People's Democratic Republic of Algeria
Ministry of Higher Education and Scientific Research
Mohamed El Bachir El Ibrahimi University of Borj Bou Arréridj
Faculty of Mathematics and Computer Science
Department of Computer Science

THESIS

In order to obtain the Doctorate degree in LMD (3rd cycle)
Branch: Computer Science
Option: Decision Support Computer Science Engineering

THEME

Towards biometric recognition system based on explainable classifier methods

---

By: Djouamai Zineb

Publicly defended on:

In front of the jury composed of:

Pr. Nouioua Farid.	University of B.B.A	President
Dr. Attia Abdelouahab.	University of B.B.A	Supervisor
Dr. Belhadj Fodil.	University of B.B.A	Examiner
Pr.Akrouf Samir.	University of Msila	Examiner
Dr.Beghriche Abdesselem .	University Setif 1.	Examiner

2023/2024

Abstract

Over the past decade, biometric systems have advanced significantly, achieving high classification accuracy and minimal equal error rates (EER). However, many conventional methods lack transparency and explainability, which are critical in areas like security and identity verification, where trust is paramount. This limitation restricts the ability to understand these systems' decision-making processes, making it difficult to ensure reliability and accountability in sensitive applications.

To address these challenges, we propose the development of an efficient biometric system based on explainable, rule-based classifiers. Unlike traditional approaches, our method incorporates explainability at its core, offering clear insights into the system's decision-making process while maintaining high performance. This approach ensures that the system is not only accurate but also adaptable and user-friendly, enabling its application across a range of classification and predictive tasks.

By prioritizing transparency alongside performance, the proposed system aims to meet the growing demand for trust and usability in biometric applications. Its dual focus on achieving low EER and delivering explainable outcomes ensures it is suitable for deployment in critical domains. This balance between accuracy and explainability positions the system as a reliable and advanced solution for high-stakes environments like security and identity management.

Keywords: rule-based algorithm, explainable classification methods, biometric system, performance.

Résumé

Au cours des dix dernières années, les systèmes biométriques ont connu des avancées significatives, notamment dans le domaine de la classification, qui est devenu un sujet central. Des modèles de pointe ont été développés, atteignant des niveaux d'exactitude exceptionnels et des taux d'erreur égaux (EER) très faibles. Cependant, ces progrès s'accompagnent d'une limitation majeure : le manque de transparence et d'explicabilité des méthodes conventionnelles. Cette lacune pose des problèmes importants, en particulier dans des domaines critiques comme la sécurité et la vérification d'identité, où la confiance dans les décisions du système est essentielle.

Les méthodes classiques des systèmes biométriques échouent souvent à fournir une visualisation claire des composants explicables du modèle, ce qui complique la compréhension et la prévision de leur comportement. Pour remédier à ces insuffisances, nous proposons de développer des systèmes biométriques basés sur des classificateurs explicables et des algorithmes robustes, ancrés dans des règles de logique floue. Cette approche vise à allier performance élevée, convivialité, et transparence, tout en s'adaptant à divers scénarios de classification et de prédiction.

Le système que nous envisageons vise à différencier efficacement les utilisateurs authentiques des imposteurs avec un niveau d'exactitude remarquable. L'objectif principal de cette étude est de lever les obstacles liés à la fiabilité et à l'utilisabilité des classificateurs explicables basés sur la logique floue. En garantissant une précision élevée et un taux d'erreur minimal tout en assurant une explicabilité optimale, ce système s'inscrit comme une solution fiable et adaptée aux environnements sensibles où la performance et la transparence sont primordiales.

Mots-clés : Algorithme basé sur des règles de la logique flou, Méthodes de classification explicables, Système biométrique, Performance.

ملخص

في السنوات العشر الماضية، شهدت الأنظمة البيومترية بروز التصنيف كموضوع ذو أهمية كبيرة، مما أثار نقاشًا واسعًا في هدا المجال.حيث تم إنشاء العديد من النماذج المتطورة خلال هذه الفترة، مما أظهر مستويات دقة استثنائية وحقق معدلات خطأ منخفضة .(EER) ومع ذلك، على الرغم من هذه التطورات الملحوظة، فإن المشكلة الشائعة التي لوحظت في العديد من المصنفات التي تعتمد على المنهجيات التقليدية هي افتقادها لالشفافية والتفسير. يمثل هذا النقص تحديًا كبيرًا، خاصة في مجالات التطبيق الحيوية مثل الأمن والتحقق من الهوية، حيث تكون الشفافية ذات أهمية قصوى. من المتوقع أن توفر الأنظمة البيومترية التي تعمل بناءً على هذه النماذج أداءً عاليًا وتقدم رؤى حول مبررات عمليات اتخاذ القرار الخاصة بها.

غالبًا ما تقصر التقنيات التقليدية في الأنظمة البيومترية في هذا الجانب، حيث تفشل بشكل متكرر في توفير تصور كافٍ للمكونات التفسيرية للنموذج. نتيجةً لذلك، يعيق هذا القيد القدرة على توقع سلوكها أو فهم خصائص أدائها بشكل شامل. في ضوء هذه التحديات، تدور اقتراحاتنا حول إنشاء أنظمة بيومترية تعتمد على خوارزميات فعالة ومرنة مصممة لتكون أكثر ملاءمة للمستخدم. تركز استراتيجيتنا على المصادقة البيومترية من خلال استخدام المصنفات القائمة على قواعد المنطق الضبابي والمستندة بقوة إلى المنهجيات التفسيرية. الهدف الأساسي من هذه الخوارزميات هو ضمان مستوى مرتفع من السرية والحماية مع أن تكون متعددة الاستخدامات بما يكفي لمعالجة مجموعة واسعة من مهام التصنيف أو التنبؤ. الأنظمة البيومترية القابلة للتفسير مصممة للتمييز بين ما إذا كان المستخدم أصيلًا أو محتالًا بمستوى استثنائي من الدقة في التعرف. يركز هذا البحث على التغلب على العقبات المرتبطة بتحسين قابلية الاستخدام وموثوقية المصنفات القائمة على القواعد التفسيرية للمنطق الضبابي. هدفنا النهائي هو تحقيق مستويات دقة فائقة ومعدل خطأ ضئيل ،(EER) وبالتالي إنشاء نظام يتفوق ليس فقط في الأداء ولكن أيضًا في تلبية معيار التفسيرية الحاسم، مما يجعله موثوقًا ومناسبًا للنشر في المجالات الحساسة.

الكلمات الرئيسية: خوارزمية قائمة على قواعد المنطق الضبابي، طرق التصنيف التفسيرية، نظام بيومتري، الأداء.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my advisor, Dr. Attia Abdelouahab. Your guidance, patience, and unwavering support throughout this journey have been invaluable. Your insights and expertise have not only shaped this dissertation but have also greatly influenced my academic growth.

I would also like to extend my sincere thanks to the members of my dissertation committee, Pr.Nouioua Farid. ,Dr. Belhadj Fodil, Dr.Akrouf Samir, and Dr.Beghriche Abdesselem for their time, constructive feedback, and encouragement. Your diverse perspectives have enriched this work and pushed me to refine my thinking.

To my family, thank you for your endless love, patience, and belief in me. Your support has been my foundation and strength throughout this process.

Dedication

As I reach the culmination of this incredible journey, I find myself overwhelmed with gratitude and indebted to those who have been instrumental in my success.

First and foremost, I dedicate this thesis to my beloved parents. Words cannot express the depth of my appreciation for your unwavering love and support. You have been my pillars of strength, guiding me with your wisdom and instilling in me the values of perseverance and dedication. Your sacrifices have been the bedrock upon which I have built my dreams. Thank you for believing in me even when I doubted myself, and for providing me with the opportunities to pursue my passions. This achievement is as much yours as it is mine.

To my dearest husband, my partner, and my best friend, your love and encouragement have been my anchor throughout this journey. You have shared in my triumphs and consoled me in my moments of despair. Your patience and understanding, especially during the times when my focus was solely on my research, have been nothing short of extraordinary. Thank you for being my sounding board, my cheerleader, and my source of unwavering support. Your faith in me has been a constant source of motivation, and I could not have done this without you by my side.

To my brothers, Mahdi and Taha, for your unwavering support, constant encouragement, and the countless moments of laughter. This work is as much yours as it is mine.

I would also like to extend my heartfelt thanks to my academic advisors, colleagues, and friends who have supported me along the way. Your guidance, insights, and camaraderie have been invaluable. Each of you has contributed to this work in unique ways, and for that, I am deeply grateful.

Lastly, to everyone who has believed in me and stood by me during this arduous yet fulfilling

journey, thank you. This thesis stands as a testament to the collective support and love I have received, and I am forever indebted to you all. To my future self, a reminder that perseverance and passion can turn dreams into reality.

Contents

Acknowledgements **4**

List of Figures **11**

List of Tables **14**

1 Introduction **16**

1.1 Problem Statement 16

1.2 Thesis objectives 17

1.3 Thesis structure 18

1.4 Contributions 19

2 Literature Review of explainable biometric system **20**

2.1 Introduction 20

2.2 Context 20

2.3 Facial Feature 23

2.3.1 Face Popular Databases 25

2.4 Finger Knuckle Print: FKP 31

2.4.1 FKP Popular Databases 33

2.5 Explainable Biometric systems 36

2.5.1 Face-based Explainable Biometric Systems 37

2.5.2 Fkp-based Explainable Biometric Systems 39

2.6 Conclusion 40

3 Theorical background about biometric systems **42**

3.1 Introduction . . . 42

3.2 brief history of biometric system . . . 42

3.3 Principal of Biometric Recognition . . . 43

3.3.1 Principal Fundamental . . . 43

3.3.2 Types of Biometric systems . . . 45

3.4 Importance of biometrics in various applications . . . 48

3.5 Biometric Traits . . . 49

3.6 Performance Analysis . . . 57

3.7 Conclusion . . . 60

4 Methods and Tools **61**

4.1 Introduction . . . 61

4.2 Pre-Processing . . . 61

4.2.1 FKP Pre-Preprocessing Techniques . . . 62

4.2.2 Face Preprocessing Techniques . . . 64

4.3 Feature Extraction . . . 70

4.3.1 Gabor Filter Bank . . . 70

4.3.2 Binary Similarity and Intensity Feature (BISIF) descriptor . . . 72

4.4 Dimensionality Reduction (PCA,LDA and t-SNE) . . . 73

4.4.1 Principal Component Analysis . . . 74

4.4.2 Linear Discriminant Analysis . . . 75

4.4.3 t-Distributed Stochastic Neighbor Embedding . . . 78

4.5 Classification . . . 79

4.5.1 Classical Classifiers . . . 79

4.5.2 Explainable Classifier . . . 85

4.6 Conclusion . . . 89

5 Explainability in Biometric Systems **90**

5.1 Introduction 90

5.2 Fundamentals of Explainability 90

5.2.1 Basic Concepts 90

5.2.2 Explainability Approaches 92

5.3 Explainable Biometric Systems 95

5.3.1 Context and Issues 96

5.4 Applications of Explainability in Biometric Systems 97

5.4.1 Data and Privacy Management 98

5.4.2 Human-System Interactions 99

5.5 conclusion 99

6 Contribution **101**

6.1 A face recognition system based-ALMMo-0 classifer 101

6.1.1 Architecture and algorithm of the ALMMo-0 classifer 104

6.1.2 The main algorithm of ALMMo-0 classifier 104

6.1.3 Computational complexity 107

6.1.4 The proposed biometric system-based ALMMo-0 classifier architecture 108

6.1.5 Experiments and results 110

6.1.6 Conclusion 115

6.2 A Biometric system based fuzzy-Rule based Classifier for finger knuckle print (FKP) 116

6.2.1 The proposed FKP biometric system 117

6.2.2 Experiments and results 120

6.3 Explainable Deep Neural Networks Classifier for Robust face recognition . . . 124

6.3.1 The xDNN definition and main algorithm 126

6.3.2 Proposed methodology 131

6.3.3 Experement And Results 133

6.3.4 Conclusion 137

7 General conclusion **138**

7.1 Summary of Contributions 138

7.2 Implications for Biometric Systems 139

7.3 Future Research Directions 139

7.4 Concluding Remarks 140

Bibliography **141**

List of Figures

2.1 Images from The Labeled Faces in the Wild (LFW) 25

2.2 Sample Images from the Celebrity Dataset 25

2.3 Exemple of Imanges from The MORPH dataset 26

2.4 Example faces from the Face Detection Data set and Benchmark (FDDB). . . . 26

2.5 A set from WIDER FACE: A Face Detection Benchmark 27

2.6 A set of pictures from Columbia-Gaze Dataset 27

2.7 JAFFE Dataset 28

2.8 Examples of Essex face database 28

2.9 Some color images from faces94 dataset 28

2.10 Some color images from faces95 dataset 29

2.11 Some color images from faces96 dataset 29

2.12 Grimace Database Sample Images 29

2.13 Sample Images from Georgia Tech Face Database 30

2.14 A set of images from CASIA-FaceV5 dataset 30

2.15 A set from ORL Dataset 31

2.16 Finger Knuckle Print PolyU Database 34

2.17 The Hong Kong Polytechnic University Finger Image Database 34

2.18 Sample Image of IIT Delhi Knuckle Print Database 35

3.1 Architecture of Multimodel Biometric System 46

3.2 Architecture of Unimodel Biometric System 47

3.3 Metric used to measure the system's performance 58

4.1 Linear histogram equalization is implemented from the left side to the right side 65
4.2 Gamma correction curve for different values of γ 68
4.3 Gabor Filters with five scales and eight orientation 72
4.4 (a): Sample of the FKP ROI image, (b): BSIF filter with a size 11 × 11 and of length 12, (c): BSIF features (d): final BSIF 73
4.5 Principal Component Analysis (PCA) 75
4.6 Linear Discriminant Analysis (LDA) 76
4.7 Nearest Neighbor Classifier 83

6.1 An illustrative frame diagram of ALMMo-0 Classifier 104
6.2 Block diagram of the proposed method. 108
6.3 ROC and CMC curves for Jaffe database. 112
6.4 ROC and CMC curves for Faces95 database. 112
6.5 ROC and CMC curves for Faces94 database. 113
6.6 ROC and CMC curves for Faces96 database. 113
6.7 ROC and CMC curves for Grimasse database 113
6.8 ROC and CMC curves for GTdb cropped$_{f}acesdatabase$. 113
6.9 ROC and CMC curves for CASIA database. 114
6.10 ROC and CMC curves for ORL database. 114
6.11 ROC and CMC curves for YALE database. 114
6.12 The main steps of the proposed biometric system based on fuzzy rule-based classifier 118
6.13 The process of ROI extraction from the FKP image 118
6.14 ROC and CMC of RMF Database. 121
6.15 ROC and CMC of RIF Database. 121
6.16 ROC and CMC of LMF Database. 122
6.17 ROC and CMC of LIF Database. 122
6.18 The Main architecture of the xDNN Classifier 126
6.19 The Main architecture of the proposed biometric system 132

6.20 ROC and CMC curves for Faces95 database. 135
6.21 ROC and CMC curves for Faces96 database. 135
6.22 ROC and CMC curves for GTDP database. 136
6.23 ROC and CMC curves for ORL database 136
6.24 ROC and CMC curves for CASSIA database. 136

List of Tables

2.1 Summary of Popular Works in Biometric Face Modality 24

2.2 Summary of Key Contributions in FKP Recognition 33

2.3 The most popular works that propose explainable biometric systems for face modality 39

2.4 Recent and Popular Works in Explainable FKP-Based Biometric Systems . . . 40

3.1 Comparison of multimodel and unimodel Biometric Systems 48

3.2 Advantages and Disadvantages of biometric modalities 57

4.1 Strengths and weaknesses of k-NN Classifier 82

4.3 Strengths and weaknesses of the SVM classifier 85

6.1 A signification of notation of ALMMo-0 classifier 105

6.2 Accuracy, Sensitivity, and Specificity of the biometric system based-ALMMo-0 classifier. 110

6.3 Performance comparison across different classifiers 111

6.4 Comparison with other methods 115

6.5 results of applying ALMMo-0 Classifier in form of Rank and EER. 120

6.6 comparative study between ALMMo-0 Classifier and NN Classifier. 121

6.7 Comparison with the classical methods. 123

6.8 The Notations 131

6.9 Accuracy of the Proposed biometric System based on xDNN 134

6.10 Rank and EER Obtained by applying xDNN Classifier. 134

6.11 Comprative Analysis 134

Chapter 1

Introduction

1.1 Problem Statement

Despite the impressive performance exhibited by present-day biometric authentication systems, the assurance of achieving a commendable recognition rate remains elusive when employing traditional classifiers that rely on distance-based methods. It is worth noting that these approaches are consistently plagued by a myriad of significant challenges. Firstly, they struggle to effectively handle extensive datasets characterized by high dimensionality. Additionally, the descriptors utilized in the matching process prove to be highly susceptible to outliers and missing values, further complicating the accuracy of the system. Moreover, the models constructed based on classical classifiers lack transparency and interpretability, thereby posing potential risks to users. Consequently, it is prudent to restrict their utilization to non-regulated data sets to mitigate any legal liabilities stemming from decisions made based on these models.

Moreover, within the context of sensitive domains such as biometric systems applied in medical diagnoses and credit underwriting, the reliance on the aforementioned models necessitates a high level of trustworthiness. Therefore, it becomes imperative to not only assess their performance but also anticipate their behavior beyond conventional expectations. This requirement represents a challenge that conventional methods struggle to address, primarily due to their inherent lack of transparency and interpretability. These inherent limitations contribute directly to a deterioration in the performance of the authentication system, leading to increased error

rates. Consequently, such a system would not be deemed suitable for deployment in critical settings where robust security measures are paramount.

To surmount the aforementioned constraints, a proposal is put forth to develop efficient and robust biometric systems based on explainable efficient algorithms for biometric recognition. This proposal involves the utilization of rule-based classifiers founded on explainable methodologies, ensuring a heightened level of privacy and security. Such algorithms can be applied across a diverse spectrum of classification and prediction tasks, with a primary focus on determining the authenticity of users versus impostors while maintaining a precise recognition rate. The emphasis lies on enhancing the usability and reliability of these explainable rule-based classifiers, which constitutes a central challenge in this research endeavor. Undoubtedly, the ultimate goal is to achieve a high degree of accuracy and a negligible equal error rate (EER).

1.2 Thesis objectives

The primary objective of this thesis is to develop explainable biometric systems with an explaibanle classification methods based on transparent and understandable algorithms for biometric recognition, ensuring that humans can easily comprehend the decision-making process to increase trust. Additionally, the thesis aims to achieve high performance in biometric recognition by building explainable biometric systems with high accuracy and low equal error rates, providing reliable systems that accurately differentiate between genuine users and impostors. To enhance trustworthiness in sensitive applications such as medical diagnoses and credit underwriting, the classifiers must offer clear justifications for their decisions. The research also focuses on improving privacy and security by developing biometric systems that protect user data and prevent unauthorized access through secure authentication methods. Emphasizing human acceptability and usability, the thesis seeks to create efficient algorithms that are user-friendly and instill confidence in biometric recognition systems. Incorporating visualization techniques to highlight the explainable aspects of models will aid users in understanding the decision-making process of classifiers. Based on these objectives, the detailed tasks and methodologies of the thesis include biometric system development for enhanced explainability and performance,

performance evaluation to test accuracy and equal error rates, user studies to assess the acceptability and usability of the proposed systems, development of visualization tools for classifier decision-making, and conducting security and privacy analysis to ensure that the systems meet high standards of data protection. We are putting forward a proposition to develop highly efficient and robust biometric systems based on explainable classification methods, utilizing rule-based classifiers algorithm that is founded on explainable methods to ensure a significant level of privacy and security, these algorithms can be applied across a wide range of classification or prediction issues. It is essential for the system to possess the capability to accurately ascertain whether the user is authentic or an intruder, providing a precise (real) recognition rate.

The usability and dependability of the explainable rule-based classifier are regarded as the primary challenge being addressed in this particular research endeavor. Unquestionably, the aim is a high level of accuracy and an easily manageable equal error rate (EER).

1.3 Thesis structure

Chapter 2: Explains biometrics concept's history. The first part discusses biometric recognition and system evaluation. The second part introduces the apparition and developments of the explainable biometric system and algorithms.

Chapter 3: Devolves explainability in Biometric System, showing their principal role in various fields such as security, healthcare, and identity management. Despite their clear benefits, they are sometimes seen as "black boxes", leading to decisions that users may not always comprehend. This chapter explores the significance of explainability in biometric systems, its consequences, and strategies for enhancing the clarity of the intelligent machine's decision-making process.

Chapter 4: Discusses the biometric techniques in face recognition systems. The chapter provides a general definitions of the principal theatrical concepsts of biometric.

Chapter 5: Emphesizes the Methods and tools using during the biometric recognation process, from the pre-processing to matching step in details ans citing the most populars methods in addition to a comparative analysis of the most effecients algorithms.

Chapter 6: : Highlights our significant contributions made in the field, with a special focus on the application of explainable biometric systems. It emphasizes the importance of using explainable classifiers to improve the performance and accuracy of biometric systems. Additionally, the study thoroughly analyzes multimodel biometric systems, exploring the complexities of integrating multiple biometric modalities to enhance security and efficiency.

Chapter 7: General Conclusion of the study's main outcomes, contributions, practical implications, limitations, potential future research directions, and overall significance are effectively summarized. Tailor the details to align with the focus of our research study.

1.4 Contributions

Our thesis contributions can be outlined in the following four points.

1. Propose a new biometric system based on ALMMo-0 classifier using face modality. published by Evolving systems (Class A Journal) under the Title "A Face recognition system based-ALMMo-0 classifier"
   Citation : Djouamai, Z., Attia, A., Chalabi, N. E., Hassaballah, M. (2024). A face recognition system based-ALMMo-0 classifier. Evolving Systems, 15(3), 881-898.

2. Devolop a new knuckle finger print (FKP) biometric systems based of fuzzy-rule based classifier that can provide a high accuracy published by International Conference on Advanced Engineering in Process Intelligence (ICAEPI'23) Preface The 4th ICAEPI'23

3. Propose a new biometric system based on xDNN classifier using face modality which is fully transparent and explainable due to its fuzzy architecture also less complex and less expensive in term of time and resources. sent to Evolving systems (Class A Journal). Status: Under Review.

Chapter 2

Literature Review of explainable biometric system

2.1 Introduction

Biometric systems play a crucial role in authenticating and identifying individuals based on unique physiological or behavioral characteristics. In this chapter, we will explain the history of biometrics. The first part discusses biometric recognition and system evaluation. The second part introduces the apparition and developments of explainable biometric systems and algorithms.

2.2 Context

Among various biometric modalities, facial recognition stands out due to its non-intrusive nature and broad applicability. This initial discussion aims to elucidate the fundamental principles underlying biometric systems, with a specific focus on facial recognition. The use of biometric systems relies on biological or behavioral traits to verify or recognize individuals, including fingerprints, iris patterns, voiceprints, and facial features [1, 2] [3] [4]. Facial recognition, in particular, exploits distinct facial elements like eye configuration, nose shape, mouth features, and overall facial structure [5]. The process of recognition typically involves several crucial

stages. Initially, a camera, sensor or a similar imaging tool captures a digital image or video of the modality [6, 7]. This step, known as image acquisition, is vital as the quality of the captured image directly influences subsequent recognition stages. High-resolution cameras and advanced capturing methods are often used to ensure clarity and detail [8, 9]. Next, the system extracts unique attributes from the captured image, such as inter-eye distance, nasal shape, and jawline contour in the case of face modality. These features are then converted into a mathematical format known as a ”template” [10]. This phase, termed feature extraction, employs intricate algorithms to analyze and encode the features into a numerical representation. During authentication or identification, the system compares the acquired template with those stored in its database [11]. This comparison utilizes advanced matching algorithms to calculate the similarity between the stored and acquired templates. If the resemblance exceeds a set threshold, the individual is verified or identified; otherwise, the system rejects the attempt [12].In our work we have focused on the two most popular and effecient modalities: Facial Feature and Finger Knukle Print (FKP) Modality.

Facial recognition as a most popular modality offers the advantage of non-intrusive nature [13], unlike other biometric methods that require physical contact or specific actions from the individual, facial recognition can be performed remotely without the subject's active participation. This feature makes it ideal for applications where user convenience and minimal interaction are essential [14]. Moreover, facial recognition technology can be easily integrated into various devices and systems, including smartphones, laptops, security cameras, and automated access control systems. Its versatility and seamless integration contribute to its extensive adoption in diverse sectors such as finance, healthcare, law enforcement, and retail [15]. The rapid progression of facial recognition technology is driven by advancements in machine learning, computer vision, and data gathering methodologies, despite various obstacles [16]. The utilization of deep learning algorithms, particularly convolutional neural networks (CNNs), has significantly improved the accuracy and robustness of facial recognition systems by enabling the learning of intricate patterns and features from extensive datasets. These algorithms enhance the capability of recognizing faces across diverse conditions. The adoption of emerging techniques

like 3D face recognition, which captures the three-dimensional facial geometry, shows potential for enhancing accuracy and resilience to variations in pose and occlusions [17]. Moreover, the integration of multimodel biometrics, which combines facial recognition with other biometric traits such as voice or gait, can further boost security and reliability. As technology progresses, it has the capability to enhance security protocols, streamline identity verification procedures, and introduce innovative applications across various industries and sectors. Developments like real-time facial recognition in surveillance systems, contactless access control, and personalized user experiences in consumer electronics illustrate the transformative influence of this technology. The forthcoming chapter will concentrate on presenting significant contributions in facial recognition, with a focus on efficient explainable biometric systems introduced in the past decade, particularly those leveraging facial traits. Noteworthy works including Eigenfaces by [18], Fisherfaces [19], and contemporary deep learning approaches such as [13] and FaceNet by [14] will be thoroughly examined. These contributions have established the groundwork for current advancements and continue to shape ongoing research and development in biometric facial recognition.

In the other hand, The recognition of Finger-Knuckle Prints (FKP) has emerged as a significant biometric modality owing to its uniqueness, durability, and straightforward acquisition process.[20] were the pioneers in proposing FKP as a credible biometric identifier, demonstrating its efficacy in individual identification through pioneering feature extraction and classification methodologies. Building upon this seminal work, Kumar and [21] made substantial contributions to FKP recognition by incorporating texture-based approaches alongside machine learning algorithms, culminating in enhanced accuracy and resilience. Further investigations by [22] and [23] augmented FKP recognition by formulating more advanced image preprocessing and matching algorithms, thus facilitating more dependable performance across diverse security applications. Notwithstanding these developments, challenges such as image quality, intra-class variability, and inter-class resemblance remain, propelling continuous research endeavors aimed at optimizing FKP systems for practical implementation [20] [21] [22] [23]

2.3 Facial Feature

Face recognition is a critical component of biometric systems, providing non-intrusive authentication based on inherent facial characteristics [24]. Deep learning for face recognition heavily relies on large-scale, high-quality datasets, which can be difficult to obtain due to time, financial, and privacy constraints [25] [26]. Synthetic data generated through computer graphics pipelines has shown promise in achieving competitive results comparable to training with real images, highlighting the significance of data quality in model performance [27] [28]. Furthermore, the utilization of 3D ShapeNets has showcased significant progress in 3D face recognition, surpassing state-of-the-art performance on various datasets through efficient 3D shape analysis. These advancements underscore the continual evolution and innovation in face recognition technologies across diverse research domains.

Facial recognition in biometric systems is dependent on a number of crucial stages: Facial Image Acquisition is the initial step [29], where the individual's facial image is obtained through a camera or similar device, either from a static image or extracted from a video sequence. Subsequently, Facial Feature Extraction involves the extraction of unique facial characteristics from the acquired image [30], encompassing the spatial arrangement of facial components like eyes, nose, and mouth, along with finer details such as facial contours and lines. Following this is the development of a facial template, wherein the extracted features are utilized to construct a distinct mathematical representation or template specific to the individual, digitally encoding the unique facial attributes [31]for identification or authentication purposes. The resultant facial template is then securely stored in a database for future comparisons with other templates for identification. In the stage of Comparison and matching [32], when verification or identification is required, the system juxtaposes the facial template of the individual under scrutiny with templates stored in the database, employing methods like assessing similarities between templates through techniques such as Euclidean distance comparison or employing machine learning models [32]. Ultimately, a Decision is made by the system based on the level of resemblance between the individual's facial template and those archived in the database. In cases where a satisfactory match is established, the individual is successfully identified or verified;

conversely, if no match is found, the identification request is declined. In essence, the process of facial recognition in biometric systems hinges on the precise capture of facial attributes, their transformation into digital templates, and their subsequent comparison with pre-existing templates for the purpose of identifying or authenticating individuals.

Reference	**Title and Approach**	**Key Findings**
[18]	Eigenfaces for Recognition: Principal Component Analysis (PCA) to reduce dimensionality	Demonstrated effective face recognition using PCA, a foundational work in face recognition
[19]	Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection	Introduced Fisherfaces which improved recognition under varying lighting and facial expressions
[33]	Rapid Object Detection using a Boosted Cascade of Simple Features	Presented a robust real-time face detection method using Haar-like features and AdaBoost
[16]	Face Description with Local Binary Patterns: Application to Face Recognition	Introduced Local Binary Patterns (LBP) for texture-based face recognition, achieving high accuracy
[13]	DeepFace: Closing the Gap to Human-Level Performance in Face Verification	Developed a deep learning model using a 3D alignment for face verification, achieving near human-level performance
[14]	FaceNet: A Unified Embedding for Face Recognition and Clustering	Introduced FaceNet which uses a deep convolutional network to learn a mapping from face images to a compact Euclidean space
[15]	Deep Face Recognition: Implementation of deep neural networks for face recognition using the VGGFace model	Demonstrated high accuracy on face recognition benchmarks using deep learning

Table 2.1: Summary of Popular Works in Biometric Face Modality

2.3.1 Face Popular Databases

- The Labeled Faces in the Wild (LFW) [34]: dataset comprises a substantial assortment of celebrity facial images captured in diverse scenarios, rendering it a favored option for assessing facial recognition algorithms within real-world settings. comprising 13,233 images of 5,749 individuals, each resized to 250 x 250 pixels and stored in JPEG format. This dataset features natural variations in pose, expression, lighting, and background, with multiple images per individual to ensure robust testing



Figure 2.1: Images from The Labeled Faces in the Wild (LFW)

- CelebA [35]: a celebrity facial dataset, encompasses numerous images annotated with facial attributes like eyeglasses and makeup presence, commonly utilized for training and evaluating facial recognition algorithms.containing over 200,000 celebrity images of more than 10,000 individuals, each with a resolution of 178 x 218 pixels. It features 40 binary attribute annotations (such as ”smiling” and ”wearing glasses”) and five key landmarks (eyes, nose, mouth corners) for each image. This dataset's diversity in age, ethnicity, and gender.



