

**A NOVEL APPROACH FOR DEVELOPING HYBRID
BIOMETRIC MODEL FOR VERIFICATION USING
AURICLE, EAR AND SIDE FACE**

Thesis Submitted for the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

Computer Applications

By

Girish Kumar

Registration No: 41700252

Supervised By

Dr. Ankush Manocha (24829)

School Of Computer Applications (Assistant Professor)

Lovely Professional University, Phagwara



**LOVELY PROFESSIONAL UNIVERSITY, PUNJAB
2025**

DECLARATION

I, hereby declare that the presented work in the thesis entitled “A Novel Approach for Developing A Hybrid Biometric Model for Verification Using Auricle, Ear and Side Face” in fulfilment of my degree of **Doctor of Philosophy (Ph. D.)** is the outcome of my research work carried out by me under the supervision of Dr. Ankush Manocha working as an Assistant Professor School of Applications, of Lovely Professional University, Punjab, India. In keeping with the general practice of reporting scientific observations, due acknowledgments have been made whenever the work described here has been based on the findings of another investigator. This work has not been submitted in part or full to any other University or Institute for the award of any degree.



(Signature of Scholar)

Name of the scholar: Girish Kumar

Registration No.: 41700252

Department/school: School of Computer Applications

Lovely Professional University,

Punjab, India

CERTIFICATE

This is to certify that the work reported in the Ph. D. thesis entitled “A Novel Approach for Developing Hybrid Biometric Model for Verification Using Auricle, Ear and Side Face” submitted in fulfillment of the requirement for the award of degree of **Doctor of Philosophy (Ph.D.)** in the Department of Computer Applications is a research work carried out by Girish Kumar,41700252, is bonafide record of his/her original work carried out under my supervision and that no part of thesis has been submitted for any other degree, diploma or equivalent course.

Dr. Ankush Manocha

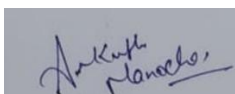
Assistant Professor

Department of Computer Applications

Lovely Professional University

Phagwara, Punjab-144411, India

Signature:



Date:03-May-2025

Abstract

Profile face recognition is the subcategory of facial recognition technology which has not yet gained recognition on the same level as the other types. Unlike frontal face recognition, it relies on photographs taken at the side profile to confirm identities. While side face features are much different from frontal ones, the number of observable parameters is significantly lower. It includes the facial perimeter, the quality of ears, and lateral panels of the nose and chin. These limited features present problems like the ability to analyze lesser amounts of data and thus affect the algorithm's accuracy. Also, angle, lighting, and camera position during capture greatly influence the system's reliability. Since solving these difficulties is critical, and different conditions in the environment and position complicate detection, reliable algorithms are required. Despite suggesting the potential to work successfully for video and streaming, the current approach appears to require more fine-tuning for it to accurately compete with systems that recognize frontal faces.

Developing algorithms capable of accurate side face recognition requires sophisticated machine learning techniques. Traditional facial recognition systems are often trained on large datasets of frontal images, where both the quantity and quality of facial landmarks are much higher. Side face recognition, by comparison, needs datasets specifically curated to include profile images, which are less common and present additional challenges due to the limited visibility of facial landmarks. The method focused on geometric features, such as the outline of the human face, the position and shape of the nose, and the distance between the visible eye and ear. Advancements in deep learning have also played a role in overcoming some of the challenges associated with side-face biometrics. The Convolutional neural networks (CNNs) are trained to recognize patterns in profile images, even with the limited information provided. We propose a novel hybrid model that combines The Principal Component Analyzer (PCA) with CNN to address the challenges of side face biometrics recognition. The increasing demand for accurate and efficient biometric recognition systems has driven the development of models that can handle the complexity and variability of real-world data. Side face biometrics, in particular, present unique challenges due to the asymmetry and occlusion often associated with profile images. By leveraging PCA, a powerful statistical technique, we reduce the dimensionality of the profile images while retaining the most significant features necessary for accurate recognition. With the very first two principal components, we have taken 70% of the necessary features from the side face for further process. However, while PCA excels in simplifying data and reducing computational complexity, it does not inherently capture spatial hierarchies or patterns that are crucial for recognizing facial features in images. This is where the integration of CNNs becomes essential. It is also very important in preparing the image data by reducing it with the

help of the Principal Component Analysis (PCA). Low dimensionality retains considerable features of the original data, excluding the features, that can be deemed redundant and noisy. This reduction helps in reducing the number of inputs that can be dealt with by the Convolutional Neural Networks (CNN). Facial features that form the most important patterns, textures, and edges can be highlighted by PCA and adjusted to CNN's focus when recognizing a face. On dimensionality reduction, the PCA process is followed by CNN, which exhibits the effect of deep learning in revealing discriminative features and numerous relations inside the compressed domain. The integration of PCA and CNN is advantageous in side face profile identification since small differences can be of paramount importance between one person and another. It implies the foundational work that helps PCA to increase the effectiveness and accuracy of CNN in distinguishing between different people and we get 99.99% accuracy with the FEI-Faculdade de Engenharia Industrial dataset of different 200 objects with different 14 poses. Therefore, PCA and CNN enhance the efficiency of biometric systems and help to improve their results in the side-face recognition task.

The hybrid model's architecture is designed to optimize the balance between dimensionality reduction and feature extraction. PCA provides a compressed representation of the side face images, ensuring that the CNN can process the data more efficiently without being overwhelmed by irrelevant details or noise. The CNN, in turn, enhances the model's ability to recognize subtle variations in facial features that are unique to each individual. This combination of techniques enables the model to achieve higher accuracy in side face recognition tasks compared to using PCA or CNNs alone. One of the key advantages of this hybrid approach is its ability to generalize well across different datasets. Side face biometrics can vary significantly due to changes in lighting, pose, and facial expressions. By using PCA to reduce the dimensionality of the data, the model becomes more robust to these variations, as it focuses on the most essential features. The CNN, with its capacity for learning complex spatial relationships, further enhances the model's ability to adapt to variations in the data. In conclusion, our proposed hybrid model that combines PCA with CNNs offers a powerful solution to the challenges of side face biometrics recognition. Combining the ability of PCA in high-dimensional data replacement with convolutional neural networks in feature representation the model possesses high accuracy with low computational power. Not only does this approach solve the problem of identifying profile image records, but it also serves as a basic case for using the generalization method for other biometric databases. The use of these techniques improves the generalization of the model in the prediction of Side facial features, irrespective of variations such as lighting or facial expression making the model ideal for applications in biometric recognition in the real world.

Acknowledgments

First and foremost, I would like to convey my sincere gratitude to my supervisor Dr. Ankush Manocha, for his constant support, helpful leadership, and supervision since the beginning of this research. His expertise and mentorship have been instrumental in shaping the trajectory of this work, and I consider myself truly fortunate to have had the privilege to collaborate with him. His insights have been immensely valuable and have greatly enriched my research journey.

