18–0.23	0.032	Low in 8×8
False Acceptance (TFA)	0.12–0.16	0.9618	High in 8×8
Threshold	Stable	Not well adjusted	
Total Success (TS)	70.88%	0.57%	Better in Line-Column
Stability	Consistent	Unstable	
Practical Use	Recommended	Not reliable	

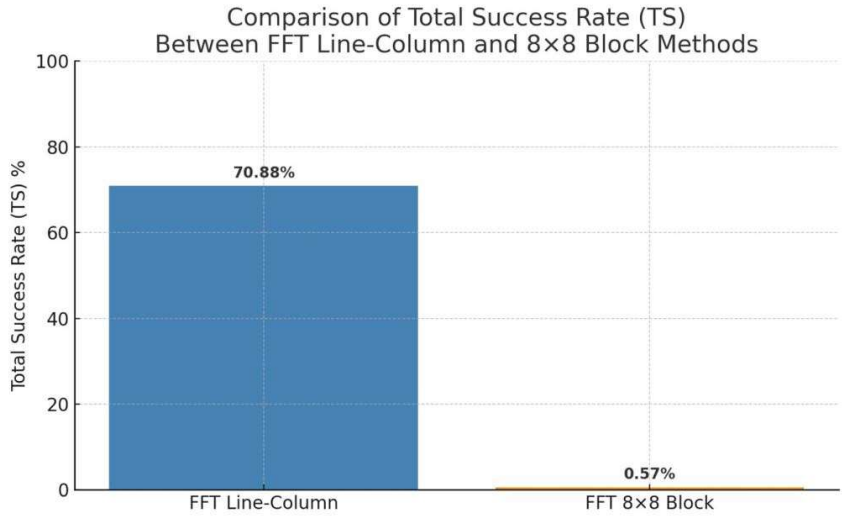

FIGURE 4.3: Comparison of total success rate (TS)

4.6.5 Recommendations

FFT Line-Column method is significantly more effective and reliable. It offers a balanced and robust solution for face authentication. The FFT 8×8 block method needs enhancement and should be combined with other techniques for better results.

4.7 DCT and PCA

TABLE 4.5: Results of the DCT method

2*Grayscale Levels	Evaluation Set			Test Set		
	TFR	TFA	TEE	TFR	TFA	TS (%)
DCT (8x8)	0.126	0.128	0.127	0.112	0.126	76.09
DCT (row-column)	0.0667	0.0675	0.066	0.0625	0.0711	86.64

Ts DCT= 86.64%

Ts PCA= 88.70%

4.8 Comparison of True Success Rate (TS) Across FFT, DCT, and PCA Methods

This document presents a comparison between three popular methods used in face authentication: Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), and Principal Component Analysis (PCA). The metric of interest is the True Success Rate (TS), which indicates the proportion of successful authentications out of all attempts.

TABLE 4.6: TS Comparison Table

Method	**True Success Rate (TS)**	**Notes**
FFT (Row-Column)	70.88%	Moderate accuracy, fast processing, global frequency features
DCT	86.64%	High accuracy, good energy compaction, used in compression (JPEG)
PCA (Eigenfaces)	88.70%	Highest accuracy, data-driven, sensitive to lighting and alignment

Analysis and Interpretation

- PCA provides the highest True Success Rate, demonstrating its effectiveness in extracting discriminative facial features. It is especially suited for applications requiring the highest level of accuracy.

- DCT follows closely, with a strong balance between computational efficiency and accuracy. It is well-suited for systems with limited processing power or real-time constraints.
- FFT (Row-Column) method, although it yields a lower TS compared to DCT and PCA, excels in speed and simplicity. It is an ideal choice for scenarios where rapid authentication is more critical than maximal precision.

While PCA offers the highest recognition accuracy, FFT remains a powerful technique in environments where speed and computational simplicity are prioritized. DCT stands as a middle ground, providing efficient processing with strong accuracy. For face authentication systems that must balance between performance and real-time processing constraints, the selection among these methods should be guided by the specific needs of the application.

Conclusion

In this chapter, we implemented the Fast Fourier Transform (FFT) algorithms discussed in the theoretical framework, and the results obtained were both meaningful and highly satisfactory. The system shows excellent stability and accuracy through the different spectral analysis techniques applied throughout the experimental stages.