Figure 2.2: Sample Images from the Celebrity Dataset

- The MORPH dataset : features facial images illustrating the aging process of individuals over time, serving as a valuable asset for investigating age-related facial changes and

assessing facial recognition algorithms in practical conditions.containing over 55,000 facial images of approximately 13,000 individuals with diverse demographics, including variations in age, ethnicity, and gender



Figure 2.3: Exemple of Imanges from The MORPH dataset

- The FDDB (Face Detection Data Set and Benchmark) [36]: Utilized for appraising face detection algorithms, involves numerous images annotated to indicate the presence of faces, thus serving as a prevalent choice for evaluating the efficiency of face detection systems.

- The Yale Face Database [37]: Showcases facial images captured under varying lighting conditions, facial expressions, and head orientations, making it a valuable resource for evaluating facial recognition algorithms under different circumstances. designed to evaluate the performance of face detection algorithms. It comprises 2,845 images that contain a total of 5,171 faces, with a wide range of variations in pose, scale, and occlusion.



Figure 2.4: Example faces from the Face Detection Data set and Benchmark (FDDB).

- The WIDER Face dataset [38]: is a collection of facial images equipped with bounding boxes for the assessment of face detection algorithms in diverse settings, encompassing both outdoor and indoor environments.

- MS-Celeb-1M [39] is a repository of more than one million pictures featuring famous individuals' faces sourced from various online platforms, establishing itself as one of the

most extensive publicly accessible facial image databases. Consisting of 32,203 images with 393,703 labeled faces. These images are collected from a wide range of settings, including varied scenes, events, and everyday activities, making the dataset highly diverse.



Figure 2.5: A set from WIDER FACE: A Face Detection Benchmark

- Columbia-Gaze: represents a dataset of facial images with annotations of gaze direction, utilized for the investigation and appraisal of gaze direction recognition and face detection techniques.It comprises 5,880 images of 56 participants, each photographed under varying head poses and gaze directions.

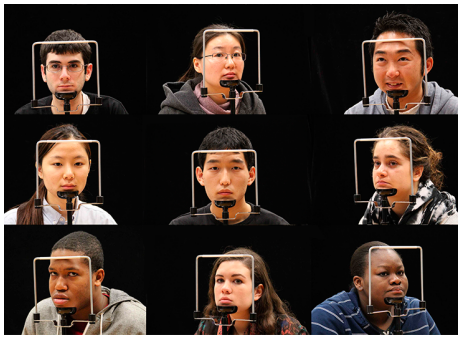


Figure 2.6: A set of pictures from Columbia-Gaze Dataset

- The Labeled Faces in the Wild Home (LFWA) is an expansion of the LFW database with supplementary annotations such as gender, race, and age, rendering it beneficial for studies on the recognition of multiple facial attributes.

- Multi-PIE (Multiple Pose, Illumination and Expression) [40] comprises facial images capturing individuals in diverse poses, lighting conditions, and facial expressions, serving as a critical asset for the evaluation of robust facial recognition algorithms.It contains the same 13,233 images of 5,749 individuals as LFW, but with additional attribute annotations. Each image in LFWA is labeled with 40 binary attributes, such as ”smiling,”

”young,” ”wearing glasses,” and ”male,” providing a rich set of data for training and evaluating facial attribute recognition models.

- The Japanese Female Facial Expression (JAFFE): The database JAFFE is a set of 10 Japanese female expressers, each expresser have 7 posed facial expressions. All 213 images are rated semantically on 6 facial expressions by 60 Japanese viewers. Each image has a resolution of 256 x 256 pixel-sized 8-bit grayscale and tiff format.

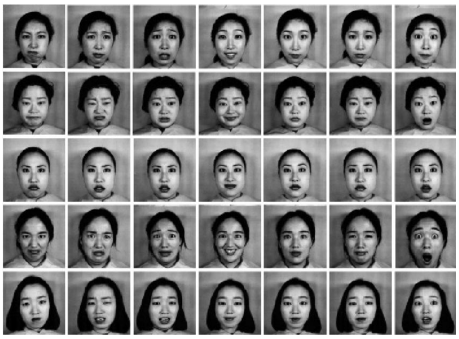


Figure 2.7: JAFFE Dataset

- ESSEX face database: a sample of 7900 pictures taken from 395 individuals. Images were taken under various environmental conditions of illumination, background, expression, and scale.



Figure 2.8: Examples of Essex face database

ESSEX database is divided into 4 sub-databases:

  - Faces94: a sample of 153 individuals, each one providing 20 images. 180x200 pixels is the resolution of the image which was taken from a subject in the speaking action time.



Figure 2.9: Some color images from faces94 dataset

– Faces95: a sample of 72 individuals, each one providing 20 images. Here, 180x200 pixels is the resolution of the image which was taken from a subject while moving one step toward the camera.



Figure 2.10: Some color images from faces95 dataset

– Faces96: a sample of 152 individuals each one providing 20 images. The images were taken in the same way as Faces95 with a different resolution of 196x196 pixels.



Figure 2.11: Some color images from faces96 dataset

– Grimace: a sample of 360 images made by taking 20 shots from 18 individuals. In this sub-database, subjects were asked for moving ahead and making grimaces while taking pictures.



Figure 2.12: Grimace Database Sample Images

- Georgia Tech face database: A set of 750 images belonging to 50 individuals. Photos are taken in two or three sessions under different conditions of lighting, facial expressions, and scales. Each image is 640x480 pixels in resolution, but the average size of the face is 150x150 pixels. In our study, we have resized the cropped database's images, to 128x128 pixels.



Figure 2.13: Sample Images from Georgia Tech Face Database

- CASIA (CASIA FACE-V5): consists of 500 individual and a total of 2500 color facial images with a seize of 16 bits each and Resolution of 640*480, all the color images are captured using Logitech USB camera in one session , and under different conditions of expression, pose, imaging distance..etc.

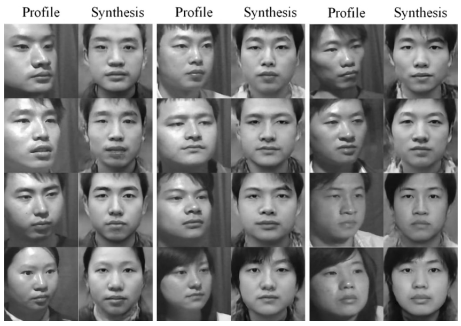


Figure 2.14: A set of images from CASIA-FaceV5 dataset

- ORL database: Abbreviation of Online Redo Log; it contains 400 images for 40 different individuals, some of the pictures were taken in various periods, light conditions, facial expressions, and accessories (wear of glasses, no glasses .. etc.). The whole collection of images where taken with a dark background in the form of frontal pictures on the upright side. Each image has a size of 92x112 pixels, with 256 grey levels per pixel.



Figure 2.15: A set from ORL Dataset

These datasets stand out as extensively utilized resources within the realm of facial recognition, owing to their superior quality, extensive size, and diversity, thereby making them well-suited for the training, evaluation, and advancement of facial recognition algorithms.

2.4 Finger Knuckle Print: FKP

The Finger-Knuckle Print (FKP) modality has attracted considerable scholarly attention as a method of biometric recognition, owing to its unique characteristics, non-invasive qualities, and temporal stability. Initial contributions by [20] established the groundwork for FKP recognition, evidencing its feasibility within biometric systems through the development of robust image acquisition and feature extraction methodologies. This foundational work was instrumental in positioning FKP as a viable alternative to conventional modalities such as fingerprints. Expanding upon this foundation, [21] propelled the field forward by integrating texture-based methodologies and machine learning algorithms, which markedly enhanced recognition accuracy. Their investigations underscored the efficacy of Gabor filters in extracting discriminative features from FKP images, establishing this approach as a benchmark in subsequent inquiries.

Further progress was achieved by [22], who proposed a collaborative representation-based classification (CRC) framework for FKP recognition, effectively addressing the challenges associated with high intra-class variability and low inter-class separability. Their methodology exhibited superior performance, especially in the context of large-scale datasets. [23] continued

to advance FKP recognition by implementing Riesz transforms to encode local image patterns, thereby augmenting the system's robustness against fluctuations in illumination and finger positioning.

In recent years, scholarly investigations have increasingly concentrated on deep learning methodologies to extend the frontiers of FKP recognition. For example, [41] examined convolutional neural networks (CNNs) for automatic feature extraction, which significantly diminished the dependence on handcrafted features and enhanced the system's adaptability to diverse environments. This paradigm shift towards deep learning has been further propelled by studies such as those conducted by [42] who employed a hybrid deep learning framework that combined CNNs with recurrent neural networks (RNNs) to capture both spatial and temporal dynamics in FKP images, resulting in even greater accuracy and robustness.

Notwithstanding these advancements, challenges persist, particularly in practical applications where FKP images are susceptible to varying degrees of noise, distortion, and incomplete data. Recent endeavors by [43] have concentrated on mitigating these challenges through the creation of innovative pre-processing techniques and adaptive classifiers capable of more effectively managing such variations. Their contributions have been pivotal in enhancing the practicality and reliability of FKP recognition across diverse operational contexts.

In summary, the progression of research concerning the FKP modality illustrates a trajectory that evolves from fundamental techniques centered on feature extraction and classification towards more sophisticated strategies that leverage deep learning and advanced preprocessing techniques. This continuous line of inquiry remains focused on augmenting the efficacy and applicability of FKP within biometric systems, thereby establishing it as a significant instrument for security and identification purposes.

Table 2.2: Summary of Key Contributions in FKP Recognition

Ref.	Contribution	Summary of Work
[20]	Foundational Work	Established the groundwork for FKP recognition by developing robust image acquisition and feature extraction methodologies, positioning FKP as a viable biometric modality.
[21]	Texture-based Methods	Integrated texture-based methodologies and machine learning algorithms to enhance recognition accuracy, emphasizing the effectiveness of Gabor filters in feature extraction.
[22]	CRC Framework	Proposed a collaborative representation-based classification (CRC) framework to address challenges like high intra-class variability and low inter-class separability, showing superior performance in large-scale datasets.
[23]	Riesz Transforms	Utilized Riesz transforms to encode local image patterns, improving robustness against fluctuations in illumination and finger positioning.
[41]	Deep Learning (CNN)	Examined convolutional neural networks (CNNs) for automatic feature extraction, reducing dependence on handcrafted features and enhancing system adaptability to diverse environments.
[42]	Hybrid Deep Learning	Employed a hybrid deep learning framework combining CNNs and RNNs to capture both spatial and temporal dynamics, resulting in improved accuracy and robustness.
[43]	Pre-processing	Focused on innovative pre-processing techniques and adaptive classifiers to mitigate challenges such as noise, distortion, and incomplete data, enhancing the practicality and reliability of FKP recognition.

2.4.1 FKP Popular Databases

Finger Knuckle Print (FKP) databases are extensively utilized in the domain of biometric research, particularly within biometric recognition systems. Below are several of the most prominent and frequently cited FKP databases:

- PolyU Finger Knuckle Print Database: This database is among the most renowned FKP repositories, developed by the Hong Kong Polytechnic University (PolyU). It is routinely

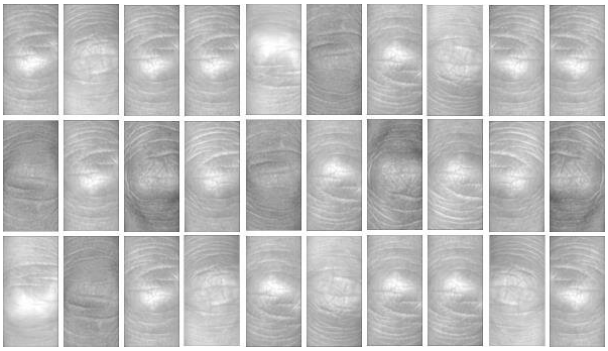


Figure 2.16: Finger Knuckle Print PolyU Database



Figure 2.17: The Hong Kong Polytechnic University Finger Image Database

employed in research pertaining to FKP recognition algorithms. Details: It encompasses images from both the left and right hands of participants. It spans multiple sessions, facilitating the examination of intra-class variability. It is extensively referenced in scholarly articles and benchmarking studies.

Link: PolyU FKP Database

- Hong Kong PolyU Contactless Hand Dorsal Images Database Description: This database represents another significant contribution from the Hong Kong Polytechnic University, concentrating on contactless hand dorsal imaging, which includes FKP. Details: It comprises high-resolution images capturing finger knuckle patterns. It proves advantageous for investigations into contactless biometric recognition systems.

  Link: PolyU Contactless Hand Database

- CASIA Multi-Spectral FKP Database: The Chinese Academy of Sciences Institute of Automation (CASIA) offers a multi-spectral FKP database. Details: It provides multi-spectral images that can enhance the robustness of FKP recognition. It supplies images captured under various wavelengths to investigate the effects of illumination conditions.

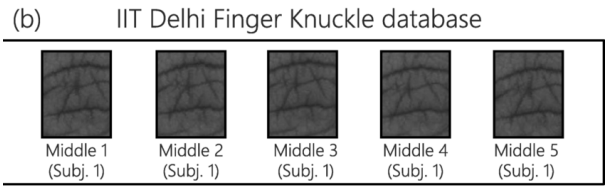


Figure 2.18: Sample Image of IIT Delhi Knuckle Print Database

Link: CASIA Biometric Databases

- IIT Delhi Knuckle Print Database: Formulated by the Biometrics Research Lab at IIT Delhi, this database encompasses knuckle print data from a diverse array of subjects. Details: It includes images captured from multiple perspectives. It is instrumental for the assessment of algorithms designed for finger knuckle recognition.
  Link: IITD Knuckle Print Database

- Tongji FKP Database: Established by Tongji University, this database is frequently utilized in research pertaining to FKP and dorsal hand recognition systems. Details: It features high-quality images of knuckle patterns. It contains images from various sessions, thereby permitting the evaluation of algorithm performance under real-world conditions.
  Link: Available upon request from the university.

These databases are routinely cited in academic inquiries centered on FKP-based biometric systems. The PolyU database, in particular, enjoys widespread popularity due to its accessibility and the extensive number of studies that have corroborated their findings through its utilization.

2.5 Explainable Biometric systems

Explainable machine learning (XAI) [44] denotes the array of methods and approaches utilized to enhance the interpretability and comprehensibility of machine learning models for individuals [45]. Although conventional machine learning models such as decision trees [46] or linear regression possess [47] inherent interpretability to a certain degree, intricate models like deep neural networks [48]often function as ”black boxes” [49], presenting challenges for humans to grasp the rationale behind their predictions. XAI methods strive to overcome this constraint by furnishing insights into how a model generates its predictions [50], thus augmenting transparency [51], confidence, and applicability. These methodologies encompass feature importance, model-agnostic techniques, visualization [52], rule extraction [53], attention mechanisms, counterfactual explanations, and saliency maps [54]. Through the application of these techniques, explainable machine learning endeavors to render machine learning models more lucid, responsible, and dependable, enabling individuals to comprehend and verify their decisions, particularly in pivotal domains such as healthcare, finance, and criminal justice. Concerning explainable biometric systems specifically, their origins can be traced back to the inception of biometrics itself [55]. Biometric systems, which verify individuals based on their physiological or behavioral traits, have a long history, including ancient practices like using fingerprints in business dealings in ancient Babylon. Nevertheless, the notion of explainability in biometric systems has become more significant in recent times [56], notably due to the rise of advanced machine learning and artificial intelligence methodologies. Initially, biometric systems emphasized accuracy and efficiency, often employing intricate algorithms and models [57] that were challenging to decipher . This lack of transparency raised concerns [58], particularly in critical sectors such as law enforcement and national security, where the rationale behind decisions was crucial. In response, researchers have initiated the development of methods to enhance the explainability nature of biometric systems [59] . One strategy is to include inherently interpretable characteristics, like utilizing specific facial regions for facial recognition or spotting unique patterns in fingerprints. Another method involves providing explanations after the fact, using techniques such as saliency maps or feature importance scores to highlight the most influ-

ential aspects of the input data in biometric decision-making. Presently, explainable biometric systems are continuously progressing, guided by a growing acknowledgment of the significance of transparency and answerability in biometric applications. As these systems advance and become more interconnected in diverse fields, the necessity for explainability will remain crucial, ensuring that biometric decisions are not just precise but also comprehensible and defensible.

2.5.1 Face-based Explainable Biometric Systems

The historical background of facial recognition biometric systems with explainable features can be traced back to the initial endeavors in facial identification during the 1960s. During their nascent stages, these systems exhibited simplicity, utilizing basic techniques like comparing facial feature point distances for recognition purposes. Through the passage of time and advancements in technology, especially in computing and machine learning domains, facial recognition has undergone significant development, progressively becoming more intricate. Nevertheless, this complexity has prompted concerns regarding the lack of transparency and comprehensibility in these systems, particularly critical in domains such as security and surveillance. Researchers have embarked on efforts to mitigate these concerns by enhancing the interpretability of facial recognition systems. This involves the utilization of easily understandable facial attributes, including eye morphology or facial feature configurations, as well as the creation of post-hoc methodologies to elucidate model decisions, such as generating salience maps highlighting facial areas with the greatest decision impact. Presently, amidst the swift technological progress and heightened awareness of privacy and individual rights, face-based explainable biometric systems are advancing further, offering more transparent and responsible solutions for diverse applications [60], spanning from border security to digital identity management.

Author(s)	Title	Key Contributions
[61]	Explainable Deep Learning for Efficient and Robust Pattern Recognition	Proposed a deep learning approach for pattern recognition with enhanced interpretability and robustness.
[62]	Towards Interpretable and Trustworthy Face Recognition	Developed methods to improve interpretability and trustworthiness in face recognition systems.
[63]	DeepExplain: Explainable Face Recognition via Spatial Attention	Introduced a spatial attention mechanism to make face recognition systems more explainable.
[64]	Explainable Face Recognition: A Survey	Provided a comprehensive survey on various methods and approaches for explainable face recognition.
[65]	Interpretable Deep Learning for Face Verification	Proposed interpretable deep learning models specifically for face verification tasks.
[66]	Explainable AI in Face Biometrics: A Review	Reviewed the existing literature on explainable AI in face biometrics, highlighting key methods and future directions.
[67]	Enhancing Explainability in Face Recognition Systems	Explored techniques to enhance the explainability of face recognition systems.
[68]	Transparent Face Recognition with Visual Explanations	Developed a face recognition system that provides visual explanations to enhance transparency.

Continued on next page

Table 2.3 – continued from previous page

References	Title	Key Contributions
[69]	XFace: An Explainable Face Recognition Framework	Introduced the XFace framework, focusing on making face recognition models explainable.

Table 2.3: The most popular works that propose explainable biometric systems for face modality

2.5.2 Fkp-based Explainable Biometric Systems

Explainable biometric systems utilizing the Finger-Knuckle Print (FKP) modality are becoming increasingly significant due to their provision of transparency and interpretability within decision-making frameworks, which are essential for fostering user trust and ensuring the dependability of the system. Contemporary investigations have concentrated on formulating methodologies that not only augment recognition precision but also deliver coherent rationalizations for the decisions rendered by the system. For example, certain research endeavors have incorporated deep learning architectures, such as convolutional neural networks (CNNs), in conjunction with explainable artificial intelligence (XAI) methodologies including Layer-wise Relevance Propagation (LRP) and Grad-CAM, to elucidate the regions of FKP images that predominantly influence recognition outcomes. These strategies facilitate the discernment of critical attributes and patterns upon which the model operates, thereby simplifying the process of comprehending and validating the determinations made by the biometric system. The amalgamation of explainable AI within FKP-oriented biometric frameworks seeks to mitigate apprehensions pertaining to algorithmic bias, bolster user acceptance, and enhance overall system accountability.

Authors	Year	Methodology	Key Contributions
[41]	2018	CNN with Explainable AI techniques	Explored the use of CNNs for automatic feature extraction in FKP, incorporating explainability through Layer-wise Relevance Propagation (LRP) to identify key areas contributing to decisions.
[42].	2020	Hybrid Deep Learning Framework	Combined CNNs with Recurrent Neural Networks (RNNs) for capturing spatial and temporal dynamics in FKP images, enhancing both accuracy and explainability through Grad-CAM visualizations.
[43].	2022	Preprocessing Techniques and Adaptive Classifiers	Focused on improving the robustness of FKP recognition against noise and distortion, with an emphasis on developing explainable preprocessing methods that clarify how variations are handled.
[70]	2021	Explainable Deep Learning with Synthetic Data	Proposed an explainable deep learning approach using synthetic FKP data to reduce bias and improve interpretability of the system's decisions.
[71]	2019	Statistical Analysis and Explainability	Analyzed the impact of dataset bias on FKP recognition and utilized statistical methods to improve explainability and fairness in decision-making processes.

Table 2.4: Recent and Popular Works in Explainable FKP-Based Biometric Systems

2.6 Conclusion

The advancement of biometric systems has shifted from basic fingerprint techniques to integrated multimodel systems, including facial recognition and Finger-Knuckle Print (FKP). This chapter has delineated the historical development of biometric identification, illustrating the

foundational role of traditional methods in the emergence of advanced techniques.

The examination of explainable biometrics has highlighted the increasing importance of transparency and interpretability in system development, responding to the essential demand for trust and accountability in security contexts. By analyzing face and FKP modalities, this chapter has demonstrated that these technologies not only improve accuracy but also enhance explainable decision-making processes.

As biometric systems progress, the integration of traditional and modern techniques presents opportunities for creating comprehensive, inclusive, and interpretable solutions. This establishes a framework for future inquiries, wherein the amalgamation of multimodel biometrics and artificial intelligence may transform security standards across diverse sectors.

Chapter 3

Theorical background about biometric systems

3.1 Introduction

Biometric, is the action of analyzing and measuring the unique characteristics of the individual (physical or behavioral) with the goal of identifying or verifying the identity of the individual in different domains of application, thus **Biometric system** refers to the technology of identifying and verifying the identity of the user based on their specific physical or behavioral unique characteristics called *Biometric Traits* .in this chapter we will provide a general definition of the principal theoretical concepts of biometric

3.2 brief history of biometric system

The biometric system has existed for thousands of years ago in a very old form of identification, In old Egyptian and Chinese civilizations, physical characteristics such as footprints and handprints have been used as primitive techniques of identification, particularly in the administrative domains. Later in the 19th century, the concept of ”anthropometry” was introduced by the French police officer Alphonse Bertillon as the first scientific approach that used the body dimension measurement for identification. In the early 20th century Sir Francis Galton’s

work emerged as a foundation of the first fingerprint recognition systems that have been rapidly adopted by law-enforcement agencies which led to the establishment of fingerprint databases to be used for criminal identification. Automated fingerprint identification systems (AFIS) appeared then in the later half of the 20th century reflecting the significant advancement in the field of biometrics.By means of the adoption of a computer-based system, AFIS had the ability of matching the fingerprint against large databases.In Time with the adoption of other modalities: iris, face, voice hand geometry..etc in different domains of application, international organizations such as IOS have established some Standardization and Regulations for the secure and private use of biometric data. The appearance of IA and technological sensors in the recent decade has led to the integration of biometric systems in information technology enabling more accurate biometric systems, thus the adoption of biometric identification in smartphones, social media access, and in the majority of consumer devices. biometric systems are continuously developing with technological advancement, recent research is focusing on the ”contactless biometric solution” with the goal of integrating it with the emerging technologies of blockchain and Internet of things (IOT).

3.3 Principal of Biometric Recognition

3.3.1 Principal Fundamental

- Uniqueness: The concept of uniqueness is the key of biometrics, it ensures the high distinctiveness of a person among a population based on its physical or behavioral traits since no two persons can possess the same and identical biometric characteristics, in other words, each person possess unique characteristics which can be physical or behavioral distinguishing him form other persons. the concept uniqueness in the fundamental concept of biometric recognition since it enables the biometric system to distinguish the user from all other users accurately as a result the biometric system can insure a high accuracy in both identification and verification mode witch is the main goal of biometrics. Overall , uniqueness insure a reliable biometric authentication with a strong level of security.

It should be notable that however biometric characteristics are highly unique but it still has a rare possibility that two individuals possess the same characteristics;as instance the identical twins in the face trait; in this case biometrics still has the possibility of insuring uniqueness by using a multi-model biometric systems that combine two or more biometric traits to enhance accuracy.

- Universality: One of the fundamental principles of biometrics denotes that the biometric characteristics are present in every individual across the world, if we take the example of fingerprint we can say that the fingerprint trait is universal because every person possesses a fingerprint, regardless of demographic factors of aging or health cases. universality is a principal condition for a biometric system's adoption, reliability and applicability it can ensure the widespread of biometric system and the effective deployment in all the domains of application. Universality is also crucial for biometric system's accessibility since biometric technologies are designed to be used by all population including individuals with special needs, the principal idea of universality ensure a high equability and accessibility for biometric authentication methods.

- Permanence: A crucial concept in biometric refers to the stability of the individual's biometric characteristics over time,therefore, the characteristic used in the biometric authentication process should stay reliable and relatively unchangeable Eventually in order to insure the persistence, long-term usability and the enduring reliability of the biometric system, as a result , it can be used for an extended period of time with stable accuracy witch ensure a high usability and applicability of the biometric system in a largest and more various domains of application. It should be highlighted that some barometric trait can stay unchangeable over time such as fingerprint but other are relatively stable and can be influenced by the factor of aging or cosmetic surgery such as face features, in this case the biometric system design should flexible to propose a solution of "up-to-date" possibility in order top ensure a long term usability and a high effectiveness of the system.

- Collectability: An important concept for the conception and implementation of the bio-

metric system signifies the easiness of data collection from the users for biometric system design an implementation, different factors are considered in data collection process including accessibility to the process of collection even for those who have disabilities or special needs, non-invasiveness since the collection process should not cause any discomfort for the individual providing the information and finally compliance with the private information of the individual. Overall, collectability can improve the data quality and increase the user acceptance against the system as a result insuring a large adoption of the system in different domain of application.

3.3.2 Types of Biometric systems

Multi-model Biometric

Utilizing a variety of biometric traits, multimodel biometric systems aim to authenticate or recognize an individual. These systems amalgamate two or more forms of biometric inputs, such as fingerprints, facial recognition, iris scans, voice patterns, etc., in order to bolster security and precision. By amalgamating multiple biometric traits, the system can diminish false acceptance and rejection rates, thereby elevating the overall accuracy significantly. Furthermore, the utilization of multiple biometric traits enhances security by making it more challenging for unauthorized individuals to trick the system, as they would need to falsify multiple types of data simultaneously. Moreover, multimodel systems exhibit robustness in diverse environments and conditions, as the failure or suboptimal performance of one modality can be compensated for by another. Additionally, users are provided with the flexibility to select from various biometric traits, rendering the system more user-friendly and adaptable to different preferences and scenarios. However, the implementation and maintenance of multimodel systems can be intricate and costly due to the necessity for multiple sensors and integration mechanisms. Moreover, the combination and processing of multiple biometric traits can prolong the time required for recognition, potentially impacting the user experience. Furthermore, the storage and management of multiple biometric data types demand more storage space and sophisticated data management techniques.

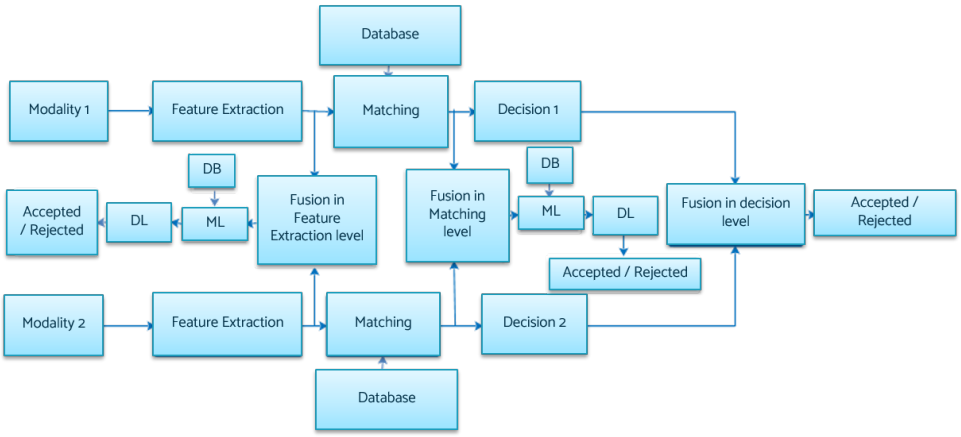


Figure 3.1: Architecture of Multimodel Biometric System

Unimodel Biometric System

unimodel biometric systems utilize a singular biometric trait for verification or identification purposes. These systems rely on a single type of biometric input, such as a fingerprint, facial recognition, or voice pattern. unimodel systems are characterized by their simplicity in design, implementation, and maintenance, which renders them cost-effective and easier to handle. Additionally, recognition processes in unimodel systems are typically swifter since they only need to process a single type of biometric data. Furthermore, users may perceive unimodel systems as less intrusive and more straightforward to use, given that only one type of biometric trait is involved. Nevertheless, unimodel systems may exhibit higher false acceptance and rejection rates compared to multimodel systems, particularly if the chosen biometric trait lacks distinctiveness. Additionally, these systems may be more vulnerable to spoofing and other security breaches since they rely solely on a single type of biometric data. Moreover, unimodel systems might underperform in specific environmental conditions, for instance, facial recognition might be affected by lighting, and voice recognition by background noise. Furthermore, some users may encounter challenges in enrolling in unimodel systems due to specific physical or environmental conditions impacting the chosen biometric trait.