I extend my sincere appreciation to the entire Lovely Professional University community for fostering an environment conducive to research excellence. I am indebted to the Division of Research and Development and the School of Computer Applications for their constant support and encouragement throughout this research work.

I am profoundly grateful to my parents, Mr. Manjit Raj and Mrs. Asha Rani, whose unwavering belief in my capabilities and boundless encouragement have driven my accomplishments. My wife, Mrs. Monika, and my children, Chakshu Bamotra and Romil Bamotra have been a constant source of moral support and understanding during the demanding period of this research. Their patience and care have sustained me through the challenges I faced.

Lastly, I would like to thank the divine for providing me with the strength to overcome obstacles and navigate the trials that presented themselves throughout this research journey. With heartfelt appreciation, I acknowledge the role of faith in guiding me through both the smooth and challenging phases of this work.



Girish Kumar

Date: 03-May-2025

List of Figures

1.1	Various types of biometric modalities.....	2
1.2	Enrolment, Verification, and Recognition procedures.....	7
1.3	A General Biometric System.....	10
1.4	Biometric Design Complexity.....	11
1.5	Processing steps of a biometric system.....	21
2.1	Generic Biometric Identification System.....	31
2.2	12 – face recognition fiduciary site of attention.....	35
2.3	Anatomy of the ear.....	37
2.4	Thermogram image. (Burge and others, 1998).....	38
3.1	Haar Cascade Classifier Workflow.....	50
3.2	Haar Features.....	51
3.3	Image calculation using Haar.....	52
3.4	CNN Architecture.....	54
3.5	MTCNN model.....	56
3.6	The operators of LBP.....	57
3.7	Architect of HOG.....	58
3.8	PCA-Flow chart.....	61
3.9	MLP Model.....	64
4.1	Sample images from the Data set FEI.....	68
4.2	Pre-processing the image.....	69
4.3	PCA of Side face images with two Principal components.....	74
4.4	Average side face images with ten Eigenfaces.....	75
4.5	Explained Variance Ratio vs Number of Components.....	76
4.6	Cumulative Explained Variance Ratio vs Number of Components.....	77
4.7	HOG and LBP feature Fusion.....	79
4.8	The Working Hybrid-Model PCA+CNN.....	81
4.9	Model Loss and Model Accuracy.....	84
4.10	Calibration Curve.....	85
4.11	Input Sample and Predicted image.....	87
4.12	3D Surface Plot.....	88
4.13	Histogram Plot.....	88
4.14	3D Gradient (x-axis).....	88
4.15	Plot, Histogram Plot and 3D Gradient (x-axis) -1.....	89
4.16	3D Plot, Histogram Plot and 3D Gradient (x-axis)-2.....	90

List of Tables

1.1	Error Rates of Different Biometrics.....	12
1.2	Scaling Performance of Different Biometrics.....	14
1.3	Assessment of biometric traits	20
2.1	Feature extraction for ear using local descriptors with different approaches.....	39
4.1	Data for training and testing purposes	79
4.2	Model Summary	83
4.3	Comparison with Baseline Model.....	93

List of Abbreviations

Abbreviation	Description
2D	Two Dimensional
3D	Three Dimensional
3DMM	3D Morphable Models
AAM	Active Appearance Models
ABS	Automated Biometric Systems
AFIS	Automated Fingerprint Identification System
AI	Artificial Intelligent
ATMs	Automated Teller Machines
CCA	Canonical Correlation Analysis
CNNs	Convolutional neural networks
CPU	Central Processing Unit
DNA	Deoxyribonucleic Acid
FAR	False Acceptance Ratio
FCL	Fully Connected Layer
FEI	Faculdade de Engenharia Industrial
FMR	False Match Ratio
FRR	False Rejection Ratio
FSLDA	Full-space Linear Discriminant Analysis
GAN	Generative Adversarial Networks
GEM	Generic Elastic Models
GPU	Graphics Processing Unit
HMM	Hidden Markov Models
HOG	Histogram of Oriented Gradient
ICA	Independent Component Analysis

IoT	Internet Of Things
KFDA	Kernel Fisher Discriminant Analysis
LBP	Local Binary Patterns
LDA	Linear Discriminant Analysis
ML	Machine Learning
MLP	Multi-Layer Perceptron
MTCNN	Multi-Task Cascaded Convolutional Neural Networks
NNs	Nearest Neighbors
O-Net	Output Network
PCA	Principal Component Analyzer
PLS	Partial Least Square
P-Net	Proposal Network
RBF	Radial Basis Function
ReLU	Rectified Linear Unit
ResNet	Residual Network
R-Net	Refine Network
ROC	Receiver Operating Characteristic
SVM	Support Vector Machines
TPU	Tensor Processing Unit
VGGNet	Visual Geometry Group Network

Table of Contents

Declaration.....	i
Certificate.....	ii
Abstract.....	iii
Acknowledgments.....	v
List of Figures.....	vi
List of Tables.....	vii
List of Abbreviations.....	viii
 Chapter 1.....	 1
1. Introduction.....	1
1.1 Biometrics traits and attributes.....	4
1.2 Biometric Systems.....	5
1.3 Multi-Biometric Systems.....	7
1.4 Biometric Scenario.....	10
1.5 Biometrics Design Complexity.....	11
1.5.1 Accuracy.....	11
1.5.2 Scale.....	13
1.5.3 Security.....	14
1.5.4 Privacy.....	15
1.6 Biometrics Comparison.....	16
1.7 Biometric Data Processing Steps.....	21
1.7.1 Biometric Operations.....	22
1.8 Biometric Applications.....	22
1.9 Motivation of the Thesis.....	24
1.10 Objectives.....	25
1.11 Problem Statement.....	26
1.12 Thesis Organization.....	26
1.13 Summary.....	28
Chapter 2.....	30
2. Literature Review.....	30
2.1 Side Face Literature Review.....	33
2.2 Ear as a Biometrics.....	37
2.3 Outcome Closure.....	43
2.3.1 Accuracy.....	43
2.3.2 Security.....	44
2.3.3 Usability.....	44
2.3.4 Technological Advancements.....	44
2.4 Identified Research Gaps.....	45
2.5 Conclusion.....	46
Chapter 3.....	48
3. Inspiration and Driving Forces Behind the Study.....	48
3.1 Detecting Face.....	48
3.1.1 HCA- The Haar-Cascade.....	49
3.2 Deep Learning Techniques for Side Face Recognition.....	52