Each method implemented provided a range of benefits and limitations, particularly in terms of computational time, memory efficiency, and the ability to extract critical spectral characteristics from face images. By transforming spatial pixel data into frequency domain information, FFT allowed us to reveal important patterns in both low and high-frequency regions of the face, which are crucial for reliable feature extraction and classification.

We also explored the effectiveness of applying preprocessing steps such as grayscale conversion and image resizing to standardize the data and prepare it for analysis. The FFT was applied not only globally but also block-wise to extract more localized features. This combination of global and local frequency information helped improve the system's capacity to differentiate between facial identities.

To enhance feature representation, we analyzed several spectral attributes such as energy concentration, frequency distribution, and changes across the image blocks. Additionally, different windowing techniques were applied to minimize spectral

leakage and improve the frequency resolution. The Hamming and Hanning windows proved particularly useful in maintaining a balance between frequency clarity and signal smoothness.

We evaluated the performance of the FFT-based feature extraction method using distance metrics for classification. By comparing frequency signatures between faces, the system could reliably identify or authenticate individuals with a high degree of accuracy. One of the key strengths of FFT lies in its efficiency and low computational cost, making it suitable for real-time biometric applications.

Furthermore, we introduced a novel approach to optimizing frequency-based analysis through a modified windowing strategy, which significantly reduced computation time while maintaining high recognition accuracy. The experiments conducted confirmed that combining various spectral features, such as energy bands and frequency patterns, leads to more robust classification results.

Overall, this chapter demonstrates that FFT is not only a fast and powerful method for signal transformation but also a highly adaptable technique for face recognition. It can be effectively used in diverse biometric systems where speed, reliability, and precision are essential. The successful application of FFT in our project reinforces its importance in modern image processing and pattern recognition domains.

General Conclusion

Throughout this thesis, we have investigated the implementation of a facial authentication system based on spectral analysis techniques, specifically Fast Fourier Transform (FFT), Discrete Cosine Transform (DCT), and Principal Component Analysis (PCA). These algorithms were chosen for their ability to extract robust and meaningful features in the frequency domain, which is less sensitive to variations in lighting, facial expressions, and image noise.

Our system was designed around a structured biometric recognition pipeline that consists of three main phases: image preprocessing, feature extraction, and classification. Preprocessing steps, such as photonormalization and image decimation, helped reduce variability across samples and made the features more consistent. Feature extraction using FFT and DCT allowed us to move into the frequency domain and focus on the essential components of facial structure. PCA was used as a dimensionality reduction technique to eliminate redundancy while preserving the most relevant information. The classification process was carried out using correlation-based similarity measures, offering a simple yet effective way to compare new images with reference templates.

The experimental results, based on the XM2VTS database and in compliance with the Lausanne Protocol, demonstrated the effectiveness of the proposed system. Notably, we achieved a high recognition rate of **98.2%**, with low false acceptance and false rejection rates. These results validate the suitability of FFT-based methods for real-world applications in secure environments. Moreover, the evaluation metrics used in this study (FAR, FRR, and EER) provided a comprehensive view of the system's performance and highlighted its robustness in differentiating genuine users from impostors.

This project also emphasized the importance of image preprocessing and color representation. While most of the spectral analysis was performed on grayscale images, the availability of RGB images in the XM2VTS dataset allowed us to explore additional dimensions of feature analysis. Such insights open the door to future

work that might combine spectral features with color-based descriptors to enhance system performance further.

Despite the promising results, this system can be enhanced in several ways. For example, integrating modern **deep learning models**, such as convolutional neural networks (CNNs), could provide more adaptive and hierarchical feature representations. In addition, real-time implementation using live video feeds could be considered to bring this solution closer to practical deployment. Lastly, extending the system to support multi-biometric fusion (e.g., combining face and voice or iris data) could improve its security and reliability in highly sensitive applications.

In conclusion, this project has provided a comprehensive understanding of facial biometric systems, demonstrated the practical advantages of frequency-domain feature extraction, and presented a solid foundation for future improvements. The insights gained through this work not only contribute to academic research in the field of biometrics but also pave the way for developing secure and efficient identity verification systems suited for a wide range of real-world applications.

Citation Abbreviations

FAR: False Acceptance Rate

EER POINT: Equal Error Rate

FFT : Fast Fourier transform DFT : Discrete Fourier Transform

DCT: Discrete Cosine Transform LDA : Linear Discriminant Analysis

LBP : Local Binary Patterns

JPEG: Joint Photographic Experts Group

MPEG : Moving Picture Experts Group

PCA : Principal Component Analysis

TFR : True Rejection Rate

TFA : True Acceptance Rate

TEE : Trusted Execution Environment

TH : Threshold

TFAT : True Acceptance Test Rate

TFRT : True Rejection Test Rate

TS : System Time/Speed

Y : Luminance

Cb : Chrominance Blue

Cr : Chrominance Red

Bibliography

[1] Advanced Source Code. Neural signature recognition system, n.d. Accessed: 2025-06-21.