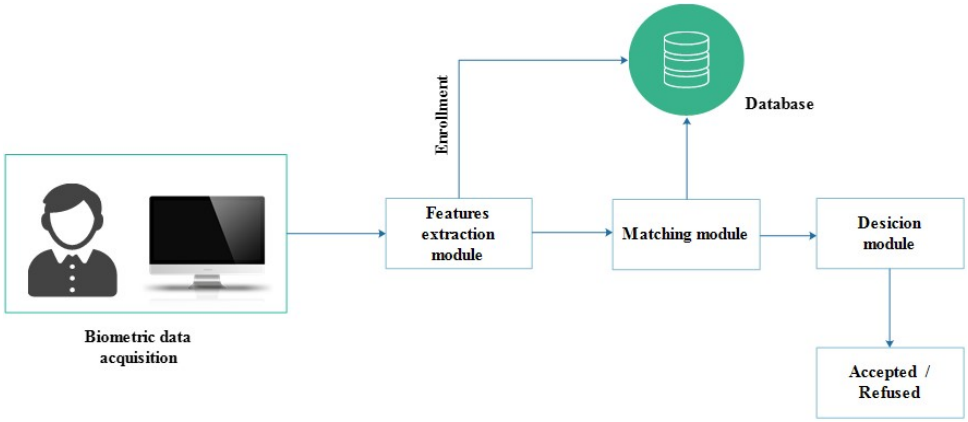


Figure 3.2: Architecture of Unimodel Biometric System

Comparison of multimodel and unimodel biometric systems

The selection between multimodel and unimodel biometric systems is contingent upon the specific requirements and limitations of the application. While multimodel systems offer heightened security and accuracy, they are accompanied by increased complexity and cost. On the other hand, unimodel systems are simpler and faster but may have constraints in terms of accuracy and robustness.

Criteria	multimodel Biometric Systems	unimodel Biometric Systems
Definition	Use multiple biometric traits (e.g., fingerprint, face, iris)	Use a single biometric trait (e.g., fingerprint)
Accuracy	High, due to combining multiple traits	Moderate to high, depending on the biometric trait
Security	Enhanced, more difficult to spoof multiple traits	Moderate, easier to spoof a single trait
Complexity	High, requires integration of multiple sensors and algorithms	Low, simpler design and implementation
Cost	High, due to multiple sensors and complex infrastructure	Low, fewer sensors and simpler infrastructure
Processing Time	Longer, as it processes multiple biometric traits	Faster, processes only a single biometric trait
Robustness	High, compensates for failure of one trait with another	Moderate, performance may degrade under specific conditions
User Flexibility	High, offers multiple options for users	Low, relies on one type of biometric input
Environmental Sensitivity	Less sensitive, as multiple traits can balance environmental effects	More sensitive, performance can be affected by environmental factors
Data Storage and Management	Complex, requires more storage and advanced management	Simple, requires less storage and management
User Enrollment	Flexible, easier to enroll with multiple options	Can be difficult if the chosen trait is affected by conditions
Use Cases	High-security applications, critical infrastructure	General use, consumer electronics
Scalability	Moderate, can be challenging to scale	High, easier to scale with fewer complexities
User Experience	Can be more intrusive, as it involves multiple scans	Less intrusive, involves a single scan

Table 3.1: Comparison of multimodel and unimodel Biometric Systems

3.4 Importance of biometrics in various applications

Biometric has proven its importance and necessity in different areas including authentication, security and identity management. biometrics solutions are becoming one of the most efficient, reliable, and robust tools for verifying an individual's identity. Security, Identity management, and authentication are the principles axes in which biometrics plays a pivotal role.

- **Security** Biometric authentication has passed to another level of efficiency in the iden-

tity verification process in differents domains of application Leaning of the principal idea of relying of the unique physiological or behavioral characteristics of the individual to confirm or deny the user's access, biometric systems can ensure high security in different contexts such as security buildings or access to sensitives areas also, by denying unauthorized access biometric systems enhance security measurements.

- **Identity Management** The principal role of biometric system is the management of a user's identity since the efficiency and accuracy of the provided biometric systems offer an accurate verification of an individual's identity thus recently biometrics have been applied in different domains such as Border Control, Medical Domain, Low Enforcement, Banking..etc. The uniqueness of traits that biometric systems leans on to identify, verify and authentify the individual's identity make its role pivotal in the organisations by ensuring security, detecting and predicting fraud identity, and making sure only authorized identities can have access to private information thus protecting precious and sensitive data.

- **Authentication** biometrics is considered as a robust and secure method of authentification it protects the digital and physical system against fraud and unauthorized access, Biometric authentication enhances the security and confidentiality of the systems and the data since it uses unique physical or behavioral traits such as fingerprint, voice, iris..etc. Biometric authentication has passed to another level of efficiency in the identity verification process in differents domains of application

3.5 Biometric Traits

Biometric Traits called also Biometric Modalities are the specifics and unique characteristics of the individual that the system leans on to identify or verify the identity of the user, it can be divided into two types: physiological traits and behavioral traits

Physical Traits

A group of physiological characteristics of the individual's body this type of characteristics are stable and unchangeable over time because its directly divided from the anatomical features of the user, it includes:

- **Fingerprint** Is one of the widely used physiological biometric modalities, it represents the specific ridges in the surface of the individual's fingertips, the unique structure of the ridges is stable and remains unchanged throughout time, it is also a high distinctive biometric traits since there no possibility to find two identical fingerprints even among identical twins. The fingerprint modality is relatively preferred for researchers in the domain of biometrics due to its robustness and distinctivity.

- **Iris** Reffers to the colored part of the eye, in the context of biometrics, Iris is seen as the lines, ridges and the unique pattern of the color in the iris of the individual's eye witch is stable within the individual's life time and also high distinctive since there is no identical Iris characteristic even for identical twins. the recognition of the iris's texture, color and pattern requires specialized cameras and scanners to capture the high-resolution image of the iris.

- **Retina** In Biometric "Retina" is defined as blood vessel's unique patterns, the blood vessels are positioned in the back of eye's retina, it is a biometric modality that requires a specialized scanning camera to capture the reflection of low-intensity infrared light into the eye , exactly on the retina, as a result of the scanning process we usualy get an image that represents the complex pattern of the blood vessels of the eye's retina, which is unique and stable over the individual's life. despite its high stability, the Retina is considered as less used modality compared to other biometric traits such as face and fingerprint since it often requires a close distance to the scanning tool.

- **Facial Feature**: A Widely used universal biometric modality, it refers to analyzing the individual's face features to identify or verify the user's identity. it utilizes the position

of facial landmarks such as nose, mouth, eyes..etc which are permanent and highly distinctive for identification in biometric systems. The major advantage of the face feature is the non-intrusiveness since it doesn't require any physical contact in addition to the availability of large databases ready for the researchers. Also, the face feature is considered as "speed"; since time is critical in the domain of biometric systems, a faster scanning process leads directly to a faster recognition and verification process so faster and more accurate results.

- **Hand Geometry**: refers to different hand features such as the hand's length and shape, and the distance between knuckles. In biometric domain Hand geometry is a modality that captures, measures, and analyzes the different hand features for identification and verification purposes

- **Earshape**: Can be defined as the unique characteristic of the person's ear, it is a highly distinctive feature that can be a reliable means of identification and verification. the identification using ear shape includes analyzing: shape, length, edges, ridges, and notches. the process usually starts by scanning the ear and capturing the image, extracting the most relevant features, and creating a digital model of the ear that will be used later for the identification of verification. Despite the big challenges of ear orientation variation and occlusion witch effect directly the accuracy of recognition, the ear shape modality still has several advantages such as uniqueness and non-intrusivity.

- **DNA** The deoxyribonucleic acid (DNA) contains the unique genetic information of the individual, in the biometrics domain DNA traits refer to scanning and analyzing a specific area of DNA sequences to create a model that can be used as a biometric identifier, the DNA traits has several advantages of uniqueness and high distinctively while its the major challenge is related directly to the need of specialized material of analysis.

Bihavioral Traits

The major advantage of behavioral traits is the possibility of capturing and collecting information specifically the information related to the individual's identity without requiring the individual's participation, in addition to the stability over time, compared to the physical trait that can be affected and changed by age or getting old, the behavioral traits can be more reliable.

- **Handwriting Characteristics :** refers to the unique pattern and features in the writing process of the individual, the handwriting characteristics can be analyzed based on different aspects such as the form and size of the individual's letters, the space between letters, words, and lines, the quality of lines or the how smooth are the drawn lines during the writing, the line's thickness and darkness can show the pressure applied in the moment of writing the letters. the extracted feature from the handwriting characteristics can be used in document examination and signature verification it helps experts in identifying individuals and detecting signs of forgery in different domains such as law enforcement and historical research.

- **Mouse Movement :** the specific pattern of an individual's interaction with the pointing device, the principal aspects that form the pattern are the timing, precision, direction, and acceleration of the movement based on these pattern algorithms can generate a unique and distinctive behavioral profile, mouse movement offers the advantage of continuous authentication where the risk of unauthorized access and fraud is high including online banking and e-commerce transactions.

- **Signature Dynamics** unlike the classical static signature that focuses on shape and form in the analysis process **The signature dynamics** leans on pressure, rhythm, and fluidity in the signature process In other words it analyses the dynamic aspect of an individual's signature and extract the characteristic and the pattern from it. the analysis process of signature dynamic is an exact operation that emphasizes the details of how the pen was held, the sequences of writing, the applied pressure on the pen while signing, and all the temporal and spatial activities while signing. As a behavioral biometric trait, signature

dynamics is used widely in fraud detection, authentication, and signature verification. Capturing and analyzing deeply the timing and sequences of the pen movement generates the data that the advanced algorithms can use to create a unique profile of the individual and verify the signature authenticity and forgery tentative later. It generally requires a specialized device to capture the signature dynamics such as touch-sensitive screens.

- **Voice Patterns:** This trait combines the analysis of both physical and behavioral characteristics of an individual vocalization since the physical characteristics include the tract shape and the cord length of the vocal in addition to the lung capacity while the behavioral ones include accent, pronunciation and the rate of speech. overall the voice patterns analyze the different elements of frequency, articulation, pitch, and duration from the speech sample using a sophisticated technique of signal processing and machine learning algorithms to extract the relevant features and build the individual's unique profile to be used for identification and verification later. the voice pattern stays unstable over time it evolves due to aging factors or health condition factors.

- **Typing Patterns:** known also as keystroke dynamics, it refers to the rhythm, speed, and style of typing on a keyboard or touchscreen, the individual's typing pattern, error pattern, and all the variations in typing behavior are analyzed by specific algorithms of high complexity to extract the specialized features and build the biometric profile which will be used later as reference of identification and verification of individuals. keystroke dynamics is used in different domains of application including continuous authentication in computer systems and online transactions.

- **Gait Analysis** The trait of analyzing the individual's walking pattern in order to build its biometric profile, the gait analysis leans on assessing the different bio mechanical characteristics related to gait including movement of limb, length of stride, placement of the foot, the duration of step, and the segment of the body. specific techniques are applied to capture and analyze the individual's gait such as special mats sensitive to pressure and motion capture systems. gait analysis is used in the context of biometric as a unique

biometric traits to identify and verify the identity of the used for the goal of protecting its personal data or denying unauthorised to sensitive area or information.

Biometric Trait	Advantages	Disadvantages
Physiological Traits		
Fingerprint	Uniqueness, universality, and reliability	Potential vulnerability to tampering and counterfeiting
Iris	Reliability, precision, stability, very accurate, and difficult to falsify	Requires specific equipment for capturing the iris image
Retina	Extremely accurate and difficult to falsify, not affected by external factors like lighting	Requires specialized equipment for the retinal image capture, may be seen as intrusive by some users
Facial Feature	Non-intrusive, no direct contact needed, can be used remotely, evolves rapidly with technological advances	Risk of false matches, especially in variable lighting conditions or with changes in hairstyle/beard
Hand Geometry	Easy to collect, not intrusive, can be used in difficult working environments	Less accurate than other biometric modalities, sensitive to changes in weight or hand shape
Ear Shape	Can be collected non-intrusively	Less accurate than other biometric modalities, sensitive to minor changes in ear shape

DNA	Extremely precise and unique to each individual, can be used for forensic and medical applications	Requires a complex collection and analysis process
Behavioral Traits		
Handwriting Characteristics	Can be used for authentication online and offline	Sensitive to changes in writing style due to fatigue or other factors, can be affected by the quality of the writing material and surface used
Mouse Movement	Can be used continuously during normal operation of the computer	Less accurate than other biometric modalities, the natural variation in mouse movement can result in false positives or false negatives
Signature Dynamics	Can capture unique characteristics of the signature process, such as pressure and speed, can be used for real-time authentication	Sensitive to variations in the signature process due to fatigue or other factors, may require more complex data capture than simply capturing a static image of the signature
Voice Patterns	Non-intrusive and easy to use, can be used in noisy environments	Can be affected by environmental conditions such as noise or microphone quality

Typing Patterns	Can be performed without the need for additional sensors or equipment	Typing patterns can be influenced by a variety of factors such as hand injuries, typing fatigue, or changes in typing habits over time, which can affect the accuracy of authentication
Gait Analysis	Can be performed without the need for physical contact or additional equipment, just look at the way individuals walk, difficult to counterfeit	Limited distance: Observing gait patterns from a distance can be challenging, especially in crowded or noisy environments where visual clarity is compromised

Table 3.2: Advantages and Disadvantages of biometric modalities

3.6 Performance Analysis

- Metrics of Accuracy: a quantitative measures used to evaluate the level of performance of the biometric system thus how accurate are decision generated by the system in confirming of denying the user's access, shown in figure 3.3 it includes:
  - FAR: False Acceptance Rate : The measure of accepting the impostor as genuine
  - FRR: False Rejection Rate : The measure of rejecting the genuine as impostor
  - EER: Equal Error Rate : A point of balance at which the FRR and FAR are equals, An EER near to Zero reflect a perfect accuracy as both FRR and FAR are Zero , and An EER near to 100% reflect a low accuracy of the system as FRR and FAR are near to be equals.

– ROC: Receiver Operating Characteristic : A curve that represent the FAR against FRR over various threshold configurations

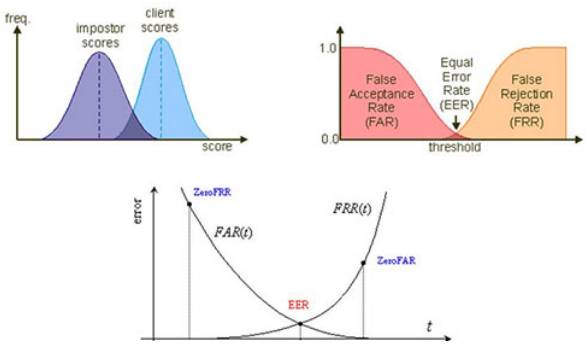


Figure 3.3: Metric used to measure the system's performance

- Reliability Metrics: Measurement used to evaluate the level of consistency of the biometric system's performance aver time and across different criteria, including:

  – FTE: Failure to Enroll Rate: Used to measure the proportion of individuals who attempt to enroll the process of the system unsuccessfully, it is the percentage of balance between the unsuccessful enrolment attempt and the total number of attempts.

  – FTC: Failure to Capture Rate: Used to measure the pourcentage of of individuals who attempt to capture the system unsuccessfully, it is the percentage of balance between the unsuccessful enrolment attempt and the total number of attempts. A metric that measure the proportion of unsuccessful attempt to capture the biometric data by the system, how many times does the system fail to capture a usable information from the user

  – FTA: Failure to Acquire : is a phenomenon within biometric systems wherein the apparatus does not successfully acquire or produce a legitimate biometric sample during the phases of enrollment or authentication. This impedes the system's capacity to finalize the identification or verification procedures.

    Failure to Acquire (FTA) can transpire as a consequence of sensor constraints, environmental variables, or user-related considerations, and it has a direct impact on

the comprehensive performance, usability, and dependability of biometric systems.

- Efficiency Metrics
  - Time of recognition: Denotes the duration required for a recognition system to process input and generate an output. This duration encompasses the entire sequence from input reception to comparison with templates or models, and eventual output generation. The criticality of the time of recognition as a metric lies in its influence on the efficiency of the recognition system. Shorter recognition times are imperative for real-time applications like speech recognition, image recognition, and biometric systems. Streamlining the time of recognition enhances user experience and system efficiency.
  - Throughput : Within the temporal domain of recognition, denotes the pace at which the recognition system can handle incoming data and yield outcomes. This metric is commonly quantified by the number of recognitions or tasks completed within a specific timeframe (e.g., recognitions per second or recognitions per minute). The significance of high throughput lies in the system's capability to efficiently manage a substantial amount of data, a critical requirement for applications necessitating real-time processing or the handling of extensive datasets.
  - Size of Template: Pertains to the quantity of data or the intricacy of the pattern utilized for recognition. In systems reliant on templates for recognition, a template serves as a predetermined pattern or model for matching and identifying input data. The importance of the template's size is profound as it can notably impact the recognition duration. Larger or more intricate templates may demand increased computational resources and processing time, while smaller or simpler templates can expedite the process. Striking a balance between template size, desired precision, and speed of recognition is paramount for enhancing performance.

In synthesis, throughput gauges the quantity of recognitions achievable within a specific timeframe, the size of the template impacts complexity and processing time, and the time

of recognition represents the actual duration for input recognition. Striking a harmonious equilibrium among these aspects is fundamental for optimizing the efficiency of recognition systems.

3.7 Conclusion

This chapter has established a foundational comprehension of biometric systems, elucidating the fundamental principles, primary modalities, and underlying theoretical constructs that facilitate their functionality. By examining the physiological and behavioral characteristics employed for identification and authentication, we have underscored the advantages and constraints associated with diverse biometric methodologies.

The discourse has underscored the significance of uniqueness, permanence, and universality in the selection of biometric traits, while concurrently addressing the challenges introduced by environmental variables, the aging process, and susceptibility to spoofing attacks. This theoretical foundation serves as an essential precursor to comprehending the advancements and applications that will be examined in the following chapters.

As biometric technology continues to progress, this theoretical framework provides a perspective through which emerging trends and innovations can be evaluated, thereby fostering a more profound appreciation of the intricacies and potentialities inherent in contemporary biometric systems.

Chapter 4

Methods and Tools

4.1 Introduction

This chapter elucidates the principal methodologies and instruments employed in the development and assessment of biometric systems. It encompasses the strategies for data acquisition, preprocessing, feature extraction, and performance evaluation, thereby ensuring both accuracy and reliability.

The choice of tools and algorithms is of paramount importance in constructing efficient and interpretable biometric models. This chapter establishes the foundational framework for the experimental investigations and outcomes that are elaborated upon in the subsequent sections.

4.2 Pre-Processing

The preprocessing stage within biometric systems comprises multiple procedures aimed at readying raw biometric data for subsequent analysis. An in-depth examination of the typical occurrences during this phase is presented here: Initially, biometric data is acquired by retrieving data from the appropriate sensor. This process may encompass gathering fingerprints through a fingerprint scanner, capturing facial images using a camera, recording voice samples via a microphone, and so forth.Rectification of flaws within the raw biometric data is necessary, as it may harbor imperfections or artifacts stemming from factors like brightness, blurring, or noise. Im-

age correction methods are then implemented to enhance the quality of the data. Standardization of biometric data is carried out to align it with future processing systems. This procedure may involve activities such as scaling, rotating, cropping, and other adjustments to ensure uniformity in the data. Subsequent to preprocessing and standardization, pertinent features are extracted to effectively and concisely represent the biometric information. For instance, minutiae like bifurcations and endings can be extracted in the case of fingerprints. Filtering procedures and dimensionality reduction techniques may be employed in certain scenarios to eliminate noise or redundant data. Principal component analysis (PCA) is an example of a technique used for reducing data dimensionality while preserving crucial information. Statistical normalization of biometric data is conducted to enable a fair and precise comparison between different samples. This may involve normalizing the mean and standard deviation of the extracted features. To sum up, the preprocessing phase in biometric systems is crucial for priming raw data for subsequent analysis. It encompasses rectifying imperfections, standardization, feature extraction, filtering and dimensionality reduction, as well as statistical normalization to ensure precise and dependable outcomes in biometric applications.

4.2.1 FKP Pre-Preprocessing Techniques

- Image Acquisition:

  The acquisition of images involves using high-resolution cameras or sensors to capture clear images of the finger knuckle. To ensure high-quality image capture, consistent lighting conditions are maintained to avoid shadows and reflections.

- Noise Reduction:

  To reduce noise in the images, Gaussian Filtering is used to smooth the image while preserving edges. Additionally, Median Filtering effectively removes salt-and-pepper noise by replacing each pixel's value with the median value of neighboring pixels.

- Contrast Enhancement:

  For enhancing contrast, Histogram Equalization adjusts the contrast by spreading out the

most frequent intensity values in the image. Another technique, Adaptive Histogram Equalization, enhances contrast locally within small regions of the image.

- Region of Interest (ROI) Extraction:

  The extraction of the region of interest involves using algorithms like Sobel, Prewitt, or Canny for edge detection to isolate the knuckle area. Morphological operations such as dilation and erosion refine the detected edges and remove small artifacts.

- Alignment and Normalization:

  Alignment and normalization techniques include Affine Transformations to correct rotations, translations, or scaling in the FKP images. Size Normalization resizes the extracted ROI to a standard dimension for uniformity across all images.

- Feature Enhancement:

  Gabor Filters are applied to enhance ridge and valley structures in the knuckle print by emphasizing specific frequency and orientation characteristics. Local Binary Patterns (LBP) capture texture information by encoding local texture patterns around each pixel.

- Binarization:

  Binarization involves thresholding to convert the grayscale image into a binary image, simplifying the image for further processing where ridges are represented by white pixels and valleys by black pixels.

- Skeletonization:

  Thinning algorithms reduce binary ridge patterns to a one-pixel-wide skeleton, preserving essential structural information of the FKP.

- ROI Enhancement:

  Smoothing and sharpening techniques may be applied to further enhance the clarity of ridges and valleys in the ROI. Additionally, edge enhancement techniques like unsharp

masking or gradient-based methods can be used to enhance prominent features in the knuckle print.

- Geometric Normalization:

  Geometric normalization ensures that the aspect ratio and orientation of knuckle print features are consistent, facilitating more accurate feature matching in subsequent stages.

By systematically applying these pre-processing techniques, the quality of FKP images is significantly improved, resulting in more reliable feature extraction and higher accuracy in biometric recognition. Each technique addresses specific challenges such as noise, contrast, and alignment to ensure accurate representation of FKP patterns.

4.2.2 Face Preprocessing Techniques

The approaches relying on image processing methodologies to address illumination challenges typically aim to standardize all facial images to a reference illumination for the purpose of conducting comparisons under consistent lighting conditions. These approaches are often conceptualized in a standardized manner:

$$I = T(I) \tag{4.1}$$

$'I'$ represents the original image, while T denotes the transformation operator leading to the creation of I'. The application of the transform T aims to mitigate the adverse impact of inconsistent illumination, resulting in the production of image I' which can serve as a standardized representation in a facial recognition framework.Consequently, the facial recognition system is anticipated to exhibit resilience towards changes in lighting conditions.

Histogram Equalization (HE)

Histogram Equalization stands out as a widely employed approach in the realm of preprocessing. Within the domain of image manipulation, the notion of balancing a histogram involves expanding and rearranging the initial histogram across the complete spectrum of discrete levels

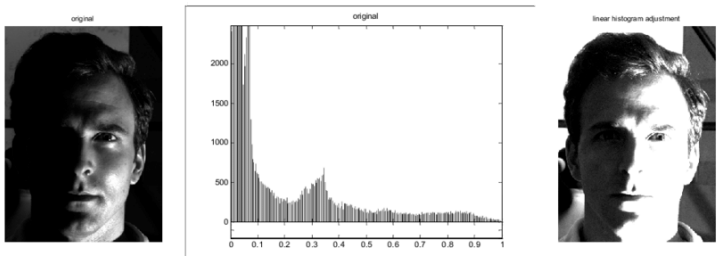


Figure 4.1: Linear histogram equalization is implemented from the left side to the right side

within the image, resulting in a heightened contrast. The prevalent technique for histogram normalization is histogram equalization, where the aim is to transform the image's histogram into a uniform distribution for all brightness values. This transformation would create a scenario where each brightness value holds an equal likelihood. For an image $I(x, y)$ with k discrete gray values, the histogram is characterized by the probability of each gray level i occurring.

$$p(i) = \frac{n_i}{N} \tag{4.2}$$

where i belongs to the set $\{0, 1, \ldots, k-1\}$ of grey levels.and N represents the entirety of pixels in the image, there exists a profound metamorphosis to a fresh level of intensity. This transformation is defined as:

$$I_{\text{out}} = \sum_{i=0}^{k-1} \frac{n_i}{N} = \sum_{i=0}^{k-1} p(i) \tag{4.3}$$

The output values are derived from the domain of [0, 1]. In order to convert these pixel values back to their original domain, they need to be rescaled by the reciprocal of K. The histogram equalization is illustrated in 4.1.

The logarithmic transform

The logarithmic transform, often abbreviated as LOG, is a commonly employed technique for grayscale image enhancement. It emulates the logarithmic response of the human eye to changes in light intensity. While LOG proves effective in addressing lighting inconsistencies across certain datasets, its application significantly reduces recognition rates in other subsets of the CAS-PEAL database. One potential explanation for this disparity could be the substantial variation in mean brightness values among transformed images of the same individual. The utilization

of the logarithmic transformation in grayscale image processing is a frequently employed technique. This method serves the purpose of enhancing the contrast within an image, especially in cases where the distribution of pixel values is skewed towards lower intensities.

Typically, in grayscale image processing, pixel values span from 0 to 255, with 0 denoting black and 255 representing white. Nevertheless, instances occur where pixel values tend to cluster towards the lower end of this range, resulting in images with diminished contrast.

The logarithmic transformation involves the application of a logarithmic function to the pixel values, thereby expanding lower intensity values and compressing higher intensity values. This action facilitates the dispersion of pixel values over a broader spectrum, consequently augmenting the overall contrast of the image.

The logarithmic transformation function is generally put into effect on each pixel p within the image, following a specific formula:

$$P = clog(1 + p) \tag{4.4}$$

Here: P: Refers to the output pixel value p: refers to the original intensity value of the pixel. c: stands as a constant that dictates the potency of the transformation (often determined through empirical means). log: signifies the natural logarithm function.

Through the implementation of this transformation, dimmer areas of the image are accentuated more than brighter regions, thereby enhancing the visibility of intricate details, particularly within shadowed sections. Nevertheless, it is imperative to acknowledge that while the logarithmic transformation can heighten image contrast, it may also introduce artifacts or amplify noise within the image, especially in areas characterized by extremely low pixel values. Consequently, a prudent approach entails the judicious use of this technique in conjunction with other methods to achieve optimal outcomes.

Spectral Quality Index

SQI is established on the reflectance-illumination model:$I = RL$, in which I represents the image, R stands for the reflectance of the scene, and L represents the lighting. The lighting

component L can be viewed as the low-frequency element of the image I and can be approximated by means of a low-pass filter F, indicating $L\ F * I$. Consequently, the self-quotient image can be obtained as

$$R = \frac{I}{F * I} \tag{4.5}$$

This technique employs a weighted Gaussian filter that interacts with solely the larger parts within edge areas, thereby leading to a reduction in halo effects. In cases where there exist significant lighting fluctuations (as observed in the "illum" subset of the CMU-PIE database), the edges generated by lighting effects become conspicuous and this approach proves to be effective. Nonetheless, in scenarios where lighting variations are less pronounced, the primary edges are produced by the facial attributes. The continued use of this type of filter under such circumstances would result in a diminishment of the pertinent information required for accurate recognition.

Gamma Correction

Gamma correction is a non-linear operation utilized to modify the luminance of pixels within an image through altering the correlation between input and output luminance levels. This adjustment is commonly expressed mathematically with the equation:

$$P_{out} = P_{in}^{\gamma} \tag{4.6}$$

Where: P_out is the luminance of the output pixel post-gamma correction.
P_in is the luminance of the input pixel pre-gamma correction.
γ represents the gamma parameter that governs the configuration of the gamma correction curve.

The formula illustrates that the luminance value of the output pixel (P_{out}) is derived from raising the luminance value of the input pixel (P_{in}) to the power of γ. A higher γ value results in a more significant transformation, thereby impacting the expansion or compression of luminance levels.

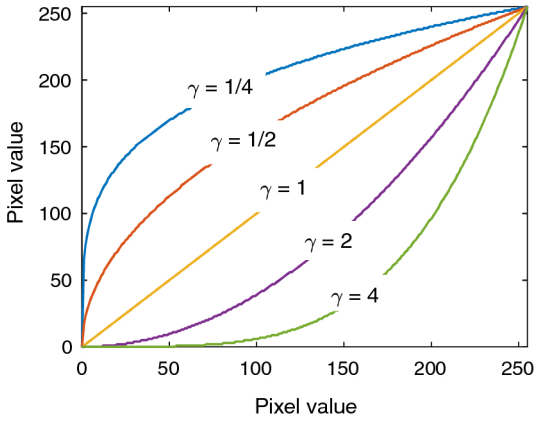


Figure 4.2: Gamma correction curve for different values of γ

Gamma correction is frequently employed to enhance the luminance and disparity of images, particularly when exhibited on screens or reproduced on media with non-linear response traits. It enables the attainment of outcomes that are aesthetically more harmonized and in accordance with human perception of luminance. The gamma correction curve demonstrates the transformation of input pixel intensity values to output pixel intensity values through a nonlinear function, as defined by a specific equation. In cases where $\gamma = 1$, the curve exhibits linearity, signifying the absence of any correction. Conversely, when $\gamma < 1$, the curve becomes concave, enhancing low intensity values and brightening the resulting image; whereas for $\gamma > 1$, the curve turns convex, compressing high intensity values and darkening the image. As mentioned before, Gamma correction serves the purpose of adjusting the brightness and contrast levels in digital images, rectifying non-linearities present in display devices, and enhancing visual perception by taking into account the non-linear response of the human eye. Its practical applications span across various fields such as image processing, video display, digital photography, and medical imaging.

Gamma Intensity Correction

Gamma Intensity Correction (GIC) is a method employed for adjusting the intensity values of an image based on the concept of gamma correction. This approach is utilized to rectify the non-linear luminance response of display devices or to enhance the visual perception by adjusting the contrast and brightness of images.It alters the intensity values of an image through

the utilization of a gamma correction curve. The primary objective of GIC is to rectify any discrepancies between the brightness of the captured or displayed image and the way the human eye perceives brightness. The formula for gamma correction utilized in GIC is as follows:

$$P_{out} = P_{in}^{\gamma} \tag{4.7}$$

Where: P_{out} is the intensity output post gamma correction.

P_{in} is the intensity input pre-gamma correction.

γ represents the gamma parameter that governs the configuration of the gamma correction curve.