3.2.1 Convolutional Neural Networks-CNNs.....	53
3.2.2 Transfer Learning.....	55
3.2.3 MTCNN: Multi-Task Cascaded Convolutional Neural Networks.....	55
3.3 Feature Extraction Methods.....	56
3.3.1 LBP - The Local Binary Pattern.....	57
3.3.2 HOG- Histogram of Oriented Gradient.....	58
3.3.3 PCA- Principal Component Analysis.....	59
3.4 Face Recognition Techniques.....	61
3.5 MLP- Multi-Layer Perceptron.....	64
3.6 Conclusion.....	66
Chapter 4.....	67
4. Proposed System.....	67
4.1 Dataset Used.....	67
4.2 Dataset Preparation.....	68
4.2.1 The Algorithm for Side-Face Image Pre-processing.....	70
4.2.2 Implementation of PCA.....	71
4.2.3 Optimum Number of Principal Components.....	75
4.2.4 Feature Fusion Based on HOG and LBP.....	78
4.2.5 Breaking the Data.....	79
4.2.6 Feed Reduced-Dimension Data into CNN.....	79
4.3 Experimental Results.....	83
4.4 Calibration Curve.....	85
4.5 Implementation and Results Obtained.....	85
4.6. Comparative Analysis.....	93
4.7. Conclusion.....	94
Chapter 5.....	95
5. Conclusion and Future Work.....	95
5.1 Conclusion.....	95
5.2 Impact on the Field.....	97
5.3 Future Work.....	97
List of Publications.....	99
List of Patents.....	100
List of Copyrights.....	101
References.....	106

Chapter 1

1. Introduction

“Biometric is the automated recognition of individuals based on their behavioral and biological characteristics.”

In Greek, "Bio" means "life", and "metrics" means "measure", which is where the name "biometrics" originates. It is the study of quantifying the physical characteristics and attributes of living things. The evolution of Automated Biometric Systems (ABS) in recent decades has been facilitated by extraordinary advances in computer processing technology, particularly in image processing. Remarkably, many modern automated procedures are based on historical principles used for identifying individuals for hundreds or thousands of years. Characteristics connected with the human body, such as the face, voice, and movement, are among the earliest and simplest examples of identifying individuals based on distinguishing qualities. Humans have historically used these characteristics for identification [108]. While the use of automated biometric systems is a relatively new development, the fundamental ideas behind them date back to ancient times. Biometrics involves using computers to recognize human physical and behavioral characteristics, capturing traits for one-to-one authentication and one-to-many comparisons. Biometric measurements are categorized into two main types:

1. *Physiological traits.*
2. *Behavioral traits.*

Physiological features can make an individual's body different from another's, so behavioral traits simply mean a way to distinguish above-average and below-average humans. As an example, Figure 1.1 illustrates two different types of biometrics. Physical characteristics refer to things such as the face, ear shape, fingerprints, and DNA. These qualities of our bodies are classically defined as “somatic” and tend to remain rather fixed over the life course. On the other hand, behavioral traits are rooted in an individual's varied behaviour patterns. Behavioral characteristics (such as walking, or the way a person speaks), and Signature styles. Those traits can change for any number of reasons over time, but they stay distinct.

Figure 1.1 illustrates the many biometric types, emphasizing the diversity of traits and patterns that can be used for identification and authentication.

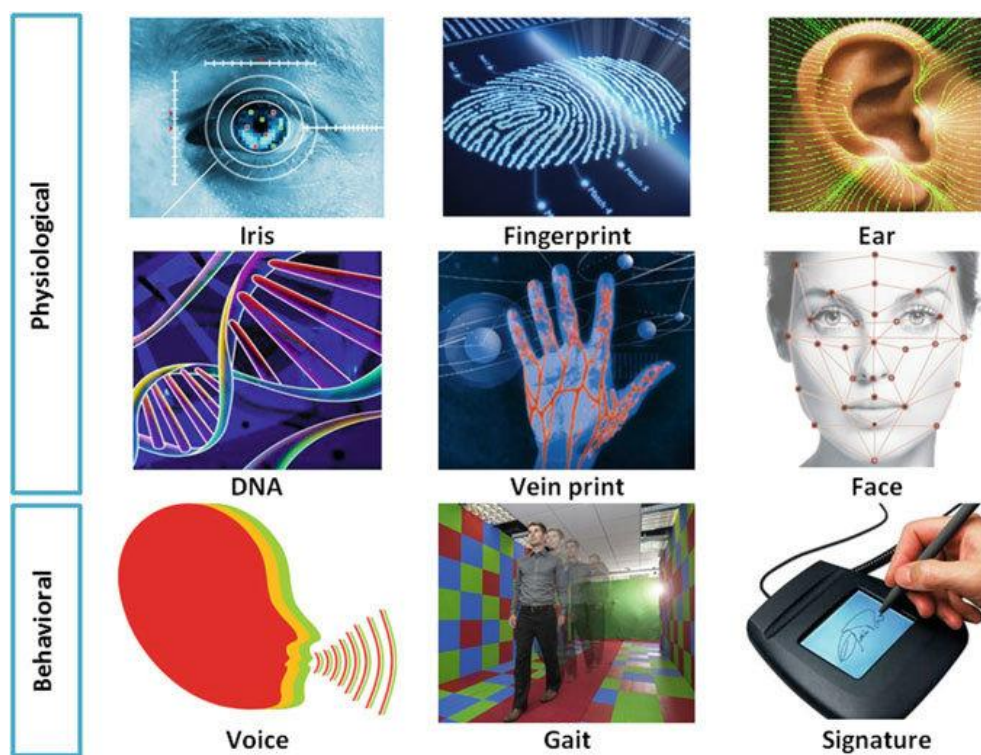


Figure 1.1 Various types of biometric modalities [108]

In theory, any physiological or behavioral trait can serve as the foundation for a biometric system, provided it meets the following criteria [108]:

1. **Universality:** This is a quality every human should have. The implication is that the selected biometric trait should be frequent among nearly all of the sample population, and atypical occurrences, if any exist, are few and minor.
2. **Uniqueness:** The traits must vary for each person. Biometric assets upon which identification and differentiation are based do not have to be common amongst two or more bodies.
3. **Permanence:** To achieve this, the biometric trait must remain constant over time and change only slowly because of aging or other factors to enable correct system operation.
4. **Collectability:** Anything using biometric data should be easily measurable -- it's very intrusive. The manner of collection shall not cause discomfort or interfere with performing the biometric authentication process on an individual.

5. **Performance:** Regardless of whether or not the system can place a person, it should recognize only persons and people through numerous scans of that very same biometric characteristic. This includes precision, accuracy, and the ability to deal with variation in a trait.
6. **Resistance to circumvention:** The biometric trait that is chosen should be hard to replicate or cheat. A better system is one that, even when facing artificial attempts to emulate the biometric data (e.g., via photos or voice recordings), does not easily fall for being spoofed.
7. **Acceptability:** Everyone should feel comfortable and willing to provide their biometrics for Identification. However, ethical considerations and the issue of privacy are major factors as well that need to be addressed if future biometric technologies truly want widespread acceptance.
8. **Circumstances of use:** The biometric trait must be applicable across different scenarios and should add versatility regarding environmental conditions, light, noise, etc. This makes the biometric system practical and flexible.