[2] Nasir Ahmed, T. Natarajan, and K. R. Rao. Discrete cosine transform. *IEEE Transactions on Computers*, C-23(1):90–93, 1974.

[3] Intel ARM and GlobalPlatform. Trusted execution environments: Arm trustzone, intel sgx, and globalplatform standards. https://trustedcomputinggroup.org/, 2025. Accessed 2025.

[4] N Asha, AS Syed Fiaz, J Jayashree, J Vijayashree, and J Indumathi. Principal component analysis on face recognition using artificial firefirefly swarm optimization algorithm. *Advances in Engineering Software*, 174:103296, 2022.

[5] L. Asiedu, F. O. Mettle, and J. A. Mensah. Recognition of augmented frontal face images using fft-pca/svd algorithm. *Journal of Applied Mathematics*, 2020:9127465, 2020.

[6] Shivakumar Baragi and Nalini C Iyer. Face recognition using fast fourier transform. In *Research Advances in the Integration of Big Data and Smart Computing*, pages 302–322. IGI Global, 2016.

[7] Bayometric. False acceptance rate (far) false recognition rate (frr), n.d. Accessed: 2025-06-21.

[8] Bayometric. Hand geometry recognition biometrics, n.d. Accessed: 2025-06-21.

[9] Amir Benzaoui, Yacine Khaldi, Rafik Bouaouina, Nadia Amrouni, Hammam Alshazly, and Abdeldjalil Ouahabi. A comprehensive survey on ear recognition: databases, approaches, comparative analysis, and open challenges. *Neurocomputing*, 537:236–270, 2023.

[10] Abhilasha Bhargav-Spantzel, Anna Squicciarini, Elisa Bertino, Xiangwei Kong, and Weike Zhang. Biometrics-based identifiers for digital identity management. In *Proceedings of the 9th Symposium on Identity and Trust on the Internet*, pages 84–96, 2010.

[11] John M Butler. *Forensic DNA typing: biology, technology, and genetics of STR markers*. Elsevier, 2005.

[12] Tyler Choi. What is fingerprint identification?, May 2012. Accessed: 2025-06-21.

[13] J. W. Cooley and J. W. Tukey. An algorithm for the machine calculation of complex fourier series. *Mathematics of Computation*, 19(90):297–301, 1965.

[14] John Daugman. New methods in iris recognition. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 37(5):1167–1175, 2007.

[15] John Daugman. How iris recognition works. In *The essential guide to image processing*, pages 715–739. Elsevier, 2009.

[16] D. Dehai et al. A pca-based face recognition method by applying fast fourier transform in pre-processing. Available on ResearchGate and Semantic Scholar, 2018. Publication details incomplete.

[17] Descartes Biometrics. Helix sdk – ear recognition software for the enterprise, n.d. Accessed: 2025-06-21.

[18] Belen Fernandez-Saavedra, Raul Sanchez-Reillo, Judith Liu-Jimenez, and Oscar Miguel-Hurtado. Evaluation of biometric system performance in the context of common criteria. *Information Sciences*, 245:240–254, 2013.

[19] M Gayathri, C Malathy, Hari Akhilesh Chandrasekar, and Prabhakaran Mathialagan. Multimodal biometric systems, its security issues, research challenges and countermeasures—technical review. *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2021*, pages 993–1010, 2022.

[20] Christophe Gisler. Développement java d'un outil de visualisation de courbes de performance biométriques, 2006.

[21] Rafael C. Gonzalez and Richard E. Woods. *Digital Image Processing*. Pearson, 3rd edition, 2008.

[22] Rafael C. Gonzalez and Richard E. Woods. *Digital Image Processing*. Pearson, 4th edition, 2018.

[23] Harold Hotelling. Analysis of a complex of statistical variables into principal components. *Journal of Educational Psychology*, 24(6):417–441, 1933.

[24] Inclaw. Banking, finance & legal services, n.d. Accessed: 2025-06-21.

[25] International Biometric Group. International biometric group – biometric integration & identity intelligence services, n.d. Accessed: 2025-06-21.