Operation

The GIC has a process of three principal steps :

- Non-linear Adjustment: The gamma correction curve exhibits non-linear characteristics, leading to differential adjustments for low and high intensity values. Typically, a gamma value exceeding 1 results in a darker image, whereas a gamma value less than 1 results in a brighter image.
- Human Perception: Brightness is perceived by the human eye in a non-linear fashion, with a higher sensitivity to changes in dark tones compared to light tones. Gamma correction addresses this by aligning image intensity values to better correspond to human vision.
- Calibration of Display Devices: Numerous display devices such as monitors and televisions do not exhibit a linear response to input signals. Gamma correction assists in calibrating these devices to ensure that the displayed image remains consistent with the original scene.

GIC is apllied in various domains such as image Processing for Enhancing the contrast and brightness of digital images. Ensuring that rendered images appear natural on a variety of display devices in Computer Graphics, also it helps in Adjusting images to guarantee accurate representation on different viewing platforms and Maintaining consistent brightness and contrast in videos across various screens and projectors in Photography and Video Treatment.

4.3 Feature Extraction

Pattern detection and recognition play a crucial role in various signal and image processing tasks, such as face recognition, text analysis, and image classification. The centerpiece of these procedures is the vital process of feature extraction. Feature extraction involves converting raw data into more concise and informative representations that are valuable for tasks like classification and clustering.

The feature extraction section delves into the different methods used to extract and pinpoint pertinent information from raw data. This stage is pivotal as it influences the quality and efficiency of machine learning and artificial intelligence models utilized in subsequent applications. Effective feature extraction can notably enhance model performance by decreasing data dimensionality while preserving crucial information.

We are commencing with an overview of the basic principles of feature extraction, including essential definitions and the significance of this process in data processing. Subsequently, we will explore diverse feature extraction techniques, ranging from traditional methods based on statistics and signal analysis to contemporary approaches using neural networks and deep learning.

4.3.1 Gabor Filter Bank

Gabor filters are a powerful and widely used tool in image processing and computer vision, especially for texture analysis and feature extraction. They are named after Dennis Gabor, who introduced the concept of using sinusoidal functions modulated by a Gaussian for signal analysis. These filters are able to capture both spatial and frequency information, making them very effective for various applications.

Characteristics of the Gabor Filters

- Spatial and Frequency Representation: Gabor filters are designed to analyze the spatial frequency content of an image. They can be tuned to specific frequencies and orientations, allowing for multi-scale and multi-orientation analysis.

- Gaussian Modulation: The plane sine wave (a cosine function) is modulated by a Gaussian envelope. This modulation helps locate the filter in the spatial and frequency domains.
- Orientation and Scale: Gabor filters can be applied to different orientations and scales, making them versatile for capturing features such as edges, textures and patterns that depend on orientation and scale.

The Gabor Filter Bank descriptor is shown as a Gaussian envelope modulated by a sinusoidal plane wave. The following equations depict the filter defined in the spatial domain.

$$\psi(X,Y) = \frac{f_u^2}{\pi k \eta} \exp\left(\frac{f_u^2}{k^2} X'^2 + \frac{f_u^2}{\eta^2} Y'^2\right) \exp\left(j 2\pi f_u X'\right) \tag{4.8}$$

$$X' = X \cos\theta_v + Y \sin\theta_v \tag{4.9}$$

$$Y' = -X \sin\theta_v + Y \cos\theta_v \tag{4.10}$$

$$f_u = \frac{f_{\text{MAX}}}{2^{(u/2)}} \tag{4.11}$$

$$\theta_v = \frac{v\pi}{8} \tag{4.12}$$

where f_u represents the central frequency, θ_v denotes the orientation, and k and η represent the ratio between the size of the Gaussian envelope and the central frequency. In the standard scenario, the parameters are initially set as$k = \eta = \sqrt{2}$ and$f_M AX = 0.25$. The number of banks containing filter scales and orientations can be predefined by developers according to their requirements. In our works, to extract multi-orientation and multi-scale features from the input facial image, we set the parameters with five scales ($u = 0, 1, ..4$) and eight orientations ($v = 0, 2, .., 7$) shown in figure 4.3 , which are widely accepted values. Therefore, the process of feature extraction can be described as:

$$G_{u,v}(X,Y) = I(X,Y) * \psi(X,Y) \tag{4.13}$$

The symbol$G_{u,v}(X,Y)$ is used to signify the intricate filtering result.

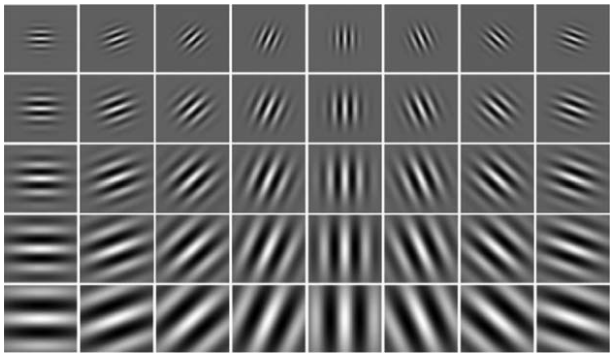


Figure 4.3: Gabor Filters with five scales and eight orientation

4.3.2 Binary Similarity and Intensity Feature (BISIF) descriptor

The Binary Similarity and Intensity Feature (BISIF) descriptor is an advanced method used in image processing to extract distinctive features from images. This descriptor combines binary similarity and pixel intensity information, providing a robust representation of textures and patterns in an image. Binary similarity is a measurement that compares neighboring pixels in an image to determine whether their intensity values are similar or different. This binary comparison is performed on each pixel by looking at its neighboring pixels and assigning binary values (0 or 1) depending on whether they are similar or not. This step helps capture the local patterns and fine textures present in the image. Pixel intensity, on the other hand, is a direct measure of the brightness or color of a pixel. The BISIF descriptor takes into account not only binary similarity but also absolute intensity values of the pixels. By combining these two types of information, BISIF can represent both the fine variations in texture and the more global changes in intensity in an image. The calculation of the BISIF descriptor takes place in several steps: extraction of local patches, binary coding of similarities, combination with pixel intensities, and formation of a global feature vector representing the entire image. This detailed approach allows to extract rich and discriminative information from the images. The Main process of BISIF can be summerized in equation 4.4

$$\text{BISIF} = \sum_{i,j} \left(B_{ij} \cdot I_{ij} \right) \tag{4.14}$$

Where

B_{ij}: refers to The similarity of the pixels at positions i and j can be described as binary. It is

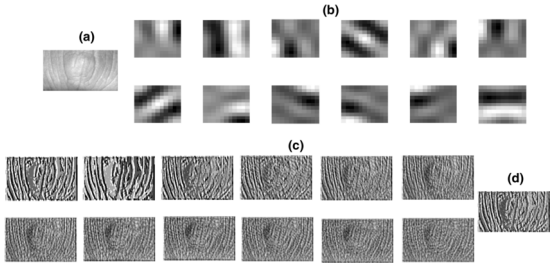


Figure 4.4: (a): Sample of the FKP ROI image, (b): BSIF filter with a size 11 × 11 and of length 12, (c): BSIF features (d): final BSIF

considered as 1 when the pixels are alike, and 0 when they are not.

I_{ij} : refers to the intensity value of the pixel at position i and/or j. This could be a mean or another calculation based on the intensities of the two pixels.

The BISIF descriptor is used in various computer vision applications, including face recognition, texture analysis, and object detection. In face recognition, BISIF effectively captures fine textures and intensity variations, allowing different faces to be distinguished. For texture analysis, BISIF offers a rich representation that helps classify or segment images based on their textures. In object detection, the combination of binary similarity and intensity is used to identify objects under various lighting and noise conditions. The BISIF descriptor has several advantages, such as robustness to lighting and noise variations, as well as good discrimination of fine textures. However, the calculation of BISIF can be complex and resource intensive, requiring optimization for real-time applications. In summary, the BISIF descriptor is a powerful method for extracting image features by combining binary similarity and intensity information, making it a valuable tool in the field of computer vision.In figure4.4 a sample of image to each BSIF was used to extract the relevant features.

4.4 Dimensionality Reduction (PCA,LDA and t-SNE)

The main goal of feature extraction is to decrease the number of variables considered, a process known as dimensionality reduction. Dealing with high-dimensional data can be difficult due to the curse of dimensionality, where the feature space volume grows exponentially with dimensions, resulting in sparse data. Techniques like Principal Component Analysis (PCA), Linear

Discriminant Analysis (LDA), and t-Distributed Stochastic Neighbor Embedding (t-SNE) are commonly utilized to reduce dimensionality by identifying the most significant features that capture the majority of the data's variability.

4.4.1 Principal Component Analysis

PCA, also known as Principal Component Analysis (PCA) [72], serves as a technique for reducing dimensionality in data analysis and machine learning. The primary goal of PCA is to convert a set of potentially correlated data into a fresh set of uncorrelated variables known as principal components. These components capture most of the variance found in the original data while decreasing the number of dimensions. The process of PCA comprises multiple steps: Initially, the data is standardized to ensure each variable has a mean of zero and a variance of one. Next, the covariance matrix of the standardized data is computed to reveal the correlations among the variables. Subsequently, the eigenvalues and eigenvectors of this matrix are identified, with the eigenvalues indicating the variance explained by each eigenvector. The eigenvectors that correspond to the largest eigenvalues are chosen to create the new dimensions or principal components. It can be resumed in the following equation 4.15 , The centered data matrix, denoted as X, has each column representing a variable and each row representing an observation. The covariance matrix C is defined as follows

$$\mathbf{C} = \frac{1}{n-1}\mathbf{X}^T\mathbf{X} \tag{4.15}$$

$$Y = XV \tag{4.16}$$

First, we compute the eigenvalues λ_i and the eigenvectors v_i of the matrix C. The new projected data Y is then obtained by equation 4.16 . Alternatively, V is the matrix that consists of eigenvectors corresponding to the k largest eigenvalues, where k represents the desired number of dimensions. Lastly, the original data is projected onto these eigenvectors to acquire the new data coordinates in principal component space as shown in figure 4.5 . PCA finds widespread

application in various fields such as shape and face recognition, genetic data analysis, data compression, and data mining. It aids in simplifying models, visualizing complex data, and enhancing data quality by eliminating noise.

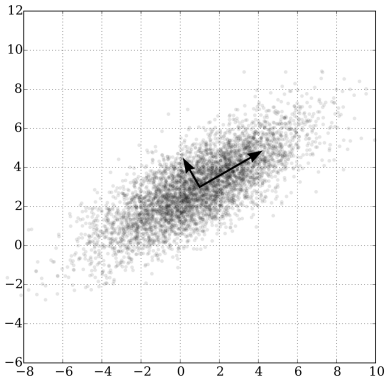


Figure 4.5: Principal Component Analysis (PCA)

4.4.2 Linear Discriminant Analysis

Linear Discriminant Analysis (LDA) is a statistical technique employed for both classification and reducing dimensionality. It proves especially valuable in the realms of machine learning and pattern recognition. The primary objective of LDA involves identifying a linear combination of features that effectively separates various classes of objects or events. This is achieved by maximizing the variance between classes and minimizing the variance within classes. The process commences with computing the mean vectors for each class, followed by determining the intra-class (which gauges variance within each class) and inter-class (which gauges variance between classes) dispersion matrices. Subsequently, the task revolves around solving for the eigenvalues and eigenvectors of the matrix derived from the inverse product of the intra-class and inter-class dispersion matrices. The eigenvectors linked to the largest eigenvalues are chosen to construct a transformation matrix that projects the original data into a new, reduced-dimensional space. This transformation retains most of the crucial discriminating details.Linear Discriminant Analysis (LDA) is a statistical method utilized for both classification and dimensionality reduction as

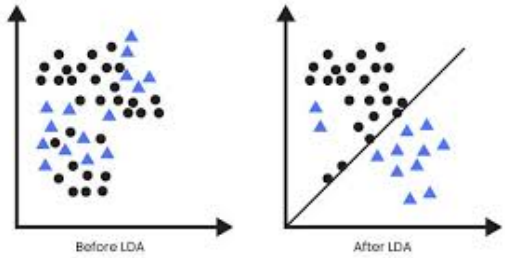


Figure 4.6: Linear Discriminant Analysis (LDA)

shown in figure 2.1. WhenLda it comes to dimensionality reduction, LDA focuses on mapping data to a lower-dimensional space while enhancing the distinction between classes, applicable in different scenarios. It works principally as follow :

- **Calculation of Average Class Vectors**: The initial stage involves computing the average vectors for every class. For a class k, the average vector is determined in the following manner:

$$\mathbf{m}_k = \frac{1}{N_k} \sum_{\mathbf{X} \in C_k} \mathbf{X} \tag{4.17}$$

  The variable N_k represents the quantity of samples within the class k. The set C_k denotes the collection of samples that are categorized under the class k, while X signifies an individual sample from this particular class.

- Calculation of the Intra-Class Dispersion Matrix (S_W): This matrix evaluates the spread of samples around their class mean vectors.

$$\mathbf{S}_W = \sum_{k=1}^{K} \sum_{\mathbf{x} \in C_k} (\mathbf{x} - \mathbf{m}_k)(\mathbf{x} - \mathbf{m}_k)^T \tag{4.18}$$

- Calculation of the Inter-Class Scattering Matrix (S_B): This matrix measures the dispersion of class mean vectors relative to the global mean vector of all classes as equation 4.19 shows.

$$\mathbf{S}_B = \sum_{k=1}^{K} N_k (\mathbf{m}_k - \mathbf{m})(\mathbf{m}_k - \mathbf{m})^T \tag{4.19}$$

$$\mathbf{m} = \frac{1}{N} \sum_{i=1}^{N} \mathbf{x}_i \tag{4.20}$$

where m is the overall average vector of all classes calculated using equation 4.20 with N the total number of samples.

- Solving the Equal Values and Eigenvectors Problem: The goal is to maximize the inter-class variance while minimizing the intra-class variance. This results in the resolution of the generalized problem of eigenvalues as equation 4.21 resumes

$$\mathbf{S}_W^{-1}\mathbf{S}_B\mathbf{w} = \lambda\mathbf{w} \tag{4.21}$$

where W is the eigenvector (or discriminant) and λ is the eigenvalue.

- Eigenvector Selection: Eigenvectors corresponding to the largest eigenvalues are selected. These eigenvectors form the transformation matrix W which will be used to project the original data into a new space of reduced dimension.

- Data Projection: The original data X is projected into the new reduced dimension space using the transformation matrix W:

$$\mathbf{Y} = \mathbf{XW} \tag{4.22}$$

where Y represents the new data coordinates in the main component space.

In summary, LDA for dimensionality reduction aims to project data into a lower dimension space while maximizing separability between classes. By solving the eigenvalue problem for intra-class and inter-class dispersion matrices, LDA identifies the directions that maximize the distance between classes, thus facilitating the task of classification and data analysis in spaces of reduced dimension.It finds extensive application in various fields, such as facial recognition, aiding in distinguishing faces by reducing image dimensions, or in medical diagnosis for categorizing patients into different disease groups. Moreover, within the financial sector, it assists in differentiating between valid and fraudulent transactions. In essence, LDA stands out as a potent instrument for streamlining intricate datasets while enhancing the classification efficacy of predictive models.

4.4.3 t-Distributed Stochastic Neighbor Embedding

t-SNE, or t-Distributed Stochastic Neighbor Embedding, is a nonlinear dimensionality reduction technique mainly used for the visualization of high-dimensional data. Developed by Laurens van der Maaten and Geoffrey Hinton in 2008, t-SNE is particularly suited for the visualization of datasets with complex structures, such as clusters, in lower-dimensional spaces (typically two or three dimensions). The method works by converting similarities between data points into joint probabilities and by minimizing the Kullback-Leibler divergence between these probabilities in high and low dimension spaces. In high dimension, similarity is measured using a Gaussian distribution, while in low dimension, a one-dimensional Student distribution is used. The aim is to preserve the local structure of the data by adjusting the positions of the points in the low-dimensional space through gradient descent. t-SNE is widely used for data visualization, exploratory analysis and pre-processing for clustering. Keywords However, it is expensive in terms of computation, sensitive to parameters and sometimes difficult to interpret. It works Principally as follow:

- Pairwise Similarities:

  The similarity among data points in the high-dimensional space is assessed by utilizing a Gaussian distribution centered at each specific point. The correlation $p_{i,j}$ between points i and j is directly proportional to the likelihood of j being selected as a neighbor of i under this Gaussian distribution.

- Joint Probabilities:

  To ensure equality between $p_{i,j}$ and $p_{j,i}$ $p_{i,j} = p_{j,i}$, the joint probability $p_{i,j}$ is symmetrized. In the low-dimensional space, the similarity $q_{i,j}$ between points is calculated using a Student's t-distribution, where it has one degree of freedom and is known for being a heavy-tailed distribution.

- Cost Function:

The goal of t-SNE is to reduce the Kullback-Leibler divergence, which measures the difference between two probability distributions, from the joint probabilities P in the high-dimensional space to the Q in the low-dimensional space.The cost function can be defined as follows:

$$C = \sum_{i \neq j} p_{ij} \log \frac{p_{ij}}{q_{ij}} \tag{4.23}$$

- Gradient Descent: Achieving the minimization of the cost function usually involves using gradient descent, which involves iteratively adjusting the positions of points in a lower-dimensional space to more closely align with the similarities in a higher-dimensional space.

4.5 Classification

Classification stands as a crucial aspect of machine learning and pattern recognition, with significant implications in various fields from facial recognition to fraud detection. Its primary goal is to label a new observation based on a training dataset comprising labeled observations. This chapter aims to delve into the fundamental concepts, techniques, and algorithms of classification, offering a comprehensive framework for both theoretical comprehension and practical application and introduce the technical aspect of the tools used in our work also the most efficient algorithms

4.5.1 Classical Classifiers

Classical classifiers constitute essential algorithms within the field of machine learning, employed for the purpose of classifying data points into predefined categories. The functioning of these classifiers hinges upon the utilization of a specific set of features derived from the data in order to determine the appropriate class labels. The following enumeration presents a selection of the classical classifiers that are utilized as references to our contribution

NN Classifier

The Nearest Neighbor (NN) classifier is a straightforward and intuitive machine learning algorithm commonly used for classification tasks. It categorizes a data point by looking at the class labels of its closest neighbors in the feature space. In this discussion, we will explore the k-Nearest Neighbor (k-NN) version, which expands the NN classifier to take into account k neighbors rather than just one. The fundamental concept behind the NN classifier involves assigning a label to a query point based on the labels of the nearest points in the training dataset. The k-NN classifier enhances this concept by considering the k closest points and utilizing methods like majority voting to determine the class label of the query point.

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2} \tag{4.24}$$

$$d(x, y) = \sum_{i=1}^{n} |x_i - y_i| \tag{4.25}$$

$$d(x, y) = \left(\sum_{i=1}^{n} |x_i - y_i|^p \right)^{\frac{1}{p}} \tag{4.26}$$

The Main Algorithm of NN Classifier

The K Value The k value plays a crucial role in the k-NN algorithm, being a critical hyperparameter. A low k value (e.g., $k = 1$) can result in a model that is highly responsive to noise in the training data, whereas a high k value offers more smoothing but might obscure the class boundaries. Common methods for k selection are as follows:

Utilizing cross-validation: Divide the training data into multiple folds and assess the performance for various k values.

Heuristics: Occasionally,$k = \sqrt{N}$(where $N$is the number of training samples) is employed as a rule of thumb.

NN Applications Domain The NN classifiers find many applications in various fields thanks to their ability to learn complex models from large amounts of data. Here are some common

Algorithm 1 The NN Classifier Algorithm

1: **1. Feature Extraction:** Extract features from the dataset.
2: **2. Distance Metric:** Select a distance metric to quantify the similarity among data points. Options include:

- Euclidean Distance (Equation 4.24)
- Manhattan Distance (Equation 4.25)
- Minkowski Distance (Equation 4.26)

3: **3. Determine Nearest Neighbors:** Calculate the proximity of a query point to all data points in the training dataset to determine the k nearest neighbors.
4: **4. Class Assignment:**

- **Majority Voting:** Assign the class label that appears most frequently among the k nearest neighbors.
- **Weighted Voting:** Assign weights to neighbors based on their distance (closer neighbors have greater influence) before determining the class label.

applications in different fields,

- 1. Computer Vision Neural classificators are widely used in computer vision for tasks such as: Object recognition: identify and classify objects in images. Face Detection: Find and recognize human faces. Image Segmentation: Split an image into meaningful segments. Character recognition: Automatic reading of text in images (OCR).

- 2. Natural Language Processing (NLP) In the field of natural language processing, NN classifiers are used for: Sentiment analysis: Determine the emotion or opinion expressed in a text. Machine translation: Translate text from one language to another. Auto Summary: Generate summaries of long texts. Text classification: Categorize documents based on their content.

- 3. Health and medicine Medical applications of neural classifiers include: Computer-aided diagnosis: Help identify diseases from medical images, such as x-rays or MRIs. Genome analysis: Identify genetic mutations and disease risks. Patient monitoring: Detect abnormalities in vital signs.

- 4. Finance In the financial sector, NN classifiers are used for: Fraud detection: Identify

Positive Aspects	Limitations
The attribute of simplicity is exemplified by its ease of comprehension and implementation.	Due to the necessity of calculating the distance to all training points for each query, it can be computationally intensive, particularly with large datasets.
The absence of a training phase characterizes k-NN as a lazy learner, obviating the need for an explicit training phase.	An essential weakness lies in the requirement to retain all training data, leading to significant storage demands.
Its versatility is demonstrated by its applicability to both classification and regression tasks.	The model's sensitivity to irrelevant features can result in performance degradation when numerous irrelevant or redundant features are present. The choice of distance metric is pivotal as it greatly impacts the model's performance.

Table 4.1: Strengths and weaknesses of k-NN Classifier

fraudulent transactions. Market prediction: Predict trends and fluctuations in financial markets. Credit analysis: Assess the creditworthiness of loan applicants.

- 5. Industry and manufacturing Industrial applications include: Predictive maintenance: Predict machine failures before they happen. Quality control: Detect defects in manufactured products. Process automation: Optimize production chains.

- 6. Transport In the field of transport, NN classifiers are used for: Autonomous vehicles: Helping cars navigate by recognizing roads, traffic signs and obstacles. Traffic Management: Predict and optimize traffic flows. Route planning: Optimize routes for delivery services and public transportation.

- 7. Security Security applications include: Facial Recognition: Identify individuals for security purposes. Video surveillance: Detect suspicious behavior in surveillance videos. Biometric authentication: Use biological features to secure access.

- 8. Agriculture In agriculture, neural classificators are used to: Plant Disease Detection: Identify diseases and pests from plant images. Yield Forecast: Estimate crop yields based on environmental conditions. Agricultural automation: Control agricultural machinery and optimize crops.

Overall, Neural classifiers have become indispensable tools in many fields thanks to their ability to process and analyze complex data. Their use improves efficiency, reduces costs and discovers new opportunities in a variety of industries.

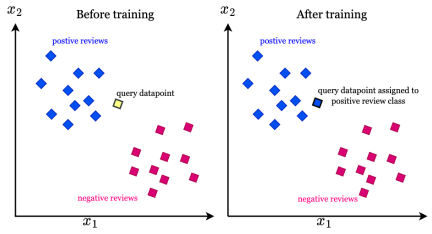


Figure 4.7: Nearest Neighbor Classifier

Support Vector Machine (SVM) Classifier

Support Vector Machines (SVMs) represent potent supervised learning models utilized for both classification and regression tasks. The principal objective of an SVM is to identify the optimal hyperplane that effectively segregates the data into distinct classes. SVMs demonstrate particular suitability for binary classification issues, although their applicability extends to encompass multi-class classification scenarios as well.It endeavors to ascertain the hyperplane that maximizes the margin between two classes. This margin is delineated as the distance between the hyperplane and the closest data points from each class, denoted as support vectors. The optimal hyperplane emerges as the one that maximizes this margin. Given a collection of training data points $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$, where x_i signifies the feature vector of the i-th instance and y_i denotes its label ($y_i \in \{-1, 1\}$ for binary classification), the main goal of SVM is to address the subsequent optimization problem. It can mathematically formulate the problem in Primal or dual form using equations 4.27 and 4.28, respectively.

$$\begin{aligned} &\min_{w,b,\xi} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n}\xi_i \\ &\text{subject to: } y_i(w \cdot x_i + b) \geq 1 - \xi_i, \quad i = 1, \ldots, n, \\ &\xi_i \geq 0, \quad i = 1, \ldots, n \end{aligned} \tag{4.27}$$

where:

The weight vector w is defined as a fundamental component in the context of the problem at hand. The bias term b represents an essential parameter that influences the decision boundary in the given model.The slack variables ξ_i are introduced to accommodate potential misclassifications in scenarios where the data is not linearly separable.The regularization parameter C plays a crucial role in balancing the optimization objectives by managing the trade-off between margin maximization and classification error minimization.

The issue can alternatively be expressed in its dual manifestation, a method that proves to be especially valuable for integrating kernel functions.

$$\begin{aligned} &\min_{w,b,\xi} \frac{1}{2}\|w\|^2 + C\sum_{i=1}^{n}\xi_i \\ &\text{subject to:} \quad y_i(w \cdot x_i + b) \geq 1 - \xi_i, \quad i = 1, \ldots, n, \\ &\qquad\qquad \xi_i \geq 0, \quad i = 1, \ldots, n \end{aligned} \tag{4.28}$$

The Lagrange multipliers are denoted as α_i. The kernel function $K(x_i, x_j)$ represents a key aspect in the formulation.

Positive aspects	Limitations
SVMs demonstrate efficacy in high-dimensional spaces by performing effectively when the number of features surpasses the number of samples.	The complexity arises in the selection of the kernel, as well as its parameters, which significantly impact the overall performance.
There is a focus on memory efficiency as SVMs utilize a subset of training points, known as support vectors, in the decision function.	There is a notable computational cost associated with SVM training, particularly when dealing with large datasets.
The versatility of SVMs is demonstrated through the ability to specify different kernel functions for the decision function.	SVMs are sensitive to noise, especially in scenarios involving non-separable data with extensive overlap among classes.

Table 4.3: Strengths and weaknesses of the SVM classifier

4.5.2 Explainable Classifier

An explainable classifier is a machine learning model designed to make its decisions and predictions understandable to humans. Unlike "black box" models like deep neural networks, which can be very powerful but opaque, explainable classifiers provide transparent and intuitive justifications for their results. These explanations can take the form of logical rules, visualizations or decompositions of the contribution of each feature to the final decision. The main objective is to enable users, including those without in-depth technical expertise, to understand why a certain decision was made, to verify the validity and fairness of the model, and to ensure compliance with regulations and ethical standards. Models such as decision trees, linear regressions, recently fuzzy rule-based classifier has been emerged as explainable classifiers also a pertinent solution to the black-box system, in this section we will introduce the most effecient classifier that have been exploited in our study

ALMMo-0 Classifier

The Adaptive Learning Model Mixture of Zero Order (ALMMo-0) classifier introduces a pioneering methodology within the realm of machine learning that amalgamates facets of fuzzy logic, adaptive learning, and clustering methodologies. This innovative approach aims to tackle issues pertaining to the interpretability and adaptability of conventional classification models.

Key Characteristics:

- Adaptive Learning:

  ALMMo-0 continually adjusts its model parameters as fresh data is introduced. This capability enables the classifier to conform to evolving data patterns and uphold accuracy without necessitating complete retraining.

- Mixture of Models:

  The classifier functions by amalgamating numerous elementary models (zero-order models, essentially constant models) to formulate a more intricate decision boundary. This blending technique empowers the classifier to encapsulate a diverse array of data distributions and patterns.

- Fuzzy Logic Integration:

  Incorporating fuzzy logic principles enables the handling of uncertainty and imprecision within the data. This incorporation renders the ALMMo-0 classifier resilient in situations where data is noisy or lacks precise definition.

- Zero-Order Models:

  Within ALMMo-0, zero-order models, the most rudimentary form of fuzzy models, are employed. These models are straightforward to interpret as they yield constant outputs for each fuzzy region delineated by the input domain.

- Explainability:

  A primary advantage of ALMMo-0 lies in its explainability. Leveraging zero-order models and fuzzy logic facilitates a transparent and comprehensible decision-making process. Users can readily discern how input features contribute to the classification outcome. Benefits: Real-Time Adaptation: ALMMo-0 can promptly adjust its parameters, rendering it suitable for dynamic environments where data patterns undergo frequent alterations. Robustness: The integration of fuzzy logic aids in effectively managing equivocal and noisy data. Interpretability: The model's configuration and decision-making

process are straightforward to comprehend, a crucial aspect for applications necessitating transparency, such as healthcare or finance. Applications: Dynamic Systems: ALMMo-0 proves particularly beneficial in scenarios characterized by continuously evolving data, like stock market analysis, real-time monitoring systems, and adaptive control systems. Healthcare: Its elucidative nature renders it apt for medical diagnostic systems where understanding the rationale behind decisions holds paramount importance. Finance: In the realms of financial risk assessment and fraud detection, the capacity to adapt to novel patterns and furnish clear results is immensely advantageous.

Consider a healthcare scenario where patient data is incessantly amassed and refreshed. An ALMMo-0 classifier could be deployed to dynamically learn from new patient records, adjusting its parameters to mirror the latest trends in patient health data. Concurrently, it offers lucid explanations for its predictions, such as identifying the symptoms that predominantly influenced a specific diagnosis, thereby aiding healthcare professionals in making well-informed decisions.

Overall, the ALMMo-0 classifier embodies a noteworthy advancement in merging the adaptability of contemporary machine learning techniques with the interpretability and resilience demanded by numerous real-world applications. Its distinctive blend of adaptive learning, fuzzy logic, and model simplicity positions it as a valuable asset in diverse fields requiring transparent and adaptable decision-making models. The main algorithm and more technical details are inroduced in Chapter 6.

xDNN Classifier

Explainable Deep Neural Networks (xDNN) signify a noteworthy progression within the realm of machine learning, catering to the essential requirement for clarity and explicability in intricate models. The xDNN classifier is crafted to furnish the formidable predictive functionalities of deep learning, all the while guaranteeing comprehensibility of the decision-making procedure to human agents.

Key Characteristics:

- Explainability:The principal characteristic of xDNN resides in its emphasis on explainability. In contrast to conventional "black-box" neural networks, xDNN integrates mechanisms to render the inner workings of the model transparent. This involves generating explanations that are interpretable by humans for every prediction, such as accentuating relevant features or offering rationale in natural language.