Biometric systems evolve in tandem with technological advancements, incorporating requirements for use, and improving accuracy, security, and user experience, among other things. These concepts can also be used as guidelines for managing and putting biometric technologies to use in many areas, such as surveillance, access control, and identification services. However, it is critical to recognize that virtually no systems provide perfect security for biometric applications. None of the biometric methods discussed can fully meet all the aforementioned criteria. Each biometric method offers its strengths and limitations, with the choice of implementation depending on the desired security level and the specific convenience needs of the application.

1.1 Biometrics traits and attributes

Among the various characteristics in humans that can be categorized as biometrics are fingerprints, facial features, and signatures. In addition, features like facial structure, retina patterns, hand and finger geometry, and hand vein patterns are also considered. Other methods include voice recognition, DNA, scent, and typing patterns [11]. These diverse attributes provide a range of options for biometric identification, with each offering distinct advantages that make them suitable for different applications.

Table 1.1 gives a comprehensive comparison of the attributes of various biometric traits. The typical stages or phases that constitute a biometric system are as follows:

1. **Enrolment:** During the enrolment phase, the system captures the unique biometric traits of each individual. This step is essential for accurate future identification. Various sensors are

utilized to facilitate this data collection process. These sensors may consist of microphones for capturing voice patterns, cameras for recording facial features, and fingerprint scanners for obtaining unique fingerprints. Each type of sensor plays a crucial role in gathering specific biometric information. The combination of these sensors provides a comprehensive profile of the individual. Ensuring precise data collection during enrolment is vital for effective biometric authentication. This approach significantly enhances both security and accuracy in identification. Ultimately, utilizing diverse sensors during enrollment strengthens the overall biometric system. This technology is pivotal for reliable identity verification across various applications.

2. **Detection and Segmentation:** The detection and Segmentation step is crucial in multimodal data, such as images, in which the system has to locate and then extract/segment, or isolate where this specific kind of n-trait lies properly for processing.
3. **Feature Extraction:** A template or feature vector is created in this stage, which truly represents the biometric trait by extracting some unique characteristic from it. Carried out on features, which are the basis for successive comparisons and matchings.
4. **Matching:** In the matching phase, it compares two feature vectors (usually an enrolled v/s presented biometric traits). This inherently allows for a similarity score or distance metric to be computed that provides the quantified level of likeness between both traits. The output of the process is used to determine whether or not the presented trait matches the enrolled one.

1.2 Biometric Systems

Biometrics involves the automated identification and verification of individuals through measurable physical or behavioral traits. This technology is built on unique characteristics that differentiate one person from another. However, it faces several challenges that can affect its effectiveness. These challenges can be clustered into four main classes:

- (a) In the area of Accuracy
- (b) In the area of Scalability
- (c) In the field of Security
- (d) In the field of Privacy.

Biometrics is an exciting challenge in recognising patterns, and when used well, it can be a powerful technology to improve security, prevent fraud, and make interactions between people and machines easier. Its potential comes from three main features:

- a) **Identification:** *deals with the procedure of establishing the ownership of an individual of the system in question. Biometrics is instrumental in this confirmation as it can give a fairly accurate assurance concerning the identity of a requested enrolment through the involvement biometric sample.*

Now, imagine a situation where somebody is using your name, for example, Girish Kumar, in the system and presenting his fingerprint. It takes the presented fingerprint to the enrolled one and validates/ rejects that claim. In the present world, identity is extensively used in business areas such as computer network identification, data protection, Automated Teller Machines (ATMS), credit card transactions through phone or Internet, and banking through mobile banking.

It enables biometric technology to maintain the integrity and security of interactions within these contexts, thereby protecting sensitive data & resources. Principles of Cost and Usability for an ID Attestation Application: Provide Fashion. Because these are broadly used, there is an economic motivation for them to balance effective security with a positive user experience. The importance of biometric technology in these efforts, with its inherent capabilities to provide effective identification regardless of the inconvenient and circumstantially challenging real-world environments, is manifest.

- b) **Large-scale identification** *involves the process of determining whether an individual's biometric sample matches any of the entries within a substantial database. In this scenario, the goal is to verify if the pattern corresponds to any of the enrolled identities within the database, which could potentially include millions of records.*

The number of applications that require large-scale identification is vast and includes such diverse arrays as the ATM card in your wallet to bio-nanotechnology. From ID cards like Aadhar Cards or national cards, border control& parentage determination to voter ID cards that can also be used in finding missing children and issuing driving licenses the same as well would help with issuing a death certificate; helping out criminal investigations purposefully by providing a variety of biographical details on demand at welfare dispensation services. One application is concerned with the domain, e.g., security, public safety, and another one is for human-facing administrative processes. At the heart of such large-scale ID applications is a requirement for high levels of throughput and velocity. The volume of data monitored in DISPATCHED systems is significantly greater, with minimal human interaction. National ID systems are designed for the comprehensive administration of citizens' identities and must be able to accommodate all such IDs.

Things like the effectiveness of security measures and how smoothly your administrative tasks run are determined largely by how efficiently these large-scale identification applications can be. At the heart of these applications lay biometric technologies, capable of matching quickly and accurately

biometric patterns against large databases, thus allowing for rapid identification, with low levels of human intervention.

- c) **Screening** applications involve discreetly determining whether an individual is included in a designated watch list of identities. These applications serve to identify individuals of interest without drawing attention to the process.

The primary goal of screening is to swiftly identify individuals who may pose a potential threat or are of interest to security personnel. Several key characteristics define screening applications:

- **Minimal Enrolment Phase:** Unlike other biometric applications, screening applications don't typically involve a conventional user enrolment phase. Instead, they aim to identify individuals without requiring them to be pre-registered in the system.
- **Challenging Imaging Conditions:** Screening scenarios offer only limited control over subjects and imaging conditions. Individuals in such scenarios may be unaware of the biometric data collection process, and the conditions may not be optimal for image capture.
- **High Throughput with Limited Human Supervision:** Screening applications require the ability to process a high number of subjects quickly and with minimal human intervention. Efficiency is crucial, as lengthy interactions could disrupt the flow of people.