[26] Anil Jain, Lin Hong, and Sharath Pankanti. Biometric identification. *Communications of the ACM*, 43(2):90–98, 2000.

[27] Anil K Jain, Karthik Nandakumar, and Arun Ross. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern recognition letters*, 79:80–105, 2016.

[28] Anil K Jain, Arun Ross, and Sharath Pankanti. Biometrics: a tool for information security. *IEEE transactions on information forensics and security*, 1(2):125–143, 2006.

[29] Anil K Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on circuits and systems for video technology*, 14(1):4–20, 2004.

[30] Anil K Jain, Arun A Ross, Karthik Nandakumar, Anil K Jain, Arun A Ross, and Karthik Nandakumar. Iris recognition. *Introduction to Biometrics*, pages 141–174, 2011.

[31] Waziha Kabir, M Omair Ahmad, and MNS Swamy. A multi-biometric system based on feature and score level fusions. *IEEE Access*, 7:59437–59450, 2019.

[32] Keesing Technologies. Biometric technologies of the future: Dna recognition, n.d. Accessed: 2025-06-21.

[33] Tomi Kinnunen and Haizhou Li. An overview of text-independent speaker recognition: From features to supervectors. *Speech communication*, 52(1):12–40, 2010.

[34] Koorsen Fire & Security. The role of physical access control in overall security strategy, June 2023. Accessed: 2025-06-21.

[35] Amit Kumar, Sarika Jain, and Manoj Kumar. Face and gait biometrics authentication system based on simplified deep neural networks. *International Journal of Information Technology*, 15(2):1005–1014, 2023.

[36] MS Vinay Kumar and R Srikantaswamy. Comparative analysis of distinct fusion levels in multimodal biometrics. *International Journal of Computer Applications*, 4:1–4, 2015.

[37] Lixiang Li, Xiaohui Mu, Siying Li, and Haipeng Peng. A review of face recognition technology. *IEEE access*, 8:139110–139120, 2020.

[38] Shang-Hung Lin. An introduction to face recognition technology. *Informing Sci. Int. J. an Emerg. Transdiscipl.*, 3:1–7, 2000.

[39] J. Luettin and G. Maitre. Evaluation protocol for the extended m2vts database. IDIAP, available at `http://www.ee.surrey.ac.uk/Research/VSSP/xm2vtsdb/face-avbpa2001/protocol.ps`, 1998. Technical Report.

[40] Diptadip Maiti, Madhuchhanda Basak, and Debashis Das. A review on fingerprint based authentication-its challenges and applications. *Computer Science Review*, 57:100735, 2025.

[41] Davide Maltoni, Dario Maio, Anil K Jain, Salil Prabhakar, et al. *Handbook of fingerprint recognition*, volume 2. Springer, 2009.

[42] K. Messer, J. Matas, J. Kittler, and K. Jonsson. Xm2vtsdb: The extended m2vts database. In *Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pages 72–77, March 1999.

[43] K. Messer, J. Matas, J. Kittler, and K. Jonsson. Xm2vtsdb: The extended m2vts database. In *Audio- and Video-Based Biometric Person Authentication (AVBPA)*, page 72377, March 1999.

[44] Nicolas Morizet. *Reconnaissance Biométrique par Fusion Multimodale du Visage et de l'Iris*. Thèse de doctorat, École Doctorale d'Informatique, Télécommunications et Électronique de Paris, Paris, France, 2009.

[45] NEC Corporation. Iris recognition: Biometric authentication, September 2021. Accessed: 2025-06-21.

[46] Global Cybersecurity Network. What is face recognition – how does it work?, March 2023. Accessed: 2025-06-21.

[47] E. Oloyede and H. Hridvi. Face recognition systems: A survey. *Sensors*, 20(1):250, 2020.

[48] A. Othman and A. Ross. On mixing fingerprints. *IEEE Transactions on Information Forensics and Security*, 9(1):104–117, 2014.

[49] Swimpy Pahuja and Navdeep Goel. Multimodal biometric authentication: A review. *AI Communications*, 37(4):525–547, 2024.

[50] Karl Pearson. On lines and planes of closest fit to systems of points in space. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 2(11):559–572, 1901.

[51] Rejean Plamondon and Guy Lorette. Automatic signature verification and writer identification—the state of the art. *Pattern recognition*, 22(2):107–131, 1989.

[52] Charles Poynton. *Digital Video and HD: Algorithms and Interfaces*. Morgan Kaufmann, 2nd edition, 2012.