- Hybrid Model Architecture: xDNN frequently amalgamates conventional deep learning architectures (e.g., Convolutional Neural Networks, Recurrent Neural Networks, or fully connected networks) with supplementary components or methodologies aimed at boosting interpretability. These components could encompass attention mechanisms, feature attribution methods, or the amalgamation of simpler, more interpretable models.

- Feature Attribution: Approaches like SHAP (SHapley Additive exPlanations) and LIME (Local Interpretable Model-agnostic Explanations) are embedded within xDNN to furnish comprehensive insights into how each feature impacts the model's output. This facilitates the comprehension of which inputs hold the utmost significance for a specific prediction.

- Attention Mechanisms: Attention mechanisms enable the model to concentrate on the most pertinent portions of the input data, thereby simplifying the interpretation of which aspects of the data influence the model's decisions. These mechanisms can be visually represented to indicate which sections of an image or which words in a text are accorded the highest weight.

- Rule Extraction: xDNN may incorporate techniques for extracting decision rules from the network. These rules are often articulated in a format that is straightforward to grasp and validate, like decision trees or sets of logical conditions.

- Modular Design: The architecture of xDNN is modular, permitting the inclusion of various explainability techniques. This adaptability implies that the model can be customized to specific applications and needs for interpretability. Benefits:

By explainability the decision-making process, xDNN establishes trust with users and stake-

holders, a critical aspect in sensitive domains such as healthcare, finance, and legal decision-making. Regulatory Compliance, Numerous industries are bound by regulations mandating model transparency. xDNN aids organizations in adhering to these regulations through the provision of interpretable models.Therefore, The presence of explainability assists in debugging models by facilitating the comprehension and rectification of errors, thereby enhancing the overall resilience and dependability of the system.also, In scenarios involving end-users, furnishing coherent explanations for predictions can amplify user contentment and involvement. An xDNN classifier employed in a medical diagnostic instrument is worthy of consideration. In the scenario of determining if a patient possesses a specific ailment based on their medical history and examination outcomes, the xDNN not only offers a prognosis but also delineates the key factors (for instance, particular test results, symptoms) that predominantly influenced the decision-making process. To illustrate, it could emphasize that heightened levels of a particular biomarker constituted the primary rationale behind the prognosis. This elucidation is subject to examination by a medical professional to authenticate the model's rationale, thereby instilling a higher level of trust in the diagnosis.

4.6 Conclusion

This chapter has comprehensively elucidated the fundamental methodologies and instruments employed in the design, execution, and assessment of biometric systems. By delineating the procedures of data acquisition, feature extraction, and performance evaluation, it establishes a rigorous framework for system development.

The methodologies articulated herein constitute the foundational support for the subsequent experimental work, thereby ensuring the validity and reliability of the findings. This systematic approach augments the precision and interpretability of the biometric models, thereby contributing to the overall efficacy of the research.

Chapter 5

Explainability in Biometric Systems

5.1 Introduction

Biometric systems play a crucial role in a variety of areas, including security, healthcare and identity management. However, despite their undeniable advantages, they are often regarded as ”black boxes”, which means that their decisions are not always justified and understandable by users. In this chapter, we examine the importance of explainability in biometric systems, its implications and methods to improve the understanding of why and how does the intelligent machine made the decisions.

5.2 Fundamentals of Explainability

5.2.1 Basic Concepts

In order to qualify an intelligent system as an Explainble system there some principles and approaches should be verified for making the models understandable to human users.

- Comprehensibility of results: Explainability aims to make the results of systems or models understandable to users, by providing clear and intuitive explanations of how these results are generated.

- Transparency of processes: It is essential to make transparent the internal processes of

systems or models, including algorithms, input data, weights and calculation steps, so that users can understand how decisions are made.

- Interpretability of models: The models used in systems must be interpretable, that is, they must be designed in such a way that users can easily understand their operation and predictions.

- Compliance with standards and regulations: Explainability is often tied to specific standards and regulations in certain areas, such as data protection and consumer rights. Systems must be designed and implemented to comply with these standards and regulations.

- User feedback: The integration of a user feedback mechanism is important to allow users to ask questions, provide comments and express concerns about decisions made by the systems. This can help improve explainability by identifying gaps and potential improvements.

- Robustness and reliability: Systems must be robust and reliable to ensure that explanations provided are consistent and accurate. This requires rigorous testing and validation to ensure the explanations are reliable in a variety of conditions and situations.

- Education and Awareness: Providing education and awareness to users on the concepts and limitations of explainable systems is essential to foster deeper understanding and wider adoption of these systems.

  In summary, the fundamentals of explainability are based on providing understandable results, transparency of processes, interpretability of models, compliance with standards and regulations, user feedback, robustness and reliability, and education and awareness. By integrating these principles into the design and implementation of systems, it is possible to create explainable systems that inspire trust and promote greater user understanding and acceptance.

5.2.2 Explainability Approaches

Explainality approaches refer to the methods and techniques used to make the decisions made by a system or model understandable to human users. Here are some of the most commonly used approaches

- Interpretable model methods: These approaches aim to use models whose predictions are easily interpreted. This may include the use of linear models, decision trees or shallow neural networks, which allow for a direct understanding of how input variables affect output predictions. Techniques such as LIME (Local Interpretable Model-agnostic Explanations) and SHAP (SHapley Additive exPlanations) are examples of methods that provide local explanations for complex model predictions.

  - LIME, acronym for "Local Interpretable Model-agnostic Explanations", is a machine learning model explanation method that aims to provide local explanations for the predictions of these models. Unlike traditional model interpretation methods that attempt to understand the model as a whole, LIME focuses on understanding a specific prediction by locally examining the neighborhood of that prediction in the feature space.

    Here is how LIME works:

    Local instance generation: To explain a given prediction, LIME starts by generating a set of "neighbors" or local instances around the instance to be explained. These local instances are generated by slightly disrupting the characteristics of the original instance while keeping the other characteristics constant.

    Calculation of local predictions: Model predictions are then calculated for each local instance generated. These local predictions provide an approximation of how the model behaves in the vicinity of the instance to be explained.

    Training a local interpretable model: An interpretable model, such as a linear model or a simple decision tree, is then fitted to the generated local instances. This interpretable model is used to approximate the behavior of the complex model in

the vicinity of the instance to be explained.

Calculation of weights of importance: For each feature, weights of importance are calculated based on the contribution of that feature to the predictions of the local interpretable model. These weights of importance are used to explain the relative importance of each characteristic in predicting the given instance. Calculation of weights of importance:

Explanation generation: Finally, an explanation is generated by highlighting the most important features for the prediction of the given instance, based on the calculated weights of importance. The advantage of LIME is that it is model agnostic, which means it can be used to explain the predictions of any machine learning model, whether it is linear, nonlinear, black box, or even from deep neural networks. This makes it a powerful tool for understanding and interpreting the decisions of complex models, even when their internal workings are difficult to understand.

– SHAP (SHapley Additive exPlanations) : The methodology known as SHAP represents a sophisticated strategy utilized for elucidating the predictions generated by machine learning models. Rooted in the principles of game theory, this methodology assigns SHAP values to individual features, thus furnishing an assessment of the incremental impact of each feature on a specific prediction. Through the utilization of the Kernel SHAP algorithm, a series of interpretation instances are produced by making slight adjustments to the characteristics of the original instance. The evaluation of the contribution of each feature on these interpretation instances enables the precise calculation of SHAP values. These values play a pivotal role in offering both global and local elucidations for the predictions made by the model. Global SHAP values serve to quantify the overall significance of each feature across all predictions made by the model, while local SHAP values furnish a detailed rationale for a particular prediction concerning a specific instance. These explanations can be effectively represented through scatterplots or bar graphs, facilitating their comprehension. By enhancing the comprehension of the specific contribution of each

feature towards a prediction, the SHAP methodology finds extensive employment within the realm of machine learning model interpretability, yielding valuable insights into the internal mechanisms of intricate models, irrespective of their design.

- Data visualization: Data visualization is a powerful approach to making the results of a system or model more understandable. This may include graphs, diagrams, or heat maps that visually represent the relationships between input and output variables. For example, scatter plots can be used to illustrate correlations between input characteristics and model predictions.

- Model interpretation techniques: These techniques aim to provide direct explanations of how a model makes decisions. This may include using heat maps to visualize the importance of different input characteristics or analyzing attention profiles in natural language processing models to understand which parts of the text are most influential in decision making.

- Decomposition methods: These approaches break down the predictions of a model into simpler, more interpretable components. For example, Singular Value Decomposition (SVD) can be used to decompose a model weight matrix into base vectors, allowing for a better understanding of how each input feature contributes to model predictions.

- Comparisons with reference models: Another approach is to compare the decisions of a model with those of a simpler or more transparent reference model. For example, a linear model can be used as a reference to evaluate the contribution of each input feature to the overall prediction of the model.

By combining these different approaches, it is possible to provide rich and comprehensible explanations about the decisions made by a system or model, which promotes better understanding and greater trust on the part of users.

5.3 Explainable Biometric Systems

An explainable biometric system is a system that incorporates mechanisms for comprehending and justifying the decisions made by the system, it renders concerning the authentication or validation of individuals. In contrast to classical biometric systems, which may be perceived as black boxes entities, explainable biometric systems furnish explications on the decision-making process, the considerations of biometric attributes involved, and their impact on making the decision. These systems aspire to enhance transparency, confidence, and societal approval of biometric technologies by enabling users to gain a deeper insight into their functionality and constraints.

Explainable biometric systems has known recently a significant progression in the domain of biometrics, offering a transparent and comprehensible method for individual's identification. Through the integration of Explainable mechanisms, these systems enable not only the recognition of individuals but also the provision of explainable and clear process of each decision. Consequently, Users are provided with valuable insights into the biometric attributes that are taken into account, the decision-making processes, and the factors influencing these determinations. This transparency fosters user trust in biometric technology, enabling them to grasp thoroughly its functioning and constraints. The primary advantage of explainable biometric systems lies in their capacity to uphold answerability and impartiality. By furnishing detailed clarifications of the choices made, these systems aid in identifying and rectifying potential biases in the identification procedures, thereby ensuring equitable treatment for all. Moreover, by offering visibility into the utilized biometric features and their respective significance, These systems promote decision-making based on knowledge and help reduce identification inaccuracies. Additionally, explainable biometric systems Play a crucial role in safeguarding privacy and individual liberties. By empowering users to comprehend the utilization and interpretation of their biometric data, these systems cultivate trust in the safeguarding of personal information. Furthermore, they advocate for increased transparency in the acquisition, retention, and utilization of biometric data, thereby Ensuring compliance with ethical and legal obligations regarding

data confidentiality and protection. To conclude, explainable biometric systems epitomizing a significant advancement in biometrics, it presents a transparent, fair, and privacy-preserving method for individual authentication. Their ability to supply unambiguous and intelligible explanation of the decisions rendered aids in fostering user confidence, advancing answerability and impartiality, and ensuring reverence for individual rights and ethical standards.

5.3.1 Context and Issues

The rise of explainable biometric systems is anchored in a dynamic technological environment, where transparency, accountability, and privacy issues are becoming increasingly prominent. As biometric technologies advance and become more integrated across various societal domains, ensuring the comprehensibility and equity of these systems has become imperative. The rise of ethical and social challenges related to biometric data usage has sparked a heightened need for mechanisms that provide explanations, empowering individuals to grasp the rationale behind the decisions made by these systems while safeguarding their privacy and individual rights. Explainable biometric systems aim to address this escalating demand by enhancing transparency and explainability in the decision-making process. By explainability how identification determinations are reached, these systems empower individuals to comprehend the factors taken into account and the rationale underpinning each identification . This fosters user trust in biometric technology by granting them full insight into its operational principles and implications. The anticipated consequence of integrating explainable biometric systems is a substantial enhancement in public trust in biometric technology. By offering rationales for the decisions rendered by biometric systems, they enable individuals to understand their operations and constraints better. This, in turn, can foster more informed and conscientious utilization of biometric technology, thereby reducing errors and potential misuse. Ultimately, explainable biometric systems have the ability to enhance public trust in biometrics as a dependable, fair, and privacy-aware method of identification.

5.4 Applications of Explainability in Biometric Systems

The utilization of explainability in biometric systems is multifaceted, with the objective of enhancing the transparency, trust, and effectiveness of these systems. The following are among the most crucial applications:

- Security and Authentication: Explainability plays a role in bolstering the security of biometric systems through providing justifications for identification or verification determinations. This capability aids in the detection and prevention of potential fraudulent activities or instances of identity theft.

- Justice and Equity: Gaining insight into the decision-making processes of biometric systems enables the promotion of equitable utilization of such systems. This serves to mitigate the risk of biases and discriminatory practices in identification procedures.

- Privacy Protection: The aspect of explainability guarantees that the actions taken by biometric systems Protect the privacy rights of individuals. By comprehending how biometric data is utilized and interpreted, it can be assured that sensitive data is managed appropriately.

- Regulatory Compliance: Various data protection laws, frequently mandate that automated decisions be explainable. Biometric systems that offer explainability assist organizations in adhering to these regulations by justifying the rationales behind their decisions.

- Education and Awareness: Explainability facilitates the education of users on the operational mechanisms of biometric systems and the repercussions of employing such technologies. This contributes to a heightened comprehension and acceptance of biometric technology within society. The integration of explainability into biometric systems has the potential to enhance their societal acceptability, effectiveness, and dependability, all while upholding principles of individual rights and ethics.

5.4.1 Data and Privacy Management

Explainable biometric systems are of paramount importance in the realm of data and privacy management as they enhance transparency and offer superior privacy safeguards. The following are critical facets of their contribution to data and privacy management:

- Transparency and user control : are facilitated by explainable biometric systems, enabling users to comprehend the utilization and processing of their biometric data. This serves to heighten transparency levels and empower individuals with increased authority over their personal data. The comprehension of how biometric systems arrive at decisions equips organizations with the ability to more effectively evaluate the security threats linked to the gathering and handling of biometric data. Consequently, this capability enables enhanced identification and mitigation of potential vulnerabilities. The explainability furnished by explainable biometric systems streamline the process of detecting abuse, bias, and errors in decision-making procedures. This, in turn, enables organizations to promptly address issues and safeguard individual privacy.

- Regulatory compliance: Numerous regulations, such as the General Data Protection Regulation (GDPR) in Europe, necessitate the presence of transparency and accountability in the handling of personal data, which includes biometric data. The utilization of explainable biometric systems aids organizations in adhering to these regulations by offering lucid explications of the decision-making processes.

- Public trust: Through the provision of elucidations regarding the functionality of biometric systems, organizations cultivate public trust in their capacity to safeguard privacy and utilize data in a conscientious manner.

Overall, explainable biometric systems assume a pivotal role in the management of data and privacy by delivering transparency, empowering users, ensuring protection against security threats, detecting and preventing abuse and errors, ensuring regulatory compliance, and fostering public trust. These systems contribute to the establishment of an ethical and responsible environment for the utilization of biometric data.

5.4.2 Human-System Interactions

Explainable systems are a critical option to Human-System Interactions (HSI) as they enhance comprehension, trust, and cooperation between human operators and computational systems. Various critical facets of their contribution to HSI can be delineated. For instance, Human-machine collaboration is significantly facilitated by explainable systems, as they render decision-making processes and system outcomes more transparent and intelligible to human users. Consequently, this fosters enhanced task coordination and optimal utilization of the complementary strengths of both humans and machines. Furthermore, the utility of explainable systems extends to the domains of training and education, wherein they serve as invaluable instruments. By enabling users to delve into and grasp the fundamental principles governing computer systems, these systems streamline the acquisition of new skills and the resolution of intricate problems.

5.5 conclusion

This Chapter emphasizes the critical significance of transparency and comprehensibility within the realm of biometrics. The incorporation of explainability mechanisms into biometric systems facilitates the establishment of user trust, enhancement of decision-making quality, and advocacy for a more ethical and conscientious utilization of biometric data.

By delineating the diverse applications of explainable biometric systems, it has been observed how these systems can contribute to various realms including security, data privacy, human-machine interactions, and regulatory adherence. Through the provision of lucid and comprehensible explanations regarding the functionality of biometric systems, collaboration between humans and machines can be enhanced, errors and biases can be identified, and a more ethical application of biometric technologies can be promoted.

In the ongoing development and deployment of biometric systems, it is imperative to uphold the principles of transparency, accountability, and privacy. The adoption of explainable biometric systems signifies a significant stride in this direction, furnishing a framework for the ethical and responsible utilization of biometric data within contemporary society.

In summary, explainable biometric systems yield substantial advantages in terms of transparency, trust, and accountability. By embedding these principles into the design and execution of biometric systems, a future can be cultivated where biometrics are employed in an ethical, responsible, and privacy-conscious manner, thereby delivering notable security and convenience benefits.

Chapter 6

Contribution

6.1 A face recognition system based-ALMMo-0 classifer

Nowadays, biometric systems have emerged as a potent tool for personal identification. Advanced research yielding significant outcomes has been furnished. Despite the notable progress, there exists a substantial requirement for enhancement in the efficacy of security applications. More recently, an Autonomous Learning Multi-Model Classifier of 0-Order (ALMMo-0) has been suggested as a versatile efficient classification tool, autonomous, non-iterative, and fully explainable the issue of supervised pattern recognition. Therefore, the objective of this paper is to introduce a novel efficient methodology based on the ALMMo-0 classifier for authentication systems Applying the face modality. The proposed methodology is entirely data-driven, non-iterative, and feedforward. The suggested approach extracts the most pertinent features from the facial image using the Gabor filter bank descriptor, which is then input into the ALMMo-0 classifier that automatically extracts the data clouds and constructs its multimodel structure, develops its AnYa Fuzzy rule base (FRB) sub-classifiers for each category, objectively generates the confidence score based on the mutual distribution, then categorizes the new data employing a ”winner takes all” strategy, thereby enabling the system to ascertain whether the individual is authentic or an impostor. Compelling evidence of ALMMo-0 efficacy was observed during experiments conducted on nine facial databases. Outcomes were depicted through rank-1, equal error rate (EER), cumulative match curve (CMC), and receiver operating characteristic (ROC)

curves. Moreover, to offer more insightful information regarding our proposed system, results were also delineated in terms of True Positive Rate (TPR) or the Genuine Acceptance Rate (GAR). The findings showcased the superior performance of the proposed strategy, boasting not only an exceedingly low error rate (EER) of 0.0% and a perfect accuracy (rank-1) of 100% but also high interpretability and minimal computational complexity. In day-to-day life, individuals are frequently and consistently interconnected to various networks and social platforms, leading to an escalating level of addiction in some individuals and serving as a crucial tool for businesses for others. Within this vast Domain of information, a fundamental necessity for all users revolves around safeguarding their personal data. Biometric systems serve this purpose by employing scientific methodologies to authenticate individuals based on their unique physical and behavioral traits like fingerprints, voice patterns, iris scans, and more. Among these identification modalities, facial recognition stands out as one of the most efficient methods, gaining significant traction recently and becoming a focal point of research across diverse fields[73] [74] [75] [76]. This success can largely be attributed to its user-friendly nature and the availability of extensive annotated face datasets [76].

Moreover, as data volume continues to surge, traditional machine learning techniques and facial recognition systems face challenges in handling a large number of stored templates for each individual in the database and adapting to changes in data distribution. Consequently, they yield subpar results characterized by low accuracy and high Equal Error Rate (EER). Nevertheless, combining facial recognition scores at the model level can significantly enhance performance by leveraging advanced multi-model recognition systems capable of accommodating data variations and efficiently processing numerous templates. Despite notable advancements in biometric technology, facial recognition systems have not received commensurate attention. Hence, there is a pressing need to develop an innovative facial biometrics recognition system that addresses existing limitations, minimizes false acceptance rates, and reduces EER.

The primary objective of this study is to introduce an effective facial recognition biometric system based on a novel strategy involving the 0-order Autonomous Learning Multiple Model (ALMMo-0) classifier to ascertain the authenticity of users. The ALMMo-0 Classifier [77] rep-

resents a promising new approach applicable in biometric applications. In contrast to conventional supervised machine learning methods that conventionally construct mathematical functions to determine the inclusion of a data sample within a specific set, the ALMMo-0 operates as a fully autonomous classifier. It constructs its multi-model framework solely based on data-driven insights, devoid of any prior assumptions, and iteratively refines its Meta-parameters directly from the data. Unlike traditional machine learning approaches, including advanced ones [78], that learn to categorize new data samples based on known category memberships within a training dataset, the ALMMo-0 stands out as non-iterative, non-parametric, and entirely self-sufficient, eliminating the need for parameter training due to its inherent feedforward structure.The ALMMo-0 classifier commences by autonomously identifying the point of convergence from the experimentally observed data; subsequently, data clouds are generated by resembling Voronoi Tessellation[79] per class. Following this, it constructs a collection of sub-classifiers for the different classes in the form of AnYa fuzzy rules derived from the non-parametric data clouds. Upon the arrival of new data, each AnYa FRB sub-classifier impartially produces a confidence score, and the label is then assigned to the new data sample using the ”winner takes all” principle.

The primary objective of this study is to introduce a system-based ALMMo-0 approach for understanding an individual's facial characteristics in biometric systems, which can serve as a valuable identification tool for discerning between genuine individuals and imposters. A key advantage of the ALMMo-0 classifier lies in its ability to construct a multi-model framework directly from data, developing sub-classifiers in the AnYa FRB format. By learning from the data, it performs classification effectively and transparently, ensuring high performance levels with superior accuracy and interpretability, as well as minimal error rates and computational complexity. Consequently, the ALMMo-0 classifier emerges as a robust alternative to existing methodologies.

The primary contribution of this research can be outlined as follows: - The present study introduces a novel biometric system based on the ALMMo-0 classifier utilizing facial modality. - ALMMo-0 (Autonomous Learning Multi-Model) represents an efficient new multi-model,

autonomous, data-centric, and non-iterative classifier, comprising a series of AnYa fuzzy Rule-Based (FRB) sub-classifiers. - Experimental outcomes underscore the exceptional performance of the ALMMo-0 classifier across

6.1.1 Architecture and algorithm of the ALMMo-0 classifer

As shown in 6.1, The proposed biometric system, which relies on Face-based multi-model approach, predominantly utilizes the ALMMo-0 Classifer. Therefore, the following section outlines the primary architecture of the ALMMo-0 classifier alongside its fundamental algorithm. The ALMMo-0 classifier represents an innovative machine learning technique capable of autonomously constructing its multi-model framework. Initially, it automatically identifies focal points from empirical data and organizes data clouds through Vernoi Teselation [79] on an individual basis. It then creates sub-classifiers for different categories using AnYa Fuzzy Rule-based (FRB) from the non-parametric data clouds, enabling the classification of future data. This section comprehensively introduces both authentication and verification procedures.

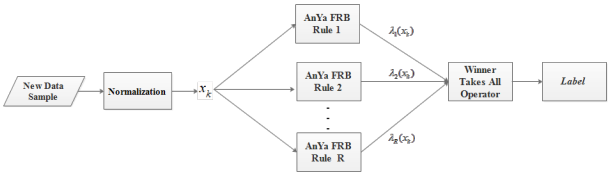


Figure 6.1: An illustrative frame diagram of ALMMo-0 Classifier

6.1.2 The main algorithm of ALMMo-0 classifier

The key notation used to introduce the ALMMo-0 classifier algorithm is summarized in 6.1. The principal algorithm employed by the ALMMo-0 classifier entails the initial normalization of input data, achieved by dividing each data sample by its respective norm. Subsequently, the algorithm designates the first data sample as the model for the first data cloud, setting its support value to 1. An essential step in the algorithm involves computing the global mean and density of the data models. In cases where the density of a new data sample surpasses the maximum or falls below the minimum density of existing models, a new data cloud is created with the new

Notation	Signification
$x^{(*i)}$	The point of convergence.
Class^i	The corresponding class of the i^{th} data cloud.
R	The number of fuzzy rules.
C	A set of different classes in the data set.
R^d	The Euclidean data space.
x_i	The data set observed at the i^{th} instance.
x_k	New coming data.
u_k	The global mean of all the data samples at the k^{th} time instance.
λ_i	Confidence score.
x_k^i	The k^{th} normalized data sample of the i^{th} class.
μ_k	The global mean.
$D_k(x_i)$	The unimodel density of the i^{th} data sample at the k^{th} time instance.
X_k	The Average Scalar Product.
$M_{(F^i)}^{(*i)}$	Number of members of data clouds.
$r_{(F^i)}^{(*i)}$	The Radius of influence of the area.
$x_N^{(*i)}$	The point of convergence of the nearest data cloud.
F^i	Number of points of convergence.

Table 6.1: A signification of notation of ALMMo-0 classifier

sample as its model. Alternatively, the algorithm identifies the nearest model (data cloud) to the new sample, updating the model's support and radius accordingly. In summary, the ALMMo-0 process encompasses four primary steps:

1. Step 1: Normalization of incoming data.

2. Step 2: Initialization of meta-parameters.

3. Step 3: Classification, which includes computing the global mean and density.

4. Step 4: Involves assigning labels to validation data by sending it to all AnYa FRB Sub-classifiers corresponding to class C and evaluating the confidence score for each sub-classifier.

After all AnYa FRB Sub-classifiers generated their scores of confidence the "Winners Takes All" strategy will be used to assign the data to the class most likely to be associated with as

Algorithm 2 The main Algorithm of ALMMo-0 Classifier

while there is a new coming data sample **do**
  Normalization:
  $x_k^i \leftarrow \frac{x_k^i}{\|x_k^i\|}$
  Initialization:
  if $k = 1$ **then**
    $\mu_1^i \leftarrow x_1^i$
    $F^i \leftarrow 1$
    $M_1^{(*i)} \leftarrow 1$
    $x_1^{(*i)} \leftarrow x_1^i$
    $r_1^{(*i)} \leftarrow r_0$
  else
    Updating μ_{k-1}^i **to** μ_k^i: $\mu_1 \leftarrow x_1$
    Calculate the unimodel density D_k **of the data sample** x_k^i:
    $D_k = \exp(-\frac{1}{2}\|x_k - x_j^*\|^2)$
    Update $D_k(x_k^{(*i)})$ **for** $j = 1, 2, \ldots, F^i$
    $D_k(x_k^{(*i)}) = \exp(-\frac{1}{2}\|x_k - x_j^*\|^2)$
    if $D_k(x_k^i) > \max_{j=1,2,\ldots,F}(D_k(x_j^{(*f)}))$ **or** $D_k(x_k^i) < \max_{j=1,2,\ldots,F}(D_k(x_j^{(*f)}))$ **then**
      Create a new data cloud around x_k^i **and initialize the parameters:**
      $F^i \leftarrow F^i + 1$
      $x_{F^i}^{(*i)} \leftarrow x_k^i$
      $M_{F^i}^{(*i)} \leftarrow 1$
      $r_{F^i}^{(*i)} \leftarrow r_0$
    else
      Find the nearest data cloud to x_k^i:
      $x_N^{(*i)} \leftarrow \arg\min_{j=1,2,\ldots,F^i}(\|x_k^i - x_j^{(*i)}\|)$
      if $\|x_k^i - x_N^{(*i)}\| \leq r_N^{(*i)}$ **then**
        Update the meta parameters of the data cloud:
        $x_N^{(*i)} \leftarrow \frac{M_N^{(*i)}}{M_N^{(*i)}+1} x_N^{(*i)} + \frac{1}{M_N^{(*i)}+1} x_k^i$
        $r_N^{(*i)} \leftarrow \sqrt{0.5\left((r_N^{(*i)})^2 + (1 - \|x_N^{(*i)}\|^2)\right)}$
      else
        Add new data cloud:
        $F^i \leftarrow F^i + 1$
        $x_{F^i}^{(*i)} \leftarrow x_k^i$
        $M_{F^i}^{(*i)} \leftarrow 1$
        $r_{F^i}^{(*i)} \leftarrow r_0$
      end if
    end if
  end if
end while

follows:

$$\text{If } (x_k \sim x_j^*) \quad \text{then} \quad \text{Rule}^j \quad (1) \tag{6.1}$$

$$\lambda_j = \exp\left(-\frac{1}{2}\|x_k - x_j^*\|^2\right) \tag{6.2}$$

$$\text{label} = \arg \max_{i=1,2,\ldots,k} (\lambda_i) \tag{6.3}$$

6.1.3 Computational complexity

The complexity analysis of the ALMMo-0 classifier may vary based on the time and space complexity of two key functions: the Identification Function, which recognizes the model (data cloud) in the input data. This function has a time complexity of O(L*NoC*W), where L represents data samples, NoC is data clouds, and W is features; the space complexity is O(L*W), needed to store input data. The Verification Function then utilizes the model from the Identification Function to classify new data samples. Its time complexity is O(L*NoC), with space complexity of O(NoC) to store the model and labels.

Consequently, the overall time and space complexity of the ALMMo-0 classifier is primarily impacted by the Identification Function's complexity of $O(L * NoC * W)$ and space complexity of $O(L * W)$. Nonetheless, the actual complexity also relies on input data characteristics and the number of identified data clouds. Thus, the ALMMo-0 classifier exhibits a linear or sub-linear complexity, making it ideal for extensive datasets. Additionally, in comparison to the popular SVM with a complexity range of $O(N^2 * D)$ to $O(N^3 * D)$ (N as training sample number and D as feature number), the ALMMo-0 Classifier typically has lower complexity. In summary, the ALMMo-0 classifier offers reduced computational complexity, enabling its adaptability to large datasets, management of high-dimensional feature spaces, and resolution of intricate classification tasks.

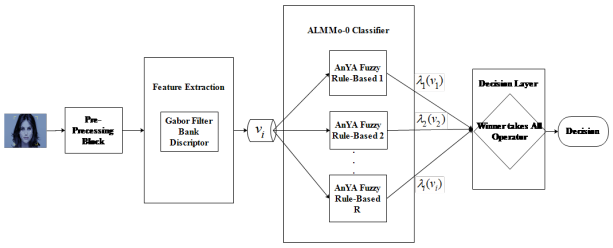


Figure 6.2: Block diagram of the proposed method.

6.1.4 The proposed biometric system-based ALMMo-0 classifier architecture

The global architecture of the proposed system is demonstrated in 6.2, where Gabor Filter Bank is utilized for feature extraction and ALMMo-0 classifier for classification. The main architecture comprises four principal steps: face image acquisition, pre-processing phase for feature extraction, utilization of Gabor Filter Bank descriptor, and classification by ALMMo-0 based on relevant features.