Both large-scale identification and screening applications rely heavily on biometric technology due to their unique requirements. The token-based or knowledge-based identification methods do not apply to such situations. The biometric approach acts as a reliable medium of ensuring the acknowledgement of individuals from the watch list within the safety and security of various scenarios. It allows discreet and quick assessment procedures that enhance the functioning of security measures with high operational efficiency. So, a biometric can be used either as an identification tool or for verification. For this specific tactic, there is a method to identify an individual based on his or her feature vector in less than 2 seconds of inference time with almost full model accuracy. Conversely, the verification process takes two inputs — one for a feature vector and another associated identity as an output. It then checks if the biometric trait that they provided corresponds with their desired identity or not. Figure 1.2 details the enrolment phase, conferring the verification and recognition. This phase includes vital steps during which the biometric characteristics of an individual are collectively enrolled in the system. It is the basis of subsequent detection or confirmation steps. The verification process verifies the veracity of a claimed identity by checking for consistency between submitted biometric data and an asserted identity. Enrolment uses that biometric trait to create a dataset, while recognition does the opposite—it tries to match against an already created database given the presented datasets. These processes together form an operational

framework of a Biometric system, which maintains the checks it is supposed to fulfil as a secure and efficient identification means. Which is the best way to identify recognition or verify, and that largely depends on what your application's requirements according them; each has different use cases.

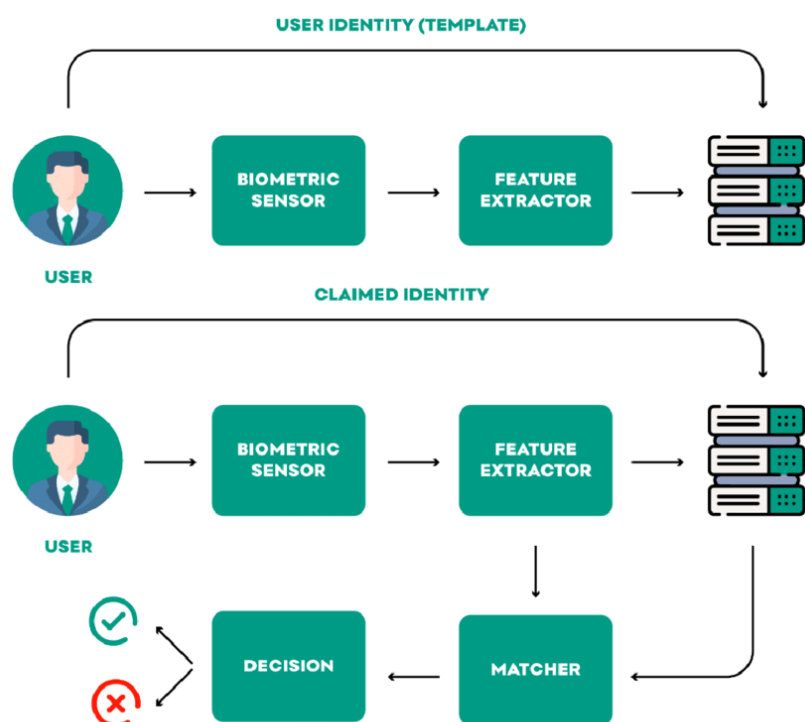


Figure 1.2 Enrolment, Verification, and Recognition procedures [109]

1.3 Multi-Biometric Systems

The base idea of biometric schemes can generally be categorised into two main types: *unimodal* and *multimodal*. Multimodal biometrics involves the integration of 2 or additional distinct biometric modalities within a single identification framework. On the other hand, unimodal biometric systems come with a range of associated challenges, including issues such as data corruption due to noise, variations within the same class, limited flexibility, lack of universality, susceptibility to spoof attacks, and strict requirements for error rates.

The concurrent utilisation of multiple biometric traits offers an added layer of safety to recognition systems. Such classifications are referred to as Multi-Biometric Platforms, also known as multimodal systems. Their growing popularity stems from their ability to address several limitations that can impact single biometric traits on their own. Some of these limitations are outlined below:

- **Iris Recognition Limitations:** The iris, while a strong biometric trait, can be affected by factors like unacceptable distance between the camera and the subject during acquisition. Additionally, partial coverage by eyelashes and eyelids can hinder accurate recognition.

- **Face Recognition Vulnerabilities:** Facial recognition can be vulnerable to spoofing attempts using masks or makeup. Moreover, facial features can change over time, reducing stability. Accessories like scarves, hats, and glasses can also obscure some portions of the face.
- **DNA Feature Extraction Challenges:** The process of extracting DNA features is time-consuming, making it impractical for real-time identification scenarios.
- **Soft Biometrics Sensitivities:** Soft biometric traits like gait and keystrokes can be influenced by the emotional state of the individual. In such cases, obtaining a consistent signature of the biometric trait may not always be feasible.

In practical applications, a biometric system needs to fulfil several criteria. It must achieve the specified level of recognition accuracy while maintaining speed and resource efficiency. Moreover, it should not pose any harm to users, gain acceptance from the target user population, and exhibit robustness against various fraudulent techniques and attacks directed at the system.

Considering these requirements, the present thesis delves into the exploration and utilisation of multimodal biometric schemes. By combining multiple biometric modalities, this approach aims to address the limitations and challenges associated with unimodal systems. Integrating different biometric traits can enhance accuracy, reliability, and security in identification processes. By so doing, the thesis seeks to advance knowledge in creating improved and reliable biometric systems that will be useful in real-life situations. The thesis focuses on identifying an appropriate fusion level of Multimodal biometrics, to analyse the integration techniques and implement the concept of ML-Machine Learning. These initiatives are meant to enhance the biometric system's performance by a very large percentage.

The study done in the research work reveals several algorithms that seem to have tremendous potential in correcting faults with either the FAR or the FRR. As such, given these algorithms' integration, one can lay down the foundations for the subsequent advancements of multimodal biometric systems and their implementation into different uses. It could be possible to achieve greater accuracy and reliability of the implemented methods in multimodal schemes than in one-mode schemes.

In a standard biometric system, as illustrated in Figure 1.3, there are four primary components: the first one is the sensor second one is the feature extractor third one is the matcher, and the last one is the decision module. Each component serves a specific role within the system's operation.

1. **Sensor:** The first component is used to collect biometric information about any specific person. It collects raw biometric data, including fingerprints, face features, voice samples, and

other pertinent characteristics. In some circumstances, a quality estimation algorithm determines if the acquired data is suitable for processing.

2. **Feature Extractor:** The feature extractor then processes the acquired biometric data to get relevant and distinctive features. It eliminates the fundamental characteristics defining the biometric trait and creates a new representation known as the “Feature Set.” Every user should have a dissimilar feature set that almost has no resemblance to other users, which must resist variation in samples from a similar user.
3. **Matcher:** Hence, the work of the matcher is to establish a match between the feature set that has been extracted from the biometric sample (called the query) and that which was formed at the time when the enrolment process was going on and stored in the database. This is so because it quantifies the extent of similarity or dissimilarity between the two sets of features and therefore offers a measure of match.
4. **Decision Module:** The decision module checks the biometric sample against the stored template to confirm or deny the identity claim, based on how similar they are. If the similarity meets a certain threshold, the system approves the authentication.

When combined, these three elements form a comprehensive biometric solution capable of verifying identities based on distinct, unique characteristics [110]. The system meticulously examines each input, comparing it against stored data to ensure accurate identification. By analysing the biometric sample—whether it's a facial scan, fingerprint, or voice pattern—the system applies advanced algorithms to determine whether the input matches the enrolled data.