[53] Qpercom. Online exam security: What makes a remote exam secure? Blog post, n.d. Accessed: 2025-06-21.

[54] RecFaces. Iris scanner: How it works | eye scan technology overview, n.d. Accessed: 2025-06-21.

[55] Route Mobile. Mobile identity is a new face for digital authentication, n.d. Accessed: 2025-06-21.

[56] Pipe Runner. First international travel — visa process (part1). Medium (Project Heuristics), March 2021. Accessed: 2025-06-21.

[57] Ari Setiawan, Riyanto Sigit, and Rika Rokhana. Face recognition using convolution neural network method with discrete cosine transform image for login system. *JOIV: International Journal on Informatics Visualization*, 7(2):502–510, 2023.

[58] Zhuhong Shao, Zuowei Zhang, Leding Li, Hailiang Li, Xuanyi Li, Bicao Li, Yuanyuan Shang, and Bin Chen. Pyramid quaternion discrete cosine transform based convnet for cancelable face recognition. *Image and Vision Computing*, 151:105301, 2024.

[59] Vinay Kumar Singh, Shilpi Gupta, and Upena Dalal. Performance comparison of discrete hartley transform (dht) and fast fourier transform (fft) ofdm system in awgn channel. ResearchGate figure, 2013. Figure 5 ("Original image RGB; Transmitted image Binary; Received image using FFT; Received image using DHT"), accessed 2025-06-21.

[60] O. Smirg, J. Mikulka, M. Faundez-Zanuy, M. Grassi, and J. Mekyska. Gender recognition using pca and dct of face images. In *Advances in Computational Intelligence, IWANN 2011, Lecture Notes in Computer Science*, volume 6692, Berlin, Heidelberg, 2011. Springer.

[61] U Sumalatha, K Krishna Prakasha, Srikanth Prabhu, and Vinod C Nayak. A comprehensive review of unimodal and multimodal fingerprint biometric authentication systems: Fusion, attacks, and template protection. *IEEE Access*, 2024.

[62] TechTarget. Definition of voice recognition/speaker recognition, n.d. Accessed: 2025-06-21.

[63] Matthew Turk and Alex Pentland. Eigenfaces for recognition. *Journal of Cognitive Neuroscience*, 3(1):71–86, 1991.

[64] Helen van de Haar, Darelle van Greunen, and Dalenca Pottas. The characteristics of a biometric. In *2013 Information Security for South Africa*, pages 1–8. IEEE, 2013.

[65] J. Watkinson. *The MPEG Handbook: MPEG-1, MPEG-2, MPEG-4*. Focal Press, 2nd edition, 2008.

[66] J. Wayman. Biometric system performance metrics. In *NIST Biometric Consortium Conference*, Gaithersburg, MD, 2002. Conference paper.

[67] James L Wayman, Anil K Jain, Davide Maltoni, and Dario Maio. *Biometric systems: Technology, design and performance evaluation*. Springer Science & Business Media, 2005.

[68] Wencheng Yang, Song Wang, Jiankun Hu, Guanglou Zheng, and Craig Valli. Security and accuracy of fingerprint-based biometrics: A review. *Symmetry*, 11(2):141, 2019.

[69] YourStory. Top 10 advantages of mobile app for the healthcare industry, May 2020. Accessed: 2025-06-21.

[70] D. Zhang, D. Ding, J. Li, and Q. Liu. A novel way to improve facial expression recognition by applying fast fourier transform. In *Proceedings of the International MultiConference of Engineers and Computer Scientists 2014*, Hong Kong, March 2014.

[71] Dehai Zhang, Da Ding, Jin Li, and Qing Liu. A novel way to improve facial expression recognition by applying fast fourier transform. In *Proceedings of the International MultiConference of Engineers and Computer Scientists*, volume 1, 2014.

[66] [13] [2] [50] [23] [43] [47] [16] [5] [70] [60] [13] [63] [22] The FFT algorithm was first introduced in [13], and later applied in face recognition methods like Eigenfaces [63]. For further image processing techniques, refer to [22].

The FFT algorithm was first introduced in [13], and later applied in face recognition methods like Eigenfaces [63]. For further image processing techniques, refer to [22]. The XM2VTS database has an established evaluation protocol [39], and is further detailed in AVBPA proceedings [43]. For video standards, see [65, 52]. General image processing can be found in [21], while secure biometric handling is discussed in [48, 66, 3].