In the biometric system, the ALMMo-0 classifier automatically categorizes new data using relevant features extracted by the Gabor Filter Bank. ALMMo-0 forms linguistic rules, builds a multimodel structure, identifies convergence points, creates shape-free data clouds, establishes sub-classifiers based on AnYa fuzzy rules, generates confidence scores for each class, and utilizes a ”winner takes all” strategy for labeling new data samples.

The various steps of the proposed approach using the ALMMo-0 classifier in 6.2 can be summarized as follows:

1. Pre-processing Layer: Basic methods like normalization, rotation, scaling, and image segmentation are required by the ALMMo-0 classifier.

2. Feature extraction Layer: Our methodology utilizes the Gabor-Filter Bank descriptor due to its high performance with face databases.

3. Classification Layer: The ALMMo-0 classifier in our approach builds sub-classifiers using AnYa Fuzzy Rule-based on non-parametric data clouds and generates confidence scores for each sub-classifier.

4. Decision Maker Layer: Based on confidence scores from each sub-classifier, the system assigns labels to new data samples corresponding to the most probable class.

Classification process with ALMMo-0

The main objective of the classification phase is to make the accurate decision regarding whether the individual is a legitimate or an imposter. The innovative approach of ALMMo-0 Classifier will be utilized in this stage due to its effectiveness and high level of explainability. The ALMMo-0 classifier consists primarily of a group of Anya fuzzy rule-based sub-classifiers, which can be differentiated from MAMDANI and TAKAGI Type by its unique feature of including an antecedent part in the form of a simplified and refined victor. This part mainly encompasses the focal point of the data cloud used for rule construction. The concept of data cloud involves a collection of data fragments sharing a common feature centered around a focal point, similar to Voronoi tessellation. Consequently, the data clouds and respective focal points of the ALMMo-0 classifier form the precursor of the "IF PART" in the fuzzy rule, representing the 0-order fuzzy rule as depicted below:

Since we are employing the Euclidean distance in our study, the dataset in the Euclidean space is defined as follows:

$$\{x\} = \{x_1, x_2, \ldots, x_k\} \tag{6.4}$$

Following the establishment of its primary structure, automatic formation of data clouds based on the observed data, and creation of sub-classifiers corresponding to each class in the Anya fuzzy rule-based format from the non-parametric data clouds, the ALMMo-0 classifier initiates the learning process by transmitting the extracted normalized feature vector of the image $v_i, (i = 1, 2, .., k)$to all AnYa FRB sub-classifiers. Subsequently, it computes the confidence scores $\lambda_i(v_i)$ for each AnYa FRB sub-classifier related to the image v_i.

decision layer

The decision layer is primarily composed of two main steps. Initially, the "winner-takes-all strategy" is applied by calculating label $= \arg\max_{i=1,2,\ldots,k}(\lambda_i)$. A high confidence score in-

Database	Accuracy	Sensitivity	Specificity	Training time (ms/per)
JAFFE	100.00%	100.00%	100.00%	0.031
FACES95	93.89%	90.00%	93.94%	0.0213
FACES94	100.00%	100.00%	100.00%	0.137
FACES96	98.61%	100.00%	98.60%	0.409
Grimace	100.00%	100.00%	100.00%	0.008
Georgia Tech face	82.75%	75.00%	82.91%	0.002
CASIA	64.73%	50.00%	64.76%	0.081
ORL	98.00%	100.00%	97.95%	0.004
Yale Face	100.00%	100.00%	100.00%	0.002

Table 6.2: Accuracy, Sensitivity, and Specificity of the biometric system based-ALMMo-0 classifier.

dicates a greater likelihood of influencing the new image to the relevant class. Subsequently, The system assigns the new image to the most probable class. Ultimately, a decision is reached regarding whether the user is authentic or an imposter.

6.1.5 Experiments and results

In this section, the outcomes of the conducted experiments on facial modality using the ALMMo-0 classifier and Gabor Filter bank across nine different databases are presented, alongside a comparative analysis demonstrating the superior performance of the proposed system in contrast to other traditional machine learning methods. The comparison focuses on ALMMo-0, NN, and SVM Classifiers.

Transitioning to 6.2, the results derived from the experimental data on the proposed facial recognition biometric system utilizing the ALMMo-0 classifier are evident. The 6.2 clearly indicates the high level of performance achieved by our proposed methodology, notably showcasing 100.00% accuracy and 0.00 error rate for 4 out of the 9 investigated databases, with minimal execution times of: 0.0310 MS/Per, 0.137 MS/Per, 0.008 MS/Per, 0.002 MS/Per for JAFFE, FACES94, Grimace, and Yale Face databases respectively. Essentially, this signifies the system's ability to accurately categorize individuals based on their facial characteristics with a 100% accuracy rate. Furthermore, five databases among the total number demonstrated an accuracy exceeding 93% with short training durations. Additionally, 6.2 also highlights a

notably high sensitivity and specificity, surpassing 90% sensitivity in seven databases and over 93% specificity in seven different databases, indicating the system's effectiveness in rejecting unauthorized individuals and thereby showcasing its high performance.

Further examination detailed in 6.3 underscores the efficacy of the proposed facial recognition biometric system employing the ALMMo-0 Classifier, showcasing superior accuracy in both verification and identification modes compared to NN and SVM Classifiers across nine diverse databases. Notably, the combination of Gabor filter bank + ALMMo-0 classifier has surpassed NN and SVM classifiers, achieving a rank of 93.89% compared to 93.19% and 92.5% for the Faces95 database respectively, as depicted in 6.4. Similarly, 6.6 demonstrates the system's ability to make correct decisions regarding individuals, outperforming NN and SVM classifiers with a rank-1 up to 98.61% using ALMMo-0, as opposed to the 98.41% rank-1 provided by NN classifier and 97.95% by SVM in the Faces96 database. Moreover, the Georgia Tech face database also highlights the efficiency of our proposed approach, yielding a result of 82.75% as opposed to 82.50% and 80.00% from the NN and SVM classifiers respectively, as evident in 6.8. The CASIA database yielded the most optimal outcomes, with a Rank of 64.73% achieved

Database	**ALMMo-0 Classifier Rank (%)**	**ALMMo-0 Classifier EER (%)**	**SVM Classifier Rank (%)**	**SVM Classifier EER (%)**	**NN Classifier Rank (%)**	**NN Classifier EER (%)**
JAFFE	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%
Faces95	93.89%	2.09%	92.50%	2.64%	93.19%	1.96%
Faces94	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%
Faces96	98.61%	0.23%	97.95%	0.53%	98.41%	0.20%
Grimace	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%
GTdb crop	82.75%	6.01%	80.00%	8.75%	82.50%	5.93%
CASIA	64.73%	33.37%	55.61%	32.28%	62.02%	12.70%
ORL	98.00%	0.50%	97.50%	1.00%	98.00%	0.50%
YALE15	100.00%	0.00%	98.67%	1.33%	100.00%	0.00%

Table 6.3: Performance comparison across different classifiers

by the proposed method in comparison to 62.02% by the NN classifier and 55.61% by the SVM classifier, as illustrated in 6.9. The proposed method exhibited 100% accuracy and 0.00% Equal Error Rate in the instances of YALE, JAFFE, Faces 94, and Grimace datasets, showcasing a sig-

nificant performance enhancement. These findings are similar to outcomes documented for the renowned NN and SVM classifiers.

Moreover, the proposed methodology stands out for its full autonomy and exceptional interpretability. Despite similar accuracy levels in a subset of the nine databases, the ALMMo-0 Classifier of the proposed method maintains a crucial edge in terms of transparency, unlike the opaque nature of NN and SVM classifiers. The interpretability challenge arises from the inscrutable nature of weights and biases acquired by the network, contrasting with the straightforward interpretability of classical algorithms like NN and SVM Classifiers. This limitation restricts their utility in contexts prioritizing interpretability, such as medical diagnoses or financial projections. Conversely, the proposed system operates autonomously and learns directly from provided images, facilitating straightforward interpretation and offering a hierarchical structure for users to comprehend decision-making processes based on input features. Additionally, the ALLMo-0 Classifier excels in handling sparse data and categorical attributes more efficiently than NN and SVM classifiers. Consequently, the results presented underscore the proposed method as a robust alternative to established classification techniques.

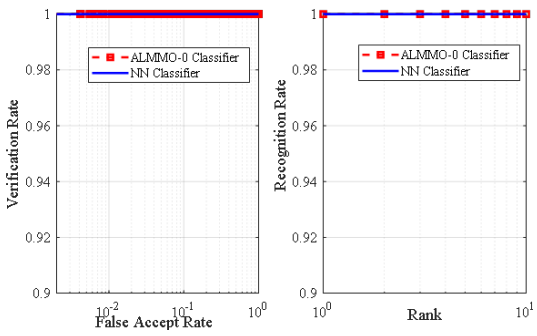


Figure 6.3: ROC and CMC curves for Jaffe database.

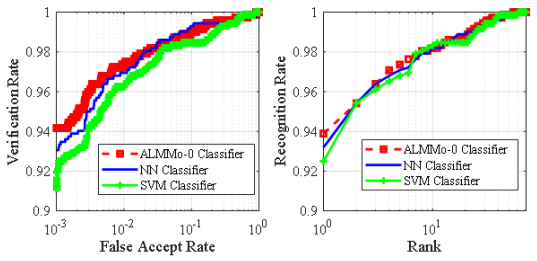


Figure 6.4: ROC and CMC curves for Faces95 database.

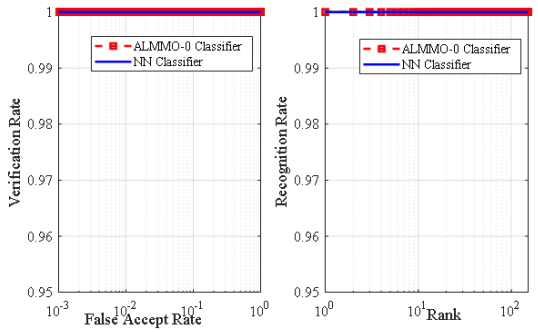


Figure 6.5: ROC and CMC curves for Faces94 database.

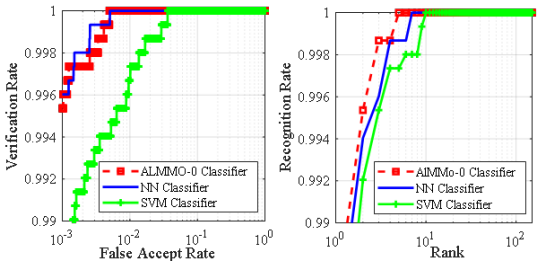


Figure 6.6: ROC and CMC curves for Faces96 database.

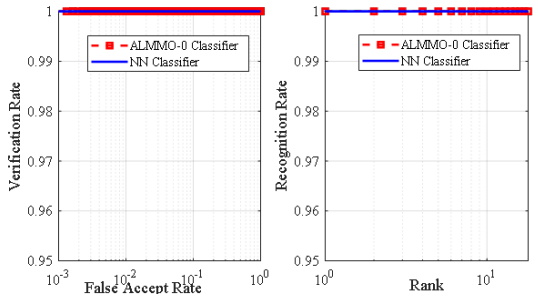


Figure 6.7: ROC and CMC curves for Grimasse database

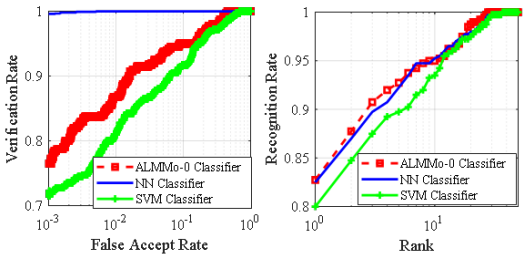


Figure 6.8: ROC and CMC curves for GTdb cropped$_f aces database$.

Comparison with other methods

The performance of the proposed approach utilizing the ALMMo-0 classifier was demonstrated compared to NN and SVM Classifiers in 6.3. This section delves into a comprehensive comparative study analysis of the data presented in 6.4, aiming to enhance the efficiency of the

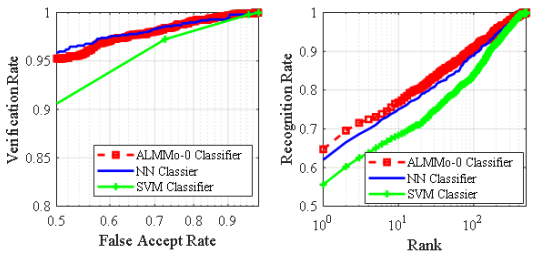


Figure 6.9: ROC and CMC curves for CASIA database.

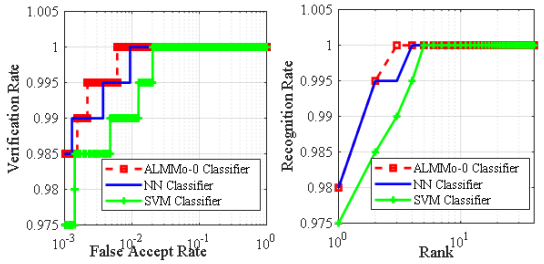


Figure 6.10: ROC and CMC curves for ORL database.

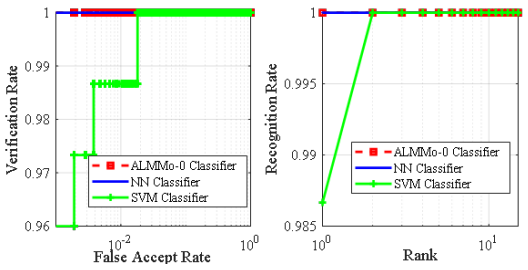


Figure 6.11: ROC and CMC curves for YALE database.

methodology. Our approach exhibits superior accuracy in comparison to the SVM Classifier in other classifiers when tested on Face96 and Grimace databases, as well as in [89] and [91] with the ORL database.

Similarly, an in-depth quantitative analysis on individual face traits using the JAFFE database showcases the outperformance of our Based-ALMMo-0 classifier approach over Gaussian process and CNN methods. The accuracy levels achieved by ALMMo-0 surpass those of other methods, such as Local Binary Pattern [84] and Deep Learning [85] on the Face95 database. Notably, our proposed approach achieves a higher accuracy level compared to existing methodologies. Furthermore, when tested on the Face 94 databases, our approach outperforms the Local Binary Patterns (LBP) method [87] and the Local Binary Pattern Network (LBPNet) [88]. The biometric system based on the ALMMo-0 classifier also outshines DWT+ HOG, SVM+ HOG, and Adaboost+ LBP methodologies when tested on the Grimasse database.

Database	Reference	Methods	Accuracy
4*Jaffe	[80]	GP classifiers (Gaussian approach)	93.43%
	[81]	Convolutional Neural Network (CNN)	78.1%
	[82]	Convolutional neural network (CNN)	65.00%
	The proposed method	ALMMo-0 Classifier	100%
4*Face95	[83]	ORB 2 -IPR Framework	88.13%
	[84]	Local Binary Pattern	92.7%
	[85]	DL system (Deep Learning) used the Face 95 database separately	88.51%
	The proposed method	ALMMo-0 Classifier	93.00%
4*Face94	[86]	DL system (Deep Learning)	99.4%
	[87]	Local binary patterns (LBP)	98.30%
	[88]	Local Binary Pattern Network (LBPNet)	99.00%
	The proposed method	ALMMo-0 Classifier	100%
4*ORL	[89]	SIFT+SVM	97%
	[90]	Firefly algorithm	97.75%
	[91]	HOG+SVM	95.50%
	The proposed method	ALMMo-0 Classifier	98.00%

Table 6.4: Comparison with other methods

The quantitative analysis highlights the superior performance and effectiveness of the proposed ALMMo-0 classifier approach for face recognition when compared to traditional machine learning methods. The aim of the proposed method is to enhance verification performance, achieving high accuracy, sensitivity, and specificity with low error rates and computational complexity. These results underscore the discriminatory and representative capabilities of the biometric system based on the ALMMo-0 classifier.

6.1.6 Conclusion

This research endeavor aimed at the development of a biometric system designed for face recognition utilizing a novel ALMMo-0 classifier. The primary research discovery can be succinctly encapsulated as follows: One of the most notable revelations arising from this investigation is that the AnYa fuzzy rule-based classifier of zero order (ALMMo-0) yields noteworthy outcomes in the realm of face recognition, both in terms of identification and verification modes, boasting an accuracy level exceeding 93% across the majority of the scrutinized databases. By leveraging the fuzzy rule-based classifier (ALMMo-0), the proposed biometric system demonstrates superior performance compared to the widely-used neural network and SVM classifiers when exploiting Faces95, Faces96, GTdb-crop, CASIA, and ORL databases.

Experimental validation and numerical illustrations corroborate the exceptional performance of

the ALMMo-0 classifier in face recognition classification specifically, and in the broader domain of biometrics, achieving remarkable results across nine distinct face databases with a high degree of accuracy and an insignificant error rate. The proposed biometric system exhibits a linear complexity, enhancing its capability to tackle intricate problems with extensive datasets more effectively than systems relying on NN and SVM classifiers, known for their elevated time and space complexity. Furthermore, a comparative analysis conducted in this study underscores the superiority of ALMMo-0 in utilizing the face modality compared to prior research endeavors. The ALMMo-0 emerges as a promising alternative to established classification methodologies. Additionally, in contrast to traditional machine learning approaches, the ALMMo-0 offers enhanced interpretability owing to its AnYa fuzzy rule-based framework, positioning it as a potent and efficient tool in comparison to existing algorithms.

Prospective research endeavors could leverage advanced multi-model systems based on the ALMMo-0 classifier to explore alternative modalities such as fingerprint, iris, and voice recognition. The ALMMo-0 classifier also holds promise for addressing more intricate challenges, such as handwriting classification. Further extensions of the ALMMo-0 architecture could be pursued to tackle increasingly complex issues, including the handling of streaming data challenges and addressing the classification of imbalanced data that may evolve over time.

6.2 A Biometric system based fuzzy-Rule based Classifier for finger knuckle print (FKP)

This paper introduces an original biometric recognition system based on knuckle fingerprint (FKP) modality that utilizes a fuzzy-rule based classifier to determine the authenticity of the user's identity. The system extracts discriminative features from the FKP image using Binary Similarity-based Iterative Fusion (BISIF) descriptor to enhance the effectiveness of biometric identification. It then applies a powerful fuzzy-rule based classifier that is autonomous, non-iterative, and fully explainable to accurately establish the individual's identity based on FKP characteristics. Experiments on the public PolyU FKP dataset demonstrate that the proposed

system surpasses the classical methodology in accuracy, presenting results in rank-1, cumulative match curve (CMC), equal error rate (EER), and receiver operating characteristic (ROC) curves. The proposed system achieves a high level of accuracy up to 98% in both identification and verification modes.

Biometrics refers to automated recognition that exploits the unique physical and behavioral characteristics of individuals to verify their identities. With technological advancements, biometrics has become essential for enhancing security and safeguarding personal and professional information in various fields such as Law Enforcement, Access Control, Border Control, Travel, Mobile Devices, Payments, Smart Homes, and Healthcare. These systems utilize characteristics like Face, Iris, Fingerprint, and voice to verify identities. Hand knuckle fingerprint (FKP) biometrics is increasingly promising due to its stability, as the knuckle area is less affected by aging compared to fingerprints. Effective classification algorithms are crucial for accurately identifying and verifying users using these traits. Traditional machine learning methods rely on mathematical models and probabilistic distributions, which establish static boundaries between classes without considering uncertainty and imprecisions in decision-making. Fuzzy-rule based classifiers, on the other hand, leverage fuzzy logic to handle uncertainty and imprecision by using linguistic rules to classify input features based on their degree of membership, allowing for flexible transitions between classes. The main goal of this research is to propose a knuckle fingerprint (FKP) biometric system based on a fuzzy-rule based classifier to achieve high accuracy. The system utilizes B-SIF descriptor for feature extraction and an efficient 0-order Autonomous Learning Multiple Model (ALMMo-0) classifier for automatic classification.

6.2.1 The proposed FKP biometric system

The primary structure of the proposed approach utilizes the BISIF descriptor primarily for extracting the pertinent features from the ROIs. The fuzzy rule-based classifier (ALMMo-0) is used for classification. The key steps of the classification process are outlined in figure 6.12. The proposed method consists mainly of four crucial steps. It commences with acquiring the FKP data, followed by extracting the region of interest (ROI). Subsequently, the BISIF descrip-

tor is utilized to extract the most relevant features. These features are then forwarded to the fuzzy-rule based classifier (ALMMo-0) to determine whether the user is genuine or an impostor.

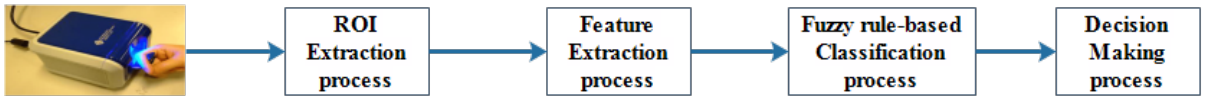


Figure 6.12: The main steps of the proposed biometric system based on fuzzy rule-based classifier

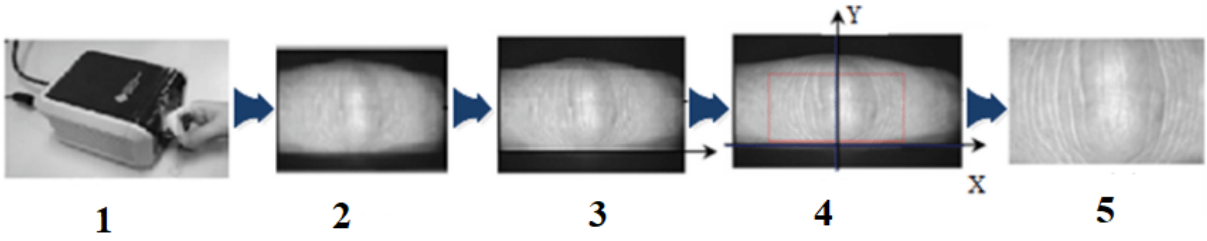


Figure 6.13: The process of ROI extraction from the FKP image

ROI Extraction

The region of interest, known as ROI, refers to the specific area containing the unique knuckle ridges and patterns of the individual, which are utilized for biometric analyses and identification. Enhancing the accuracy of the verification process in the biometric system is achieved through the extraction of ROI. Figure 6.13 demonstrates the key steps involved in extracting the ROI in the proposed system, following the extraction protocol suggested by [92].

1. **S**tep 1: Applying the operation of aussian smoothing on the FKP image, down-graded after that to 150 dpi (Dots Per Inch).

2. **S**tep 2: establishing the X-axis of the coordinate system and extracting the finger's lower edge by the canny edge detector.

3. **S**tep 3: Applying the canny edge detector to determine the Y-axis of the coordinate system, the canny edge detector will be applied on the cropped sub-image which has been extracted from the original FKP image based on X-axis, this step contributes mainly to find the outward curve coding scheme.

4. **S**tep 4: the selected ROI (inside the rectangle) is obtained.

Feature Extraction

The proposed biometric system utilizes the Binary Similarity and Intensity Feature (BISIF) descriptor to extract the most significant features for later consideration in determining the authenticity of a user. BISIF is effective in extracting features despite changes in illumination and rotation, relying on an unsupervised approach to generate a set of filters through Independent Component Analysis (ICA). Each pixel in the FKP image is converted into a binary string based on its response to these learned filters. This binary string serves as a local descriptor for the texture pattern within the image. Overall, BISIF apply a set of filters that can measure the configuration of the neighborhood of the central pixel. Hypothesize an image I with a size of $x \times y$ and a $\varphi_i^{k\times k}$ BISIF Filter, the responses can be represented as follow :

$$r_i = \sum_{x,y} \varphi_i^{k\times k} I(x, y) \tag{6.5}$$

where $\varphi_i^{k\times k}$ denotes the linear filter of size k and $i = \{1, 2, .., y\}$ represents the filter's number that are independent statistically, in order to generate the binary string, the y filter's responses can be calculated and binarized together, while the binary string can be represented as follow:

$$b_i = \begin{cases} 1 & \text{if } r_i > 0 \\ 0 & \text{otherwise} \end{cases} \tag{6.6}$$

the characteristics are created as a histogram made up of a series of pixels with binary code.

Fuzzy-rule based classification

To ensure the accurate determination of the authenticity of a user, a fuzzy-rule-based classifier has been implemented. This classifier is autonomous, data-driven, and offers high explainability, in contrast to traditional classification methods. By leveraging fuzzy logic, the fuzzy

rule-based classification establishes rules that enable effective handling of uncertainty and imprecision within the data. The classification process commences with the utilization of observed data to construct a data cloud architecture. Subsequently, non-parametric data clouds are employed to create a series of sub-classifiers associated with each class in a fuzzy rule-based format. The learning phase of our fuzzy rule-based classifier involves transmitting extracted features to all sub-classifiers. Each sub-classifier independently generates a confidence score, denoted as $\lambda_i(v_i)$ for each corresponding image v_i. Finally, a winner-takes-all approach is utilized to determine whether a user is genuine or an impostor.

Decision making

the ultimate determination regarding the validation or refusal of the user's authorization is reached through the application of the "winner takes all" principle as outlined by a specific equation.6.7:

$$label = argmax(v_i)_1, 2, .., k \tag{6.7}$$

where $i = 1, 2, ..K$ denotes the number of the images and v_i represent the current image.

6.2.2 Experiments and results

The outcomes of our conducted experiments on four distinct FKP databases (RMF, RIF, LMF, LIF) utilizing a fuzzy rule-based classifier in conjunction with the BISIF descriptor have been displayed in Table 6.5. The outcomes of the BISIF-ALMMo-0 Classifier, utilizing the FKP

Table 6.5: results of applying ALMMo-0 Classifier in form of Rank and EER.

DATABASE	ALMMo-0 CLASSIFIER	
	Rank(%)	EER (%)
RMF	98.18%	0.52%
RIF	96.67%	1.04%
LMF	98.28%	0.52%
LIF	97.88%	0.78%

modality, demonstrate the exceptional efficacy of our biometric system, achieving an accuracy

level exceeding 96% across all evaluated databases.

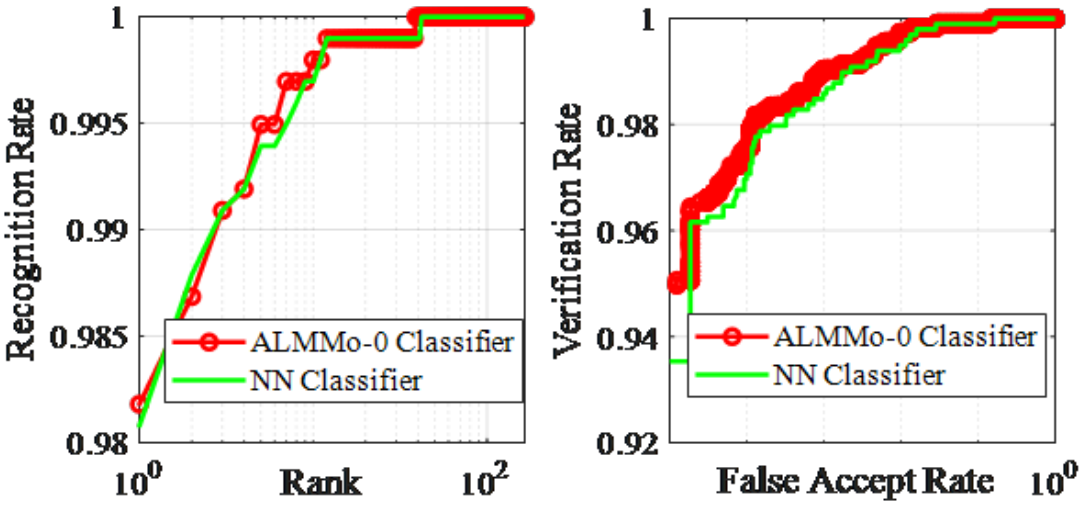


Figure 6.14: ROC and CMC of RMF Database.

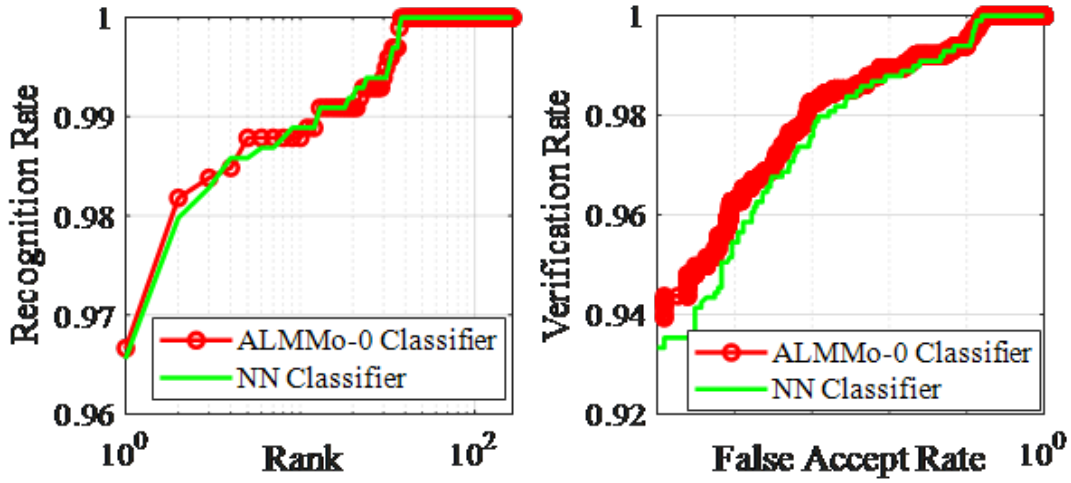


Figure 6.15: ROC and CMC of RIF Database.

Table 6.6: comparative study between ALMMo-0 Classifier and NN Classifier.