The process ensures that only authorized individuals gain access, offering high levels of security and trust. Each input undergoes a rigorous comparison, enabling the system to detect even slight variations and prevent unauthorized access. With its ability to analyse multiple factors and make intelligent decisions, this biometric solution provides a robust, reliable method of verifying identity in critical applications like secure facilities, digital services, and more. The system's precision and adaptability make it a trusted tool for safeguarding access while maintaining convenience for authorized users.

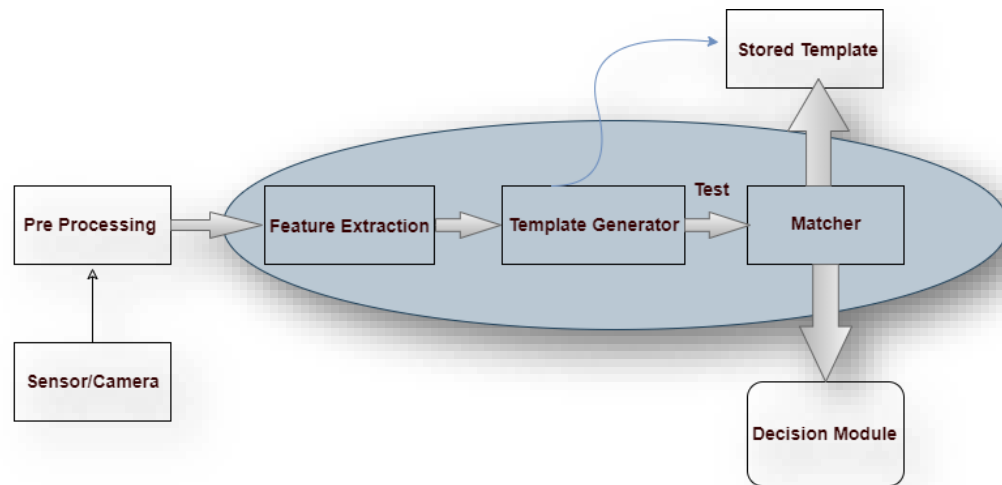


Figure 1.3 A General Biometric System [110]

1.4 Biometric Scenario

During the verification process, an individual identifies, and the biometric system confirms or denies their identity by comparing a new sample to an existing one. The acceptance or denial of the identity claim is determined by this comparison. Consequently, there are four potential outcomes to this undertaking:

1. **True Accept:** The system correctly confirms an identity claim, matching the presented biometric sample with the stored one.
2. **False Accept:** The system mistakenly validates a false identity claim, incorrectly matching the biometric samples.
3. **True Reject:** The system accurately rejects a false identity claim, recognizing that the biometric samples do not match.
4. **False Reject:** The system wrongly denies a valid identity claim, failing to match the biometric samples due to variations or other factors.

Errors can occur in the verification process, and two main types of errors can be made:

1. **False Accept:** When the working model allows an untrue uniqueness claim in the argument, then a false acceptance error is generated. That type of error could prove to be security-threatening, as an intruder could be allowed to access it.
2. **False Reject:** When a person whose claim of identity is genuine is rejected by the system, then there is a case of false rejection error. Such errors might result in inconvenience and denial of access to the right users, as recommended by scholars.

A lower EER suggests a more accurate biometric system.

1.5 Biometrics Design Complexity

The complication of designing a biometric system is influenced by 3 primary factors: The first one is accuracy, the second one is scale (database size), and the last one is usability, as depicted in Figure 1.4. Typically, a biometric system excels significantly in one of these factors while pushing the limits of that axis. Although successful systems have been developed based on this principle, the current major challenge is to devise a biometric system that balances all three factors effectively. Achieving this balance would overcome the inherent limitations of biometric systems and lead to more successful solutions. Presently, the difficulty is to create a biometric system that excels in accuracy, can handle large-scale databases, and is user-friendly. Such a system would break through the fundamental barriers that biometric systems often encounter and would offer solutions that are more secure, robust, and cost-efficient [110]. By addressing these core research issues, significant advancements can be made in the field, pushing the boundaries of what is currently achievable. This progress would result in biometric systems gaining greater acceptance, raising awareness about their capabilities, and potentially yielding profitable outcomes.

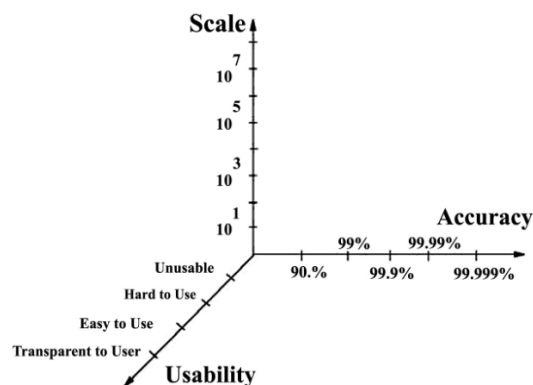


Figure 1.4 Biometric Design Complexity [110]

1.5.1 Accuracy

The ideal biometric system should incorporate the ability to make accurate decisions whenever a biometric sample is presented to it, unlike a password or token. Nonetheless, biometric systems that are in use are not as accurate and can therefore produce two main categories of error.

- a) **False Match:** False Match is carried out when the biometric trained/untrained undergoes training and the input pattern is matched to a different pattern from the record that is held or it wrongly links the input pattern with a different person during the verification process.

- b) False Non-match:** It occurs when a biometric trained/untrained model in verification or identification does not correctly match the input pattern with any correct pattern record, or when the biometric trained/untrained model in verification fails to recognize the input pattern as the correct identity.

If one wants to get a deeper insight into the biometric system, it is recommended that one measure a biometric system's performance using a "Receiver-Operating-Characteristic – ROC "curve. Such a curve enables a full view of system accuracy as shown by the graph displaying the relative frequency–verification rate (true accept rate) against the FAR, or FRR against FAR.

Table 1.1: Error Rates of Different Biometrics [1]

Biometric	FNMR%	FTE%	FMR1%	FMR3%	FMR2%
Front Face	4	Not Applicable	10	12	40
Hand Geometry	1.5	2	1.5	Not Applicable	Not Applicable
Finger	2.5	4	<0.01	<1	.01
Voice-Pitch	15	1	3	Not Applicable	Not Applicable
Iris-Retina	6	7	<0.001	Not Applicable	Not Applicable

The accuracy performance of biometrics, as shown in Table 1.1, has been evaluated through extensive third-party testing. In the table, the following notations are used:

- i. **FMR1:** FMR1 represents the verification match error rate which indicates the rate at which false matches happen during the verification process.
- ii. **FMR2 and FMR3:** These denote the (projected) match error rates for large-scale identification and screening scenarios. FMR2 corresponds to a database size of 1 million identities, while FMR3 corresponds to a database size of 500 identities.
- iii. **N/A:** This notation signifies that the data for a particular entry is not available or not applicable.

In summary, these metrics reveal how accurate the biometric systems are in a variety of cases and with different database sizes.

Face recognition results based on FRVT 2002 [1] et Eyematic data extrapolation. Jain et al. myself, fingerprint autogenetic and errors [2], straight alpha-numeric text 1.5 to 8 characters, AutoCode code only, right index finger, including invalid Vanner type: Fingerprint screening and identity source, two-finger state-of-the-art AFIS performance for 6-million individual comparison [3]. False match rates for hand geometry, voice, iris, and fingerprint are from various sources: severe arthritis incidence for hand geometry [4], speech disability statistics from the 1997 US census for voice, Sanchez-Avila et al. [5] for iris, and Jain [6] for fingerprint.

The technologies also vary in their automation potential and sensing-at-a-distance capabilities. According to Jain et al. [7], there are a total of three main reasons for the bad accuracy of biometric systems, highlighting the challenges in achieving flawless biometric accuracy.

1. **Information Limitation:** The amount of unique and consistent information in biometric pattern samples is inherently constrained by the signal's capacity. The specific characteristics that define an individual's identity may have certain limitations. These constraints can restrict the information content available in biometric identifiers. As a result, this limited data can impede accurate and reliable identification. Ultimately, the effectiveness of biometric systems can be affected by these inherent restrictions. Addressing these limitations is essential for improving identification precision.
2. **Representation Limitation:** In an ideal situation, a biometric system should collect all the unique and important information from the measurements it takes. But in reality, the systems often use simplified versions of this information. These simplified versions might miss some important details, which can lead to mistakes in identifying people. So, while biometric systems are helpful, they might not always get it exactly right because they're not capturing all the necessary details.
3. **Invariance Limitation:** Once a representation scheme is in place, creating an ideal matcher requires accurately modelling the relationship of invariance among patterns from the identical class, even under variable conditions. This task is complex due to variations in environmental conditions, imaging equipment, and physiological factors affecting captured biometric data. Building a matcher that can robustly handle these variations while producing accurate matches poses a significant technical challenge.

1.5.2 Scale

In verification systems, the database size doesn't matter much as it involves a 1:1 match between submitted samples and enrolment records. However, in large-scale identification systems with numerous identities, performing sequential 1:1 matches is inefficient, requiring

scalable solutions to maintain throughput and control false-match error rates as the database size increases.

Table 1.2 Scaling Performance of Different Biometrics [1]

Biometric Traits	Confirmation	ID Throughput	Transmission Throughput
Finger	10.00 m seconds	1 per minute	More than 1 second
Front Face	90.00 μ seconds	0.656 per minute	22.00 per second
Iris Retina	Less than 1 μ seconds	Greater than 1 per second	Greater than 2000.00 seconds

The reported performance metrics for biometric systems are subject to certain considerations:

- **Fingerprint Screening and Identification:** The evaluation assumes fingerprint screenings are part of the 2-finger fingerprint screening, and the performance utilizing 10 fingers for all other test modalities represents SOTA, which is the state-of-the-art Automated Fingerprint Identification System (AFIS) performance in fingerprint identification.
- **Face and Iris Matching Speeds:** 1:1 Match speed for face taken from Chang [4] and Ross [9], and for iris taken from Ross et al. [8]. Note that the values provided here are rough order-of-magnitude estimates without time for biometric presentation or feature extraction. These are general benchmarks for trending with what state-of-the-art system performance is obtainable.

It mentions that these values are not directly comparable because they might differ in automation, as well as the CPU power and sensing capabilities. Systems for millions of identities and nearly real-time applications can be scaled, but throwing 100 million identities at a near-real-time system is still hard to tackle. The challenges and high computational demands represent the biggest obstacles encountered, emphasizing continued research and development on biometrics.

1.5.3 Security

Security and accuracy of biometric-based systems are of the highest priority. Although there are many attack plans against biometric systems available [10], there are two major disapprovals of the biometric technology that are yet to be satisfactorily dismissed:

- **Non-Secrecy:** Biometric identifiers are less secrets. That means that an attacker could possess knowledge of legitimate biometric data, allowing them to fraudulently input this data into the biometric model to gain unauthorized access. Its concern revolves around the possibility of attackers having access to or knowledge of the biometric characteristics of legitimate users.

- **Irrevocability in Patterns:** Biometric patterns are not revocable. Once a biometric identifier has been compromised or exposed, the legitimate user cannot change or revoke their biometric traits to prevent unauthorized access. This poses a challenge when an individual's biometric data has been compromised.

It's important to note that knowing biometric identifiers doesn't necessarily equate to the ability to inject those identifiers' measurements into the system. The challenge lies in designing biometric systems that are robust and secure enough to distinguish between legitimate and manipulated biometric inputs. Such a system would only accept genuine biometric presentations and would not be fooled by tampered or spoofed measurements.

By creating a secure biometric system that reliably distinguishes between real biometric data and fake or altered inputs, we could eventually eliminate the need to revoke compromised identifiers altogether. This would mark a major step forward in biometric technology and security, tackling issues around the lack of privacy in biometrics and the inability to reverse compromised biometric data.

1.5.4 Privacy

The reliability of a biometric system in providing undeniable proof of an individual's identity raises several valid concerns among users. These concerns touch upon various aspects of privacy and potential misuse:

- **Privacy and Tracking:** Users worry whether the indisputable proof offered by biometrics could be exploited to monitor individuals, potentially encroaching upon their right to privacy. The capability of biometric systems to uniquely identify individuals has led to concerns about surveillance and unwanted tracking.
- **Unintended Use of Biometric Data:** Some people fear that the information obtained from the biometric data collected will be used in other ways different from what is planned. For instance, users may be concerned that fingerprints used for controlling access, can be used to search against criminal databases. This concern stems from the potential for biometric data to be used in ways not intended when originally entered into the system.
- **Cross-Linking of Data:** Another issue is that machine learning can be used to correlate information from different records of one individual using biometric data. For instance, the joining of health insurance records with grocery shopping references could be just a violation of privacy.

There is a growing necessity to implement safeguards that ensure the ethical and appropriate use of biometric data. A significant concern is how to reassure individuals that biometric technologies are

employed solely for their intended purposes. People need to feel confident that these systems are not being misused or repurposed for unintended objectives. Ensuring trust in biometric systems is vital for widespread acceptance. One of the biggest challenges in deploying such information systems is establishing verifiable functionality. This means that users must be able to confirm that the systems operate as promised. Transparency in the use of biometric data is essential for building trust. Furthermore, effective governance policies must be in place to oversee these technologies. Overall, addressing these issues is crucial for the responsible advancement of biometric applications. Ensuring ethical use will ultimately enhance user confidence in these systems. One way is to create a system that records the decisions for every authentication, also logs them in firmware, and then only allows people who are registered with their biometrics to use an access control policy mechanism.