DATABASE	ALMMo-0 CLASSIFIER		NN CLASSIFIER	
	Rank (%)	EER(%)	Rank(%)	EER(%)
RMF	98.18%	0.52%	98.08%	0.61%
RIF	96.67%	1.04%	96.57%	1.21%
LMF	98.28%	0.52%	98.08%	0.68%
LIF	97.88%	0.78%	97.88%	0.82%

The subsequent analyses, as outlined in 6.6, present the efficacy of the proposed fuzzy rule-based biometric system, surpassing the well-known NN classifier with a ranking of 98.18%

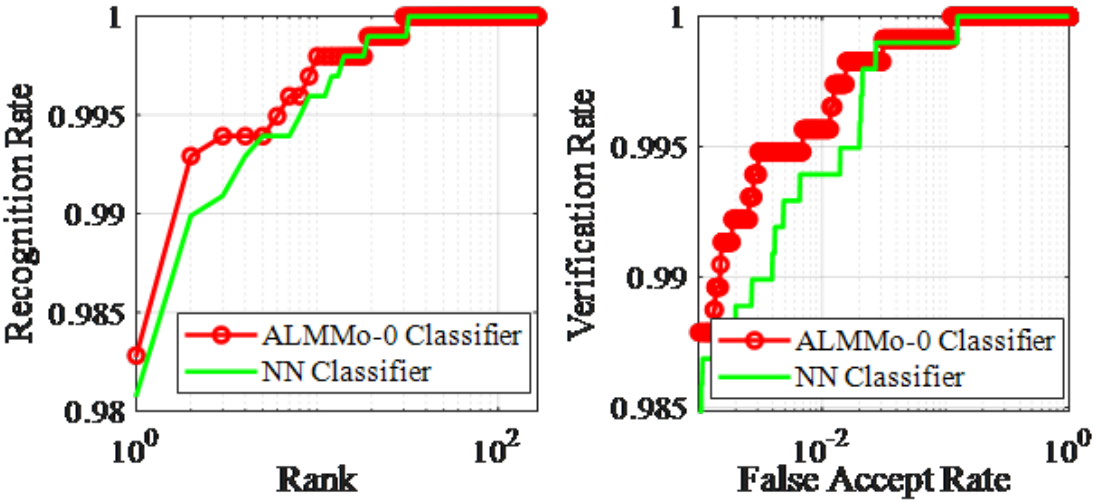


Figure 6.16: ROC and CMC of LMF Database.

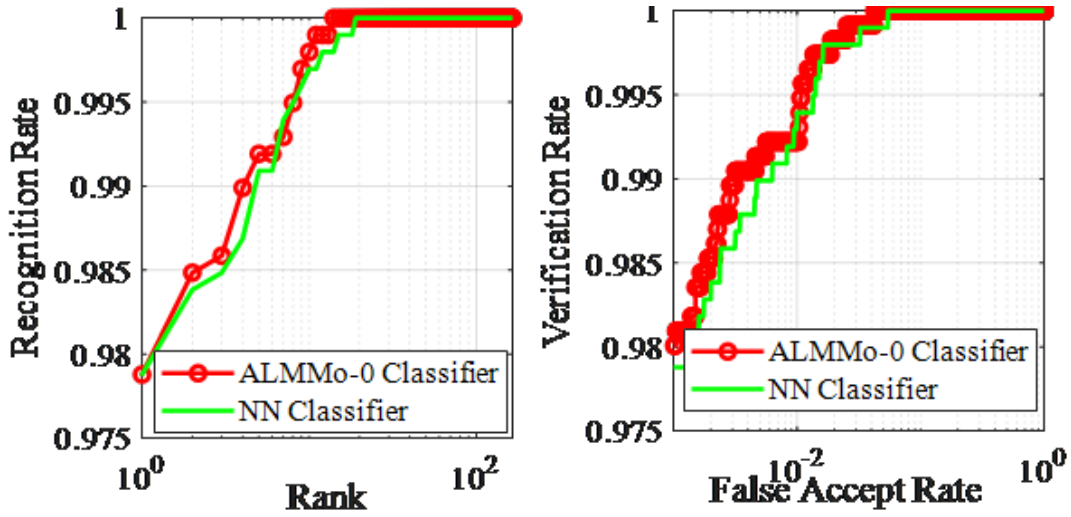


Figure 6.17: ROC and CMC of LIF Database.

compared to the NN Classifier's 98.08% using the RMF database, as depicted in 6.14. Moreover, through the utilization of the RIF database, our proposed biometric system has achieved an accuracy level of 96.67%, outperforming the NN classifier which attained 96.57%, as illustrated in 6.15. Our proposed system has also yielded intriguing outcomes, demonstrating a 98.28:% accuracy level employing the LMF database, while the NN classifier only reached 98.08%, as displayed in 6.16. Overall, the proposed biometric system utilizing a fuzzy rule-based classifier has not only attained a comparable high accuracy level to the renowned NN classifier using the LIF database, as shown in 6.17, but has also surpassed the NN classifier across RMF, LMF, and RIF databases. This highlights the superior performance of the proposed system and affirms its

potential as a viable alternative to traditional machine learning methods.

Comparison with the classical methods

Table 6.7: Comparison with the classical methods.

DATABASE	References	Method	Accuracy
RMF	[93]	Deep Learning(PCAnet+SVM)	95.15%
	[94]	B-BSIF	98.08%
	Our work	ALLMo-0 Classifier	98.18%
RIF	[93]	Deep Learning(PCAnet+RFT)	91.91%
	[94]	B-BSIF	96.57%
	Our work	ALLMo-0 Classifier	96.67%
LMF	[93]	Deep Learning(PCAnet+SVM)	97.30%
	[94]	B-BSIF	98.08%
	Our work	ALLMo-0 Classifier	98.28%
LIF	[93]	Deep Learning(PCAnet+SVM)	95.75%
	[94]	B-BSIF	97.88%
	Our work	ALLMo-0 Classifier	97.88%

the performance of the proposed work, as demonstrated in 6.7, is noteworthy as it surpasses results from other classification methods. The fkp based-ALMMo-0 classifier in the biometric system shows higher accuracy than the method using deep learning by [93] across four databases: RMF, RIF, LMF, and LIF. It also outperforms the results from [94] which used the same databases but with different BISIF descriptor sizes (17X17).

In comparison to existing biometric systems, the proposed system proves to be effective.

Conclusion

In this study, the ALMMo-0 Classifier's effectiveness is harnessed to develop a novel biometric system utilizing the FKP modality. This zero-order fuzzy rule-based classifier yields compelling results when applied to FKP in both identification and verification modes, achieving accuracy levels exceeding 96% across all evaluated databases. Moreover, the biometric system solely relying on the ALMMo-0 classifier demonstrates superior performance compared to neural networks and SVM classifiers.

The experiments conducted highlight the efficacy and remarkable performance of the ALMMo-

0 classifier within FKP classification and the broader biometric domain. The FKP-based biometric system proposed in this study delivers reliable results with minimal errors, showcasing the explainability inherent in ALMMo-0's Fuzzy Rule-Based architecture. This positions ALMMo-0 as a robust alternative to conventional classification algorithms.

Future research in biometrics may explore additional modalities such as fingerprint, retinal, and DNA matching. ALMMo-0 could also be investigated for solving more intricate handwriting classification tasks and handling uncertain data.

6.3 Explainable Deep Neural Networks Classifier for Robust face recognition

In recent years, there has been a significant increase in the utilization of face recognition in various applications and research fields. However, challenges arise in terms of security and privacy when dealing with biometric system-based face images. These challenges stem from limitations such as data quality, sensitivity to noise, lack of universality, and the opaque nature of the process. Therefore, there is a clear necessity to explore new artificial intelligence-based methods to enhance system performance. This study examines the implementation of an Explainable Deep Neural Networks Classifier (xDNN) for biometric authentication using facial traits. The proposed deep-learning architecture merges reasoning and learning concepts in a novel manner. The xDNN, as a non-parametric and non-iterative classifier, offers high efficiency in terms of time and computational resources, ultimately providing a dependable biometric authentication solution in performance aspects.

The advancement of information security technology in recent times has led to a surge in risks faced by systems and their resources, highlighting the urgent need for enhanced security measures and faster, more reliable user authentication methods. This evolving landscape has posed challenges in terms of security due to rapid advancements in communication, networking, and mobility. Human biometric traits serve as an ideal solution to ensure user identity within systems. Biometric system technologies leverage an individual's distinct physiological

or behavioral characteristics for identification and authentication purposes. Various biometric data, including fingerprints, palmprints, finger knuckle patterns, iris scans, voice recognition, and facial patterns, have been utilized across numerous applications. Consequently, the adoption of biometric systems has increased, attributed to the unique nature of human biometrics, which plays a crucial role in thwarting fraudulent access. Biometric systems typically operate in two modes: identification and verification. Identification involves comparing the input template with all stored templates to correctly attribute the person's identity, while verification compares the input template with an existing template of the same individual, utilizing a set threshold for the matching process. Face recognition technologies continue to evolve rapidly and find widespread application in various scenarios, capitalizing on the benefits of non-contact and non-cooperation, which are favored by researchers. System-based face recognition can be categorized into global image-based systems and local feature-based systems. Privacy and security constitute the primary attributes of individual authentication for controlling access to any system. Traditional machine learning techniques may yield intriguing outcomes in terms of precision. Although deep learning methods have demonstrated remarkable efficacy in facial recognition with a notably high level of performance, they still grapple with a range of drawbacks, including a lack of transparency. This deficiency primarily results in the generation of unjustified decisions by the system, posing a significant challenge in user acceptance and trust. Another major drawback of conventional deep learning approaches lies in the substantial data prerequisites, particularly labeled data, which demand extensive computational resources, alongside high complexity and processing durations. In this study, we aim to propose a novel biometric system utilizing the xDNN classifier based on facial modality. This system is characterized by its complete transparency and explainability owing to its fuzzy architecture, as well as being less intricate and more cost-effective in terms of time and resources due to its non-parametric and non-iterative model.

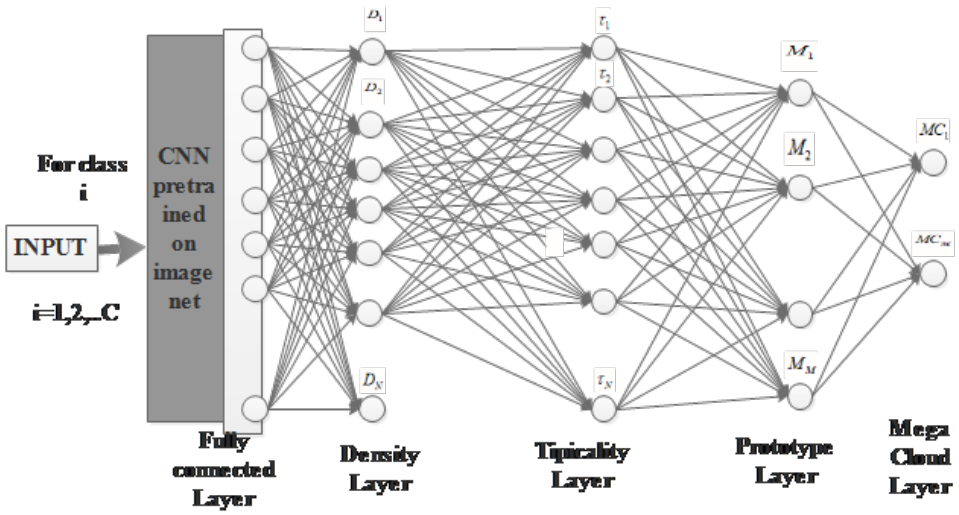


Figure 6.18: The Main architecture of the xDNN Classifier

6.3.1 The xDNN definition and main algorithm

The main architecture of xDNN Classifier

In the bulk of prior studies, statistical learning and reasoning have typically been employed in isolation. However, our study advocates and demonstrates that the collaboration of statistical learning and reasoning can yield a superior outcome. This suggested approach can be interpreted as a feedforward neural network, which integrates an algorithm that autonomously learns and enhances itself progressively by constructing its framework over time. It entails incorporating new models that showcase the dynamic evolution of the data pattern .

As illustrated in Figure 1, xDNN comprises five distinct layers, each playing a specific role in the overall classification process. In the forthcoming sections, a comprehensive definition of each layer along with a depiction of its architecture and sub-process will be provided.

Features descriptor layer: The initial phase of data dimension determination also serves as the primary stage of the proposed technique, focusing primarily on extracting vector features from the image. While numerous feature extraction methods are available, our study concentrates on pre-trained deep neural approaches that possess the ability to extract highly discriminative high-level features. The one utilized in this study is the VGG–VD–16 DCNN with a simplistic structure that can achieve a notable level of accuracy compared to other pre-trained methods. In the VGG–VD–16 DCNN method, the first fully connected layer (FCL) is capable of

accommodating vectors with dimensions of 1 × 4096, where n=4096 (number of features) [two combinations: Gabor Filter Bank/ xDNN and SVM/xDNN]. Following the extraction of pertinent features, the processes of Standardization and normalization are imperative, employing equations 6.9 and 6.10 respectively.

$$Vs_{i,j} = \frac{v_{i,j} - \mu(v_{i,j})}{\sigma(v_{i,j})} \tag{6.8}$$

$$\bar{V}_{i,j} = \frac{Vs_{i,j} - min_i(Vs_{i,j})}{max_i(v_{i,j})} \tag{6.9}$$

The initialization of the Meta-Parameters of the xDNN algorithm involves setting the meta-parameters using the initial incoming data, allowing for independent computation of each class.

$$M \leftarrow 1; \mu \leftarrow \bar{v}_i \tag{6.10}$$

Every class C will be initialized with its first incoming data sample.

$$C_1 \leftarrow \bar{v}_1; m \leftarrow \bar{v}_1; Support_1 \leftarrow 1; r_1 \leftarrow r^*; \bar{I}_1 \leftarrow I_1; \tag{6.11}$$

We derive the expression $r^* = \sqrt{2 - 2\cos(30°)}$ in accordance with [95]. This derivation is elucidated as follows. The concept of Rational r^*, which pertains to data that is inferred rather than being a specific parameter, is most clearly delineated when the angle subtended by two vectors is less than 30° and they are oriented in the same direction denoted by d. Building upon this foundation, we examine two feature vectors that exhibit an angle of less than 30° between them, categorizing them as *"Similar"*. The determination of the direction d is achieved through the utilization of equation 6.12.

$$d(\bar{v}_i, \bar{p}_i) = \left\| \frac{\bar{v}_i}{\|\bar{v}_i\|} - \frac{\bar{p}_i}{\|\bar{p}_i\|} \right\| \tag{6.12}$$

Density Layer

This layer plays a crucial role in establishing the shared proximity among the images within the data space from the layer before it. The data distribution follows a Cauchy pattern when employing the Euclidean distance, as demonstrated in [95] and [96]. The data density is determined through the formula in equation 6.13

$$D(\bar{v}_i) = \frac{1}{1 + \frac{\left\|\bar{v}_i - \mu N\right\|^2}{\sigma_N^2}} \tag{6.13}$$

Density can also be updated online in the following way:

$$D(\bar{v}_i) = \frac{1}{1 + \left\|\bar{v}_i \mu_i\right\|^2 + \sum_i - \left\|\mu_i\right\|^2} \tag{6.14}$$

The scalar coefficient $\sum_i$ can be updated as follows, where μ_i is involved.

$$\mu_i \leftarrow \frac{i-1}{i}\mu_{i-1} + \frac{1}{i}\bar{v}_i \tag{6.15}$$

$$\sum_i = \frac{1}{1-i}\sum_{i-1} + \frac{1}{i}\left\|\bar{v}_i\right\|^2 \sum_1 = \left\|v_1\right\|^2 \tag{6.16}$$

The Density value can be high if and only if the data sample is very close to the global mean, consequently the solid mutual influence between the images in the space of data due to their common adjacency.

Typicality layer

Typicality noted τ is mainly based on the probability distribution function, which is determined by utilizing the equation 6.17.

$$\tau(\bar{v}_i) = \frac{\sum_i^c Support_i D(\bar{v}_i)}{\sum_i^c Support_i \int_{-\infty}^{+\infty} D(\bar{v}_i) d_v} \tag{6.17}$$

The value of τ remains consistently below 1, even when the point $\bar{v} = p_i$.

Models Layer

The model layer serves as the primary basis of the biometric system proposed on the xDNN classifier. Its key role is to offer an interpretable model. xDNN operates independently from any prior assumptions about the data distribution type, including the random nature of data, deriving the current distribution directly from the images. An advantage of the proposed architecture is the autonomy of models from each other, implying that altering the structure of one model by adding a new one does not impact the existing models. In essence, our proposed xDNN is highly advantageous for application development by incorporating new models, ensuring a high level of flexibility and smoothness. The training of our xDNN must be conducted per class to generate a set of models for each class. Consequently, computations are performed for each class individually. These models epitomize the data density inferred from the preceding layer of the algorithm, derived from the feature vectors of the images corresponding to each class. Subsequently, the models are utilized to establish $IF/THEN$ rules as follows:

$R_c : IF(I \sim \Re_M)THENClass_c$

The symbol $\sim$ denotes similarity and the degree of membership, while other symbols are detailed in 6.8 of notation. For each model, only one rule can be formulated, and the rules of the same class can be amalgamated using the logical disjunction symbol "OR" in the following manner:

$R_c : IF(I \sim \Re_1)OR(I \sim \Re_2)OR..OR(I \sim \Re_M)THENClass_c$ We refer to the area surrounding the identified model as Data Cloud [95], where each model defines a data cloud representing all data points around it. The model is not the statistical global mean by definition but can simply be the current image [95]. The proposed algorithm processes and assimilates new incoming data gradually by assigning them to the closest model.

$$j^* = (\left\|\bar{v}_i - p_j\right\|_{j=1,2..P})^2 \tag{6.18}$$

When the following conditions are verified

$$\text{IF } \left(D(\bar{v}_i) \geq \max\left(D(p_j)\right)_{j=1,2,\ldots,P}\right) \text{ OR } \left(D(\bar{v}_i) \leq \min\left(D(p_j)\right)_{j=1,2,\ldots,P}\right) \text{ THEN (add a new data cloud } M \leftarrow \tag{6.19}$$

That indicates that the quantity $\bar{v}_i$ is situated beyond the influence region of p_j and it embarks on a novel paradigm of fresh data clusters with meta-parameters initialized utilizing the equation. 6.20 in the subsequent manner:

$$M \leftarrow M+1; C_M \leftarrow \bar{v}_i; p_m \leftarrow I_i; support_M \leftarrow 1; r_m \leftarrow r_0; \mathfrak{K}_M \leftarrow I_i. \tag{6.20}$$

Alternatively, the parameters of the data cluster can be updated in real-time utilizing equation 6.20. It is crucial to emphasize that all computations of data cluster parameters are performed globally rather than locally, meaning that computations per data cluster are conducted based on data points associated exclusively with particular data clusters.

$$C_{j^*} \leftarrow C_{j^*}+1; p_{j^*} \leftarrow \frac{Support_{j^*}}{Support_{j^*+1}} p_{j^*} + \frac{Support_{j^*}}{Support_{j^*+1}} p_{j^*} \bar{v}_i; \qquad Support_{j^*} \leftarrow Support_{j^*}+1; r$$

Mega Cloud Layer

In the Mega Cloud Layer, the clouds created in the previous model layer merge together if the adjacent models or prototypes share the same labeled class. This layer aims to ensure high interpretability and transparency to the user by combining all models of the same class. The fusion process primarily relies on fuzzy-rule based rules to merge the clouds together as shown below:

$$R_c : IF(\bar{v}_i \sim MC_1)OR(\bar{v}_i \sim MC_2)OR..OR(\bar{v}_i \sim MC_m c)THENClass_c \tag{6.22}$$

Our xDNN learning's phase can be summarized in the algorithm provided below:

Notation	Signification
v	The feature's vector
Vs	The standardized feature Vector of v
I	The current image
i	The image's ID
N	The number of the images
j	The current feature of v
n	The normalized vector of v
μ	The global mean of the class
M	The number of identified models
$\hat{I}$	The identified Model
C_i	The Current Class
p_i	The feature's vector that define the model$\hat{I}$of the Class C_i
$Sopport_i$	The equivalent support (number of members) belonging to the identified Model
r_i	the area of influence's equivalent radius of the Class C_i
σ	The Variance
D	The Density
MC	The Mega Cloud
mc	The number of mega clouds
S	The degree of similarity

Table 6.8: The Notations

6.3.2 Proposed methodology

The suggested study is based on a transparent deep neural network image-based framework, which is examined within a diverse database of facial characteristics that are primarily distinguished by their explainability. Moreover, it introduces layers that can be easily understood by humans. Specifically, the design of our proposed xDNN classifier is completely transparent and clear, making it easy to explain to the end user. The biometric system proposed in 6.19 primarily consists of four main stages:

1. Receiving and standardizing image inputs

2. Initial feature extraction using a gabor filter bank

3. Classification utilizing xDNN: featuring layers such as the Feature layer, density layer, typicality layer, and mega cloud layer

4. The decision-making process.

Algorithm 3 The Main Algorithm of xDNN Classifier

Initialization
Read $\bar{v}_i$, the initial feature vector sample of the image in process I_i of the class c
Initiate $i \leftarrow 1; n \leftarrow 1; M_1 \leftarrow 1; p_i \leftarrow \bar{v}_i; \mu \leftarrow \bar{v}_i;$ Support $\leftarrow 1; r_1 \leftarrow r_0; \hat{I}_1 \leftarrow I_1$
Execution
for $i = 2, \ldots$ **do**
    Read $\bar{v}_i$
    Compute $D(\bar{v}_i)$ and $D(p_j)$ for $j = 1, 2, \ldots, M$ applying equation (9)
    if equation (11) is verified **then**
        Generate rule applying equation (12)
    else
        Apply equation (11) to search for p_j
        Update the rule using equation (13)
    end if
end for

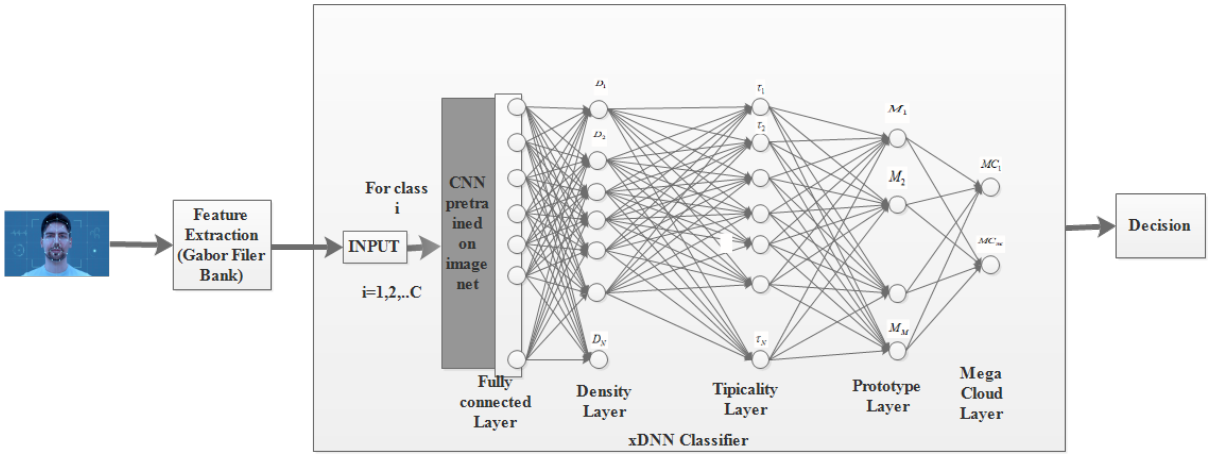


Figure 6.19: The Main architecture of the proposed biometric system

Explainable Deep Neural Networks classifier

The xDNN Classifier proposed is known for its clear semantic and functional implications, along with a specific multi-layer internal structure. Not only does our proposed xDNN Classifier offer high transparency, but it also provides a significant benefit by presenting a meaningful collection of model-based IF...THEN rules to the user. The models play a key role in accurately identifying data samples, as well as in comparing, analyzing, and evaluating the correspondence with other validation images from the user's perspective. By combining statistical learning and reasoning, our proposed xDNN harnesses a powerful capability.

Decision step

after computing the similarity degree, the final determination is made at two hierarchical levels: local and global. Prior to making a decision, the proposed system evaluates the similarity denoted as S in both the models layer and feature layer. The validation process commences by first calculating the degree of similarity for each unlabeled new data in relation to the closest model.

$$S(v_i, p_i) = \frac{1}{1 + \frac{(v_i - p_i)'}{\sigma_i^2}} \tag{6.23}$$

Local Decision

At this stage, the strategy of winner takes all for each class is implemented to determine the using the formula 6.24.

$$\lambda_c = \max_{j=1,2,\ldots,P} (S_j) \tag{6.24}$$

Global Decision

The primary function of the Global decision layer is to identify the most successful class or the winning class and construct the Decision based on the level of resemblance from the prototypes by assigning labels to the validation image. The level of resemblance is produced by the prototype identification Layer, and the global Decision is formulated using the equation 6.25, which computes the maximum of the local, per class victor to establish the overall degree of contentment as follows:

$$\lambda_c^* = \max_{c=1,2,\ldots,C} (\lambda_c) \tag{6.25}$$

Finally, The Label of the validation image is obtained by equation

$$\text{label} = \arg \max_{c=1,2,\ldots,C} (\lambda^* c) \tag{6.26}$$

6.3.3 Experement And Results

To evaluate the precision of the proposed biometric system utilizing the xDNN classifier, a series of experiments were carried out on nine distinct databases. The outcomes, as shown in

table 6.9, demonstrate the superior performance of the suggested system, achieving an accuracy exceeding 93% in seven out of the nine tested databases. Furthermore, three databases exhibited a flawless accuracy rate of 100%, indicating precise classification of all images without any errors. The least accurate results were observed in GTdb crop and Casia, with accuracies of 82.50% and 64.13% respectively. Despite being lower, these accuracy rates are still noteworthy and underline the effective performance of the proposed biometric system based on the xDNN classifier. This can be attributed to unique characteristics present in both Casia and GTdb crop databases, such as data attributes, subject diversity, and dataset size.

Table 6.9: Accuracy of the Proposed biometric System based on xDNN

DATABABE	**ACCURACY**
JAFFE	100.00%
Faces95	93.33%
Facess 94	100.00%
Faces96	98.61%
Grimasse	100.00%
GTdb crop	82.50%
Casia	64.13%
ORL	98%
YALE15	100.00%

Table 6.10: Rank and EER Obtained by applying xDNN Classifier.

DATABABE	**xDNN CLASSIFIER**		**NN CLASSIFIER**		**ALMMo-0 CLASSIFIER**		**SVM CLASSIFIER**	
	Rank(%)	EER(%)	Rank (%)	EER(%)	Rank (%)	EER(%)	Rank (%)	EER(%)
JAFFE	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%
Faces95	93.33%	2.09%	93.19%	1.96%	93.89%	2.09%	92.50%	2.64%
Facess 94	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%
Faces96	98.61%	0.26%	98.41%	0.20%	98.61%	0.23%	97.95%	0.53%
Grimasse	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%	100.00%	0.00%
GTdb crop	82.50%	6.01%	82.50%	5.93%	82.75%	6.01%	80.00%	8.75%
Casia	64.13%	13.09%	62.02%	12.70%	64.73%	33.37%	55.61%	32.28%
ORL	98%	0.50%	98%	0.50%	98%	0.50%	97.5%	1.00%
YALE15	100.00%	0.00%	100.00%	0.00%	98.67%	1.33%	100.00%	0.00%

Table 6.11: Comprative Analysis

[ht!] A Comparative analysis as depicted in 6.11shows that the proposed biometric system, which is based on the xDNN classifier, achieves a very high level of performance and delivers better results in terms of accuracy. This outperforms not only the well-known NN and SVM classifiers but also surpasses the ALMMo-0 classifier, which is recognized as the best explain-

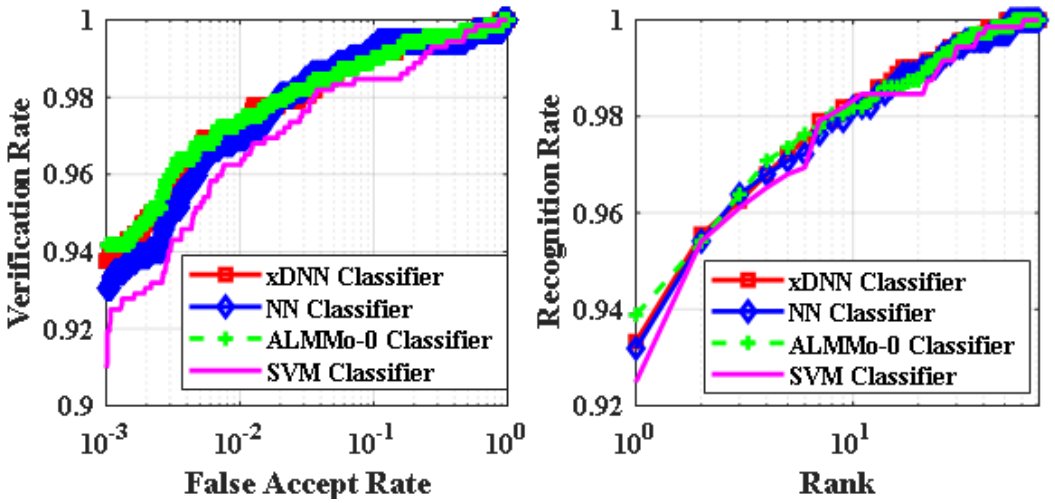


Figure 6.20: ROC and CMC curves for Faces95 database.

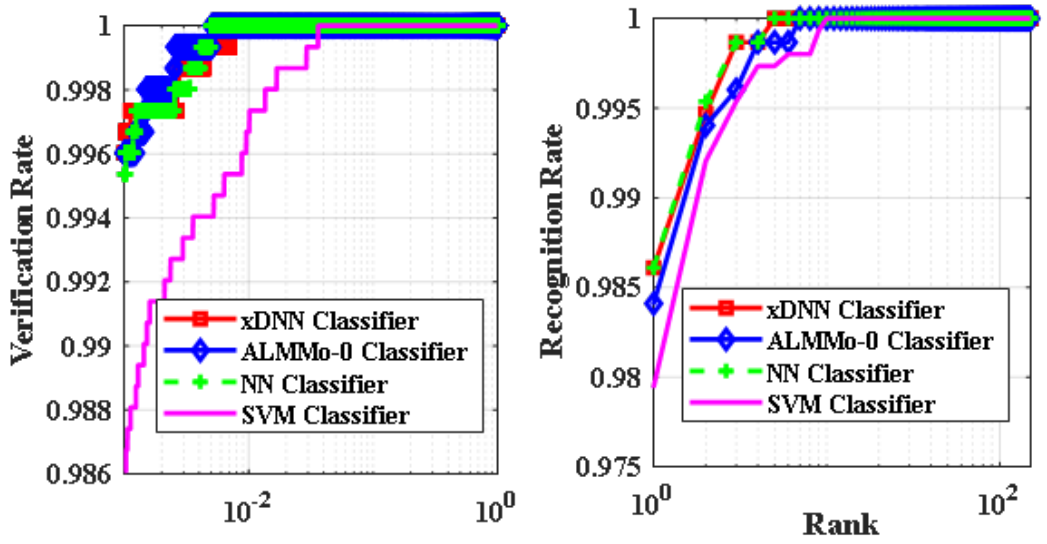


Figure 6.21: ROC and CMC curves for Faces96 database.

able classifier [97]. The ALMMo-0 classifier is known for providing both high accuracy and high expandability simultaneously. Therefore, our proposed biometric system, based on the xDNN classifier, excels over the ALMMo-0 Classifier and all other classifiers in both identification and verification modes. This is demonstrated through the utilization of the ORL and GTDP databases, as clearly depicted in figures 6.23 and 6.22. Upon observing figures 6.20, 6.21, and 6.24, it becomes evident that the proposed system yields superior results compared to the NN and SVM classifiers, while maintaining the same high level of accuracy as the ALMMo-0 Classifier.

Overall, these results indicate and confirm the remarkable success and heightened effec-

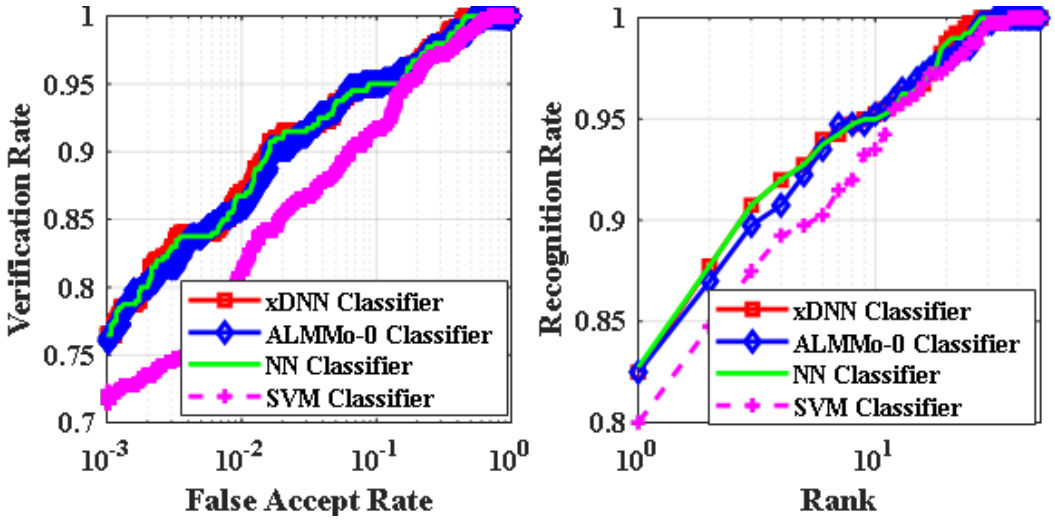


Figure 6.22: ROC and CMC curves for GTDP database.

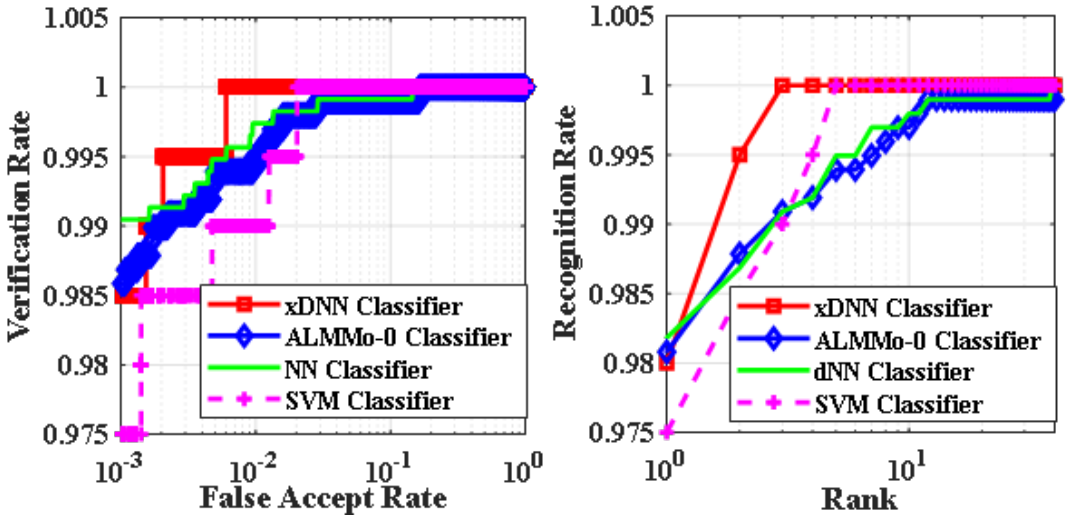


Figure 6.23: ROC and CMC curves for ORL database

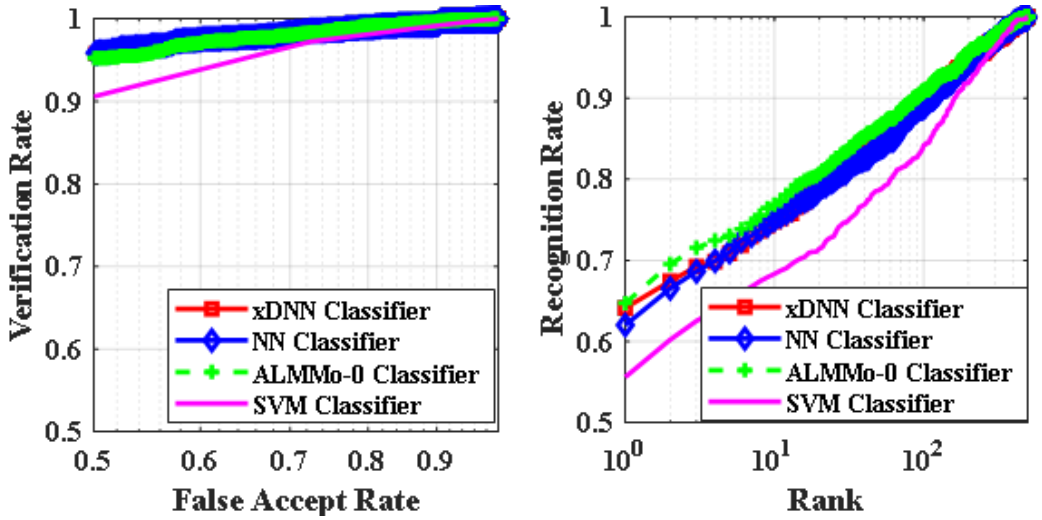


Figure 6.24: ROC and CMC curves for CASSIA database.

tiveness of the proposed xDNN-based biometric system for facial traits. The results obtained so far can be considered the most optimal for classification using an explainable method for facial modality. In terms of time/complexity, the proposed system exhibits lower complexity compared to the NN and SVM classifiers due to its non-iterative nature and simple, data-driven architecture. The structure of the proposed system can be categorized as non-parametric because both the mean and standard deviation of each data cluster are directly derived from the data itself, rather than from algorithmic parameters.

6.3.4 Conclusion

Explainable Classifiers based on biometric systems are utilized to address limitations and achieve high recognition accuracy. The XDNN architecture for Face recognition is introduced in this study among traditional classifiers, as a non-parametric and non-iterative deep learning architecture, which elucidates its efficiency when utilizing a widely used Gabor filter bank for feature extraction. The efficacy of the proposed system has been assessed across nine databases, with experimental results demonstrating the impact of the proposed system, endorsing its suitability for high-security scenarios. Furthermore, experiments indicated that the XDNN architecture for Face recognition, an Explainable-based approach, surpasses conventional methods. Primarily, the Explainable biometric system approach was introduced to surmount limitations of classical-based biometric systems. The results obtained highlight a reduction in the EER to 0.000% in the identification mode and a 100% ROC in the closed-set mode. Future endeavors will focus on enhancing the proposed model by incorporating other modalities such as fingerprint or iris images. Additionally, exploring the integration of swarm intelligence with explainable methods to enhance the functionality of biometric systems is planned.

Chapter 7

General conclusion

7.1 Summary of Contributions

The primary aim of this thesis was to tackle significant challenges in biometric recognition by creating classifier methods that are explainable and utilizing algorithms that are transparent and understandable. The main goal was to develop systems that not only deliver high performance in terms of accuracy and low equal error rates (EER) but also ensure that the decision-making processes are clear to humans. This is vital for improving trust and usability in sensitive areas like medical diagnoses and credit underwriting.

Throughout the study, several key contributions were made. Firstly, explainable algorithms were crafted by creating rule-based classifiers that offer clear justifications for their decisions. This led to improved transparency and interpretability, making it simpler for users to grasp the reasoning behind biometric recognition results. Secondly, achieving high performance in biometric recognition was done by constructing dependable systems that can accurately differentiate between genuine users and impostors, guaranteeing high accuracy and low EER. Thirdly, enhancements in privacy and security were tackled by developing secure authentication methods that safeguard user data and prevent unauthorized access, meeting stringent data protection standards. Fourthly, the thesis concentrated on human acceptability and usability by developing user-friendly algorithms that build confidence in biometric recognition systems and conducting user studies to evaluate and enhance these aspects. Finally, visualization techniques were in-

tegrated to emphasize the explainable features of models, enabling users to better comprehend the decision-making processes of classifiers, thereby boosting trust and acceptance.

7.2 Implications for Biometric Systems

The discoveries and advancements put forth in this thesis carry several significant implications for the biometric systems field. By addressing the transparency and explainability concern, the developed algorithms nurture greater trust among users, which is essential for the widespread adoption of biometric systems in various fields. The high accuracy and low EER attained by the algorithms bolster the security of biometric systems, making them more dependable for crucial applications such as identity verification and access control. The focus on privacy and security aligns with strict regulatory demands, ensuring that the developed systems can be implemented in regions with rigorous data protection regulations. Additionally, the adaptability of the algorithms to different classification and prediction tasks showcases their versatility, opening doors for their utilization across various biometric modalities and scenarios.

7.3 Future Research Directions

Significant progress has been achieved, but there are numerous areas for future research. It is essential to further explore integrating multiple biometric modalities to improve system performance and security. Delving into the synergy between various biometric traits and their combined impact on explainability and accuracy could offer valuable insights. Moreover, the development of more advanced visualization and interpretation methods to enhance the transparency of complex models is a promising avenue. The exploration of advanced machine learning techniques like deep learning alongside explainable AI methods could lead to significant progress. It is crucial to conduct extensive field tests and pilot deployments to assess the practical effectiveness and user acceptance of the proposed systems in real-world scenarios. Collaboration with industry partners to implement and refine algorithms in commercial biometric applications will be vital for widespread adoption.

7.4 Concluding Remarks

To conclude, this thesis has made significant advancements in the field of biometric recognition by addressing the critical need for explainable and transparent classifier methods. The algorithms developed not only deliver high performance but also ensure that users can comprehend and trust the decision-making processes. This research contributes to ongoing endeavors to enhance the security, reliability, and user-friendliness of biometric systems, ultimately facilitating their broader acceptance and deployment in various sensitive and critical applications. The foundation laid in this thesis creates exciting prospects for future research and development, ensuring continuous progress in the domain of biometric recognition.

Bibliography

[1] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face recognition: A literature survey," *ACM computing surveys (CSUR)*, vol. 35, no. 4, pp. 399–458, 2003.

[2] S. Z. Li and A. K. Jain, *Handbook of Face Recognition*. Springer, 2011.

[3] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 4–20, 2004.

[4] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, *et al.*, *Handbook of fingerprint recognition*, vol. 2. Springer, 2009.

[5] P. J. Phillips, H. Moon, S. A. Rizvi, and P. J. Rauss, "The feret evaluation methodology for face-recognition algorithms," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 22, no. 10, pp. 1090–1104, 2000.

[6] A. Samsal and S. Rajagopalan, "Automatic face and gesture recognition," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 22, no. 1, pp. 64–75, 1992.

[7] R. Szeliski, *Computer Vision: Algorithms and Applications*. Springer Science & Business Media, 2010.

[8] R. Gross, S. Baker, I. Matthews, and T. Kanade, "Face recognition," in *Handbook of Face Recognition*, pp. 105–140, Springer, 2005.

[9] U. Park and A. K. Jain, "Face matching and retrieval using soft biometrics," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 406–415, 2010.

[10] S. Z. Li, S. Zhou, and Z. Li, "A probabilistic approach to face recognition using partial least squares," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 37, no. 2, pp. 389–395, 2015.

[11] A. Cavoukian, A. Stoianov, and E. Wiese, "Facial recognition in the modern world: An analysis of risks and rewards," tech. rep., Information and Privacy Commissioner of Ontario, Canada, 2012.

[12] L. Introna and D. Wood, "Picturing algorithmic surveillance: The politics of facial recognition systems," *Surveillance & Society*, vol. 2, no. 2/3, pp. 177–198, 2004.

[13] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, "Deepface: Closing the gap to human-level performance in face verification," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 1701–1708, 2014.

[14] F. Schroff, D. Kalenichenko, and J. Philbin, "Facenet: A unified embedding for face recognition and clustering," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 815–823, 2015.

[15] O. M. Parkhi, A. Vedaldi, and A. Zisserman, "Deep face recognition," in *Proceedings of the British Machine Vision Conference*, pp. 41.1–41.12, 2015.

[16] T. Ahonen, A. Hadid, and M. Pietikäinen, "Face description with local binary patterns: Application to face recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 28, no. 12, pp. 2037–2041, 2006.

[17] A. K. Jain and S. Z. Li, *Handbook of face recognition*, vol. 1. Springer, 2011.

[18] M. Turk and A. Pentland, "Eigenfaces for recognition," *Journal of cognitive neuroscience*, vol. 3, no. 1, pp. 71–86, 1991.

[19] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. fisherfaces: Recognition using class specific linear projection," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 19, no. 7, pp. 711–720, 1997.

[20] D. Zhang, W.-K. Kong, J. You, and M. Wong, "Online palmprint identification," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 25, no. 9, pp. 1041–1050, 2009.

[21] A. Kumar and Y. Zhou, "Human identification using finger knuckle surface," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 112–121, 2011.

[22] Y. Wang, Y. Wang, and D. Zhang, "Finger-knuckle-print recognition using gabor feature and collaborative representation-based classification," *Sensors*, vol. 12, no. 3, pp. 3723–3739, 2012.

[23] L. Zhang and H. Li, "Encoding local image patterns using riesz transforms: With applications to palmprint and finger-knuckle-print recognition," *Image and Vision Computing*, vol. 32, no. 12, pp. 977–986, 2014.

[24] H. Candra and S. Sulaiman, "Recognizing face using the combination of singular value decomposition and hidden markov model algorithms," in *Proceeding of the 3rd International Conference on Electronics, Biomedical Engineering, and Health Informatics: ICEBEHI 2022, 5–6 October, Surabaya, Indonesia*, pp. 575–592, Springer, 2023.

[25] H. Qiu, B. Yu, D. Gong, Z. Li, W. Liu, and D. Tao, "Synface: Face recognition with synthetic data," in *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pp. 10880–10890, 2021.

[26] A. Kortylewski, B. Egger, A. Schneider, T. Gerig, A. Morel-Forster, and T. Vetter, "Analyzing and reducing the damage of dataset bias to face recognition with synthetic data," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, pp. 0–0, 2019.

[27] S. Singh, M. Sharma, and N. S. Rao, "Accurate face recognition using pca and lda," *International Journal of Managment, IT and Engineering*, vol. 2, no. 4, pp. 101–121, 2012.

[28] M. Jabberi, A. Wali, B. Neji, T. Beyrouthy, and A. M. Alimi, "Face shapenets for 3d face recognition," *IEEE Access*, 2023.

[29] A. Farman, "Fundamentals of image acquisition and processing in the digital era," *Orthodontics & craniofacial research*, vol. 6, pp. 17–22, 2003.

[30] A. Nikolaidis and I. Pitas, "Facial feature extraction and pose determination," *Pattern Recognition*, vol. 33, no. 11, pp. 1783–1791, 2000.

[31] J. Ashbourn, *Biometrics: advanced identity verification: the complete guide*. Springer, 2014.

[32] G. Givens, J. R. Beveridge, B. A. Draper, P. Grother, and P. J. Phillips, "How features of the human face affect recognition: a statistical comparison of three face recognition algorithms," in *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2004. CVPR 2004.*, vol. 2, pp. II–II, IEEE, 2004.

[33] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, vol. 1, pp. I–511, 2001.

[34] G. B. Huang and E. Learned-Miller, "Labeled faces in the wild: Updates and new reporting procedures," *Dept. Comput. Sci., Univ. Massachusetts Amherst, Amherst, MA, USA, Tech. Rep*, vol. 14, no. 003, 2014.

[35] B.-C. Chen, C.-S. Chen, and W. H. Hsu, "Face recognition and retrieval using cross-age reference coding with cross-age celebrity dataset," *IEEE Transactions on Multimedia*, vol. 17, no. 6, pp. 804–815, 2015.

[36] V. Jain and E. Learned-Miller, "Fddb: A benchmark for face detection in unconstrained settings," tech. rep., UMass Amherst technical report, 2010.

[37] R. Gross, "Face databases," *Handbook of face recognition*, pp. 301–327, 2005.

[38] S. Yang, P. Luo, C.-C. Loy, and X. Tang, "Wider face: A face detection benchmark," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 5525–5533, 2016.

[39] Y. Guo, L. Zhang, Y. Hu, X. He, and J. Gao, "Ms-celeb-1m: A dataset and benchmark for large-scale face recognition," in *Computer Vision–ECCV 2016: 14th European Conference, Amsterdam, The Netherlands, October 11-14, 2016, Proceedings, Part III 14*, pp. 87–102, Springer, 2016.

[40] R. Gross, I. Matthews, J. Cohn, T. Kanade, and S. Baker, "Multi-pie," *Image and vision computing*, vol. 28, no. 5, pp. 807–813, 2010.

[41] Y. Wang, D. Zhang, and W. Li, "Deep learning for finger-knuckle-print recognition: Convolutional neural network approach," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 12, pp. 3376–3385, 2018.

[42] W. Zhao, H. Li, and J. Zhang, "Hybrid deep learning framework for finger-knuckle-print recognition," *Pattern Recognition Letters*, vol. 135, pp. 120–128, 2020.

[43] F. Liu, X. Chen, and H. Wang, "Adaptive preprocessing and classification for robust finger-knuckle-print recognition," *IEEE Access*, vol. 10, pp. 34456–34467, 2022.

[44] A. B. Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. García, S. Gil-López, D. Molina, R. Benjamins, *et al.*, "Explainable artificial intelligence (xai): Concepts, taxonomies, opportunities and challenges toward responsible ai," *Information fusion*, vol. 58, pp. 82–115, 2020.

[45] R. Dwivedi, D. Dave, H. Naik, S. Singhal, R. Omer, P. Patel, B. Qian, Z. Wen, T. Shah, G. Morgan, *et al.*, "Explainable ai (xai): Core ideas, techniques, and solutions," *ACM Computing Surveys*, vol. 55, no. 9, pp. 1–33, 2023.

[46] L. Rokach and O. Maimon, "Decision trees," *Data mining and knowledge discovery handbook*, pp. 165–192, 2005.

[47] J. Chen, K. de Hoogh, J. Gulliver, B. Hoffmann, O. Hertel, M. Ketzel, M. Bauwelinck, A. Van Donkelaar, U. A. Hvidtfeldt, K. Katsouyanni, *et al.*, "A comparison of linear regression, regularization, and machine learning algorithms to develop europe-wide spa-

tial models of fine particles and nitrogen dioxide," *Environment international*, vol. 130, p. 104934, 2019.

[48] R. Miikkulainen, J. Liang, E. Meyerson, A. Rawal, D. Fink, O. Francon, B. Raju, H. Shahrzad, A. Navruzyan, N. Duffy, *et al.*, "Evolving deep neural networks," in *Artificial intelligence in the age of neural networks and brain computing*, pp. 269–287, Elsevier, 2024.

[49] R. Shwartz-Ziv and N. Tishby, "Opening the black box of deep neural networks via information," *arXiv preprint arXiv:1703.00810*, 2017.

[50] C. So, "Understanding the prediction mechanism of sentiments by xai visualization," in *Proceedings of the 4th international conference on natural language processing and information retrieval*, pp. 75–80, 2020.

[51] C. Agarwal, S. Krishna, E. Saxena, M. Pawelczyk, N. Johnson, I. Puri, M. Zitnik, and H. Lakkaraju, "Openxai: Towards a transparent evaluation of model explanations," *Advances in Neural Information Processing Systems*, vol. 35, pp. 15784–15799, 2022.

[52] W. Samek, T. Wiegand, and K.-R. Müller, "Explainable artificial intelligence: Understanding, visualizing and interpreting deep learning models," *arXiv preprint arXiv:1708.08296*, 2017.

[53] A. Averkin and S. Yarushev, "Explainable artificial intelligence: rules extraction from neural networks," in *International Conference on Theory and Application of Soft Computing, Computing with Words and Perceptions*, pp. 102–109, Springer, 2021.

[54] C.-Y. Hsu and W. Li, "Explainable geoai: can saliency maps help interpret artificial intelligence's learning process? an empirical study on natural feature detection," *International Journal of Geographical Information Science*, vol. 37, no. 5, pp. 963–987, 2023.

[55] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, "An introduction evaluating biometric systems," *Computer*, vol. 33, no. 2, pp. 56–63, 2000.

[56] P. J. Phillips and M. Przybocki, "Four principles of explainable ai as applied to biometrics and facial forensic algorithms," *arXiv preprint arXiv:2002.01014*, 2020.

[57] S. Tiwari, J. Chourasia, and V. S. Chourasia, "A review of advancements in biometric systems," *International Journal of Innovative Research in Advanced Engineering*, vol. 2, no. 1, pp. 187–204, 2015.

[58] G. Carswell and G. De Neve, "Transparency, exclusion and mediation: how digital and biometric technologies are transforming social protection in tamil nadu, india," *Oxford Development Studies*, vol. 50, no. 2, pp. 126–141, 2022.

[59] A. Rawal, J. McCoy, D. B. Rawat, B. M. Sadler, and R. S. Amant, "Recent advances in trustworthy explainable artificial intelligence: Status, challenges, and perspectives," *IEEE Transactions on Artificial Intelligence*, vol. 3, no. 6, pp. 852–866, 2021.

[60] J. R. Williford, B. B. May, and J. Byrne, "Explainable face recognition," in *European conference on computer vision*, pp. 248–263, Springer, 2020.

[61] L. Xie, J. Wang, J. Wang, and Y. Zhang, "Explainable deep learning for efficient and robust pattern recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 41, no. 12, pp. 2797–2811, 2019.

[62] X. Yin, X. Liu, and M. Shao, "Towards interpretable and trustworthy face recognition," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 9138–9147, 2020.

[63] M. Ghodrati, P. Kamencay, M. Benco, and J. Matas, "Deepexplain: Explainable face recognition via spatial attention," *Journal of Visual Communication and Image Representation*, vol. 73, p. 102983, 2020.

[64] M. Wang, W. Deng, and J. Wang, "Explainable face recognition: A survey," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 1, pp. 42–52, 2021.

[65] Z. Zhang, P. Luo, C. C. Loy, and X. Tang, "Interpretable deep learning for face verification," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 349–362, 2021.

[66] A. Jain, A. Kumar, and S. Agrawal, "Explainable ai in face biometrics: A review," *Pattern Recognition Letters*, vol. 152, pp. 16–24, 2022.

[67] S. Singh, S. Singh, and A. Arora, "Enhancing explainability in face recognition systems," in *Proceedings of the International Conference on Computer Vision and Image Processing (CVIP)*, pp. 175–185, 2022.

[68] H. Liu, R. Wang, and X. Tang, "Transparent face recognition with visual explanations," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 2, pp. 555–566, 2023.

[69] Y. Chen, Z. Zhou, and Z. Li, "Xface: An explainable face recognition framework," *Pattern Recognition*, vol. 125, p. 108569, 2023.

[70] X. Qiu, Y. Wang, J. Zhang, and Z. Li, "Explainable deep learning with synthetic data," *Proceedings of the Conference on Artificial Intelligence*, pp. 123–130, 2021.

[71] A. Kortylewski, B. Egger, A. Schneider, T. Gerig, and A. Morel-Forster, "Statistical analysis and explainability," *Journal of Biometric Recognition*, vol. 45, no. 2, pp. 234–248, 2019.

[72] G. J. McLachlan, *Discriminant analysis and statistical pattern recognition*. John Wiley & Sons, 2005.

[73] M. Zulfiqar, F. Syed, M. J. Khan, and K. Khurshid, "Deep face recognition for biometric authentication," in *2019 international conference on electrical, communication, and computer engineering (ICECCE)*, pp. 1–6, IEEE, 2019.

[74] N. E. Chalabi, A. Attia, A. Bouziane, M. Hassaballah, and Z. Akhtar, "Recent trends in face recognition using metaheuristic optimization," in *Handbook of nature-inspired opti-*

mization algorithms: the state of the art: volume II: solving constrained single objective real-parameter optimization problems, pp. 85–112, Springer, 2022.

[75] R. Hammouche, A. Attia, S. Akhrouf, and Z. Akhtar, "Gabor filter bank with deep autoencoder based face recognition system," *Expert Systems with Applications*, vol. 197, p. 116743, 2022.

[76] N. E. Chalabi, A. Attia, A. Bouziane, and Z. Akhtar, "Particle swarm optimization based block feature selection in face recognition system," *Multimedia Tools and Applications*, vol. 80, no. 24, pp. 33257–33273, 2021.

[77] P. P. Angelov, X. Gu, and J. C. Principe, "Autonomous learning multimodel systems from data streams," *IEEE Transactions on Fuzzy Systems*, vol. 26, no. 4, pp. 2213–2224, 2017.

[78] H. Xing, Z. Xiao, R. Qu, Z. Zhu, and B. Zhao, "An efficient federated distillation learning system for multitask time series classification," *IEEE Transactions on Instrumentation and Measurement*, vol. 71, pp. 1–12, 2022.

[79] A. Okabe, B. Boots, K. Sugihara, and S. N. Chiu, "Spatial tessellations: concepts and applications of voronoi diagrams," 2009.

[80] F. Cheng, J. Yu, and H. Xiong, "Facial expression recognition in jaffe dataset based on gaussian process classification," *IEEE Transactions on Neural Networks*, vol. 21, no. 10, pp. 1685–1690, 2010.

[81] L. S. Videla and P. A. Kumar, "Facial expression classification using vanilla convolution neural network," in *2020 7th international conference on smart structures and systems (ICSSS)*, pp. 1–5, IEEE, 2020.

[82] S. Jaiswal and G. C. Nandi, "Robust real-time emotion detection system using cnn architecture," *Neural Computing and Applications*, vol. 32, no. 15, pp. 11253–11262, 2020.

[83] A. Vinay, V. S. Shekhar, N. Manjunath, K. Balasubramanya Murthy, and S. Natarajan, "Expediting automated face recognition using the novel orb 2-ipr framework," in *Proceed-*

ings of International Conference on Cognition and Recognition: ICCR 2016, pp. 223–232, Springer, 2018.

[84] A. A. Mohammed and A. Sajjanhar, "Robust single-label classification of facial attributes," in *2017 IEEE International Conference on Multimedia & Expo Workshops (ICMEW)*, pp. 651–656, IEEE, 2017.

[85] E. Al Alkeem, C. Y. Yeun, J. Yun, P. D. Yoo, M. Chae, A. Rahman, and A. T. Asyhari, "Robust deep identification using ecg and multimodal biometrics for industrial internet of things," *Ad Hoc Networks*, vol. 121, p. 102581, 2021.

[86] M. Biswas, V. Kuppili, D. R. Edla, H. S. Suri, L. Saba, R. T. Marinhoe, J. M. Sanches, and J. S. Suri, "Symtosis: A liver ultrasound tissue characterization and risk stratification in optimized deep learning paradigm," *Computer methods and programs in biomedicine*, vol. 155, pp. 165–177, 2018.

[87] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 24, no. 7, pp. 971–987, 2002.

[88] R. D. Rakshit, S. C. Nath, and D. R. Kisku, "Face identification using some novel local descriptors under the influence of facial complexities," *Expert Systems with Applications*, vol. 92, pp. 82–94, 2018.

[89] Y. Feng, X. An, and X. Liu, "The application of scale invariant feature transform fused with shape model in the human face recognition," in *2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, pp. 1716–1720, IEEE, 2016.

[90] V. Agarwal and S. Bhanot, "Radial basis function neural network-based face recognition using firefly algorithm," *Neural Computing and Applications*, vol. 30, no. 8, pp. 2643–2660, 2018.

[91] K. Chaturvedi and D. K. Vishwakarma, "Face recognition in an unconstrained environment using convnet," in *Proceedings of the 2020 2nd International Conference on Big Data Engineering and Technology*, pp. 67–71, 2020.

[92] M. Hassaballah, H. A. Alshazly, and A. A. Ali, "Ear recognition using local binary patterns: A comparative experimental study," *Expert Systems with Applications*, vol. 118, pp. 182–200, 2019.

[93] R. Chlaoua, A. Meraoumia, K. E. Aiadi, and M. Korichi, "Deep learning for finger-knuckle-print identification system based on pcanet and svm classifier," *Evolving Systems*, vol. 10, no. 2, pp. 261–272, 2019.

[94] A. Attia, M. Chaa, Z. Akhtar, and Y. Chahir, "Finger kunckcle patterns based person recognition via bank of multi-scale binarized statistical texture features," *Evolving Systems*, vol. 11, pp. 625–635, 2020.

[95] P. P. Angelov and X. Gu, *Empirical approach to machine learning*. Springer, 2019.

[96] P. Angelov and E. Soares, "Towards explainable deep neural networks (xdnn)," *Neural Networks*, vol. 130, pp. 185–194, 2020.

[97] E. Soares, P. Angelov, and X. Gu, "Autonomous learning multiple-model zero-order classifier for heart sound classification," *Applied Soft Computing*, vol. 94, p. 106449, 2020.