1.6 Biometrics Comparison

The comparison made on various biometric technologies provides a brief view of the common biometric methods mentioned by Sinha (2007) [11]. As with the previous comparisons, ('H' – 1), ('M' – 2), and ('L' – 3) are “High”, “Medium”, and “Low”, respectively. Here is one of the most often cited lists of biometric choices:

- i. **DNA:** DNA is indeed unique to each distinct individual, making it a powerful identifier. However, its use in various applications, especially for identification, is limited by several factors:
 - a. **Contamination and Sensitivity:** DNA can be stolen and misused because it's easy to take a sample from someone without them knowing and use it for bad purposes.
 - b. **Automatic Real-Time Recognition:** Current DNA matching technology relies on cumbersome and expert-dependent chemical methods (wet processes), making it unsuitable for online, non-invasive recognition.
 - c. **Privacy Issues:** Investigation of the DNA test can give information about the likelihood of an individual to develop some diseases, about the genetic information, it is possible to speak about tendencies of discrimination during job seeking.
- ii. **Ear:** It has been suggested that the shape of the ear and its cartilage are unique to each individual. Ear recognition methods focus on comparing key points on the outer ear with specific landmarks. Despite this, ear features alone may not provide enough distinction for identification. They are often used in combination with other biometric traits. Consequently, ear recognition is not expected to be a primary identifier on its own.

- iii. **Face:** Face recognition, a non-intrusive method, primarily uses facial photos for identification, with applications ranging from dynamic, uncontrolled scenarios, such as airports, to static, regulated verifications, like mug shots. Key methods include analysing facial features' location and shape, and overall face image analysis, though current systems have limitations in image acquisition and struggle with varying angles and lighting. Reliably identifying individuals solely based on facial features remains debatable, necessitating automatic face presence detection, localization, and recognition from any viewpoint for real-world effectiveness.
- iv. **Infrared thermogram of the face, hands, and veins:** Each person has a unique way of radiating heat, which can be captured discreetly by an infrared camera, similar to how regular photos are taken. This technology could be used for hidden identification. A system that relies on thermograms is non-invasive and doesn't require touching, but it can be challenging to get clear images in environments with nearby heat sources, like car exhausts or heaters. For hand vein identification, the back of a closed fist is scanned using near-infrared imaging. However, one major barrier to using thermograms widely is the high cost of infrared sensors.
- v. **Fingerprint:** People have used their fingerprints to prove who they are for hundreds of years, and studies have shown that this method of matching fingerprints may be a pretty good way to find people [12]. Between the ridges and valleys, on the other hand, during the first seven months of pregnancy, a fingerprint is formed. Fingerprints of identical twins and people who are not identical are different from each other and from finger to finger. A fingerprint scanner now costs about 1200 Rs for large sales, and the cost of support and integration for a fingerprint-based biometric is low enough for most uses. The current generation of fingerprint recognition systems provides the adequate accuracy required for small and medium-range identification systems with fewer than a hundred to a few hundred users and mainly in verification applications. A single individual uses several hundred fingers to leave behind palms, while the sensors can also take more information from each palm to allow the scanning of millions and millions of identities for giant-scale interactions. A disadvantage of the earlier fingerprint detectors is the high levels of utilization of computational resources, especially in identification. At last, a few people have environmental, genetic, aging, or occupational special conditions fingerprint patterns that are not conducive to automatic identification. (reads: manual workers who may have a high frequency of wounded or bruised fingerprints from too much hard physical labour).

- vi. **Gait:** A person's gait is a detailed biometric that describes how they walk in space and time. Gait isn't meant to be very accurate, but it can be checked in some low-security situations because it can tell the difference. Gait might not stay the same over time due to its behavioral nature. This is especially true if there are big weight changes, serious damage to the joints or brain, or being drunk. Gait analysis could be a true biometric because learning someone's walk is like learning their face. Gait-based systems require a lot of computing power and data because they watch video sequences of a person walking and measure several different actions of each articulating joint.
- vii. **Hand geometry:** Hand geometry methods look at the unique features of a being's hand, similar to the profile of the palm and the sizes of the portions and fingerprints. These verification systems appear resilient to factors like dry climates and skin dryness. This stability makes them reliable for biometric identification. However, because hand geometry is not very unique, these systems are not well suited to finding individuals in large groups. In the same manner, a child's hand geometry may also develop since children all grow in different phases in their lives. It is difficult, for instance, to capture hand geometry data from a hand wearing an ornament like a ring or a hand affected by conditions such as arthritis. Furthermore, the size of hand geometry systems limits their use in certain products, like laptops. Some verification methods use measurements from the whole hand, often focusing on the middle and index fingers. While these devices are still larger than those used for other biometric methods, like fingerprints or facial recognition, they are more compact than traditional hand geometry systems.
- viii. **Iris:** Between the pupil and the sclera, the ring-shaped portion of the eye changes texture during foetal development. This unique pattern remains unchanged during the first two years of life. It serves as an interesting identifier, as it is specific to each individual. The early development of this texture adds to the uniqueness of a person's eye. This feature plays a fascinating role in biometric identification systems. This intricate texture is highly unique, making it useful for identifying individuals. Modern recognition systems allow for large-scale identification based on iris data due to their high accuracy and speed. Each iris is unique, even in identical twins, and it's quite difficult to surgically change its texture. In contrast, it's relatively easy to detect fake irises, such as those created by designer contact lenses.
- ix. **Keystroke:** It is believed that everyone has a unique way of typing on a keyboard. While this method of identifying people isn't expected to be completely exclusive, it offers enough distinguishing details for identity verification. Keystroke dynamics, a type of behavioral

- biometric, can show notable differences in the typical typing patterns of individuals. Additionally, keystrokes can be secretly recorded while someone is entering information into a system.
- x. **Odor:** Each thing is known to emit an Odor indicative of its chemical makeup, and this might be utilized to differentiate between different objects. A set of chemical detectors is introduced to a breath of air around an object; every detector is tuned to a specific set of (fragrant) chemicals. Everyone has a specific part of their body Odour, whether it's an animal or a human being. It's unclear whether deodorant Odors and the changing chemical makeup of the surroundings can affect the invariance of body Odors.
 - xi. **Palm print:** I was intrigued by the idea that the palmar surface of our hands is a pattern that can't be considered random because it is too studied: it is not unlike fingerprints' ridges and valleys. Since the length of the palm is much larger than an individual finger, it is capable of scanning even better and more diverse types of impressions than those of fingerprints. That is the reason they have to store results over a larger area; palm print scanners cost more than fingerprint sensors and are bigger. Furthermore, human palms have more crucial characteristics that can be distinguished, including the main lines and wrinkles, which require relatively low-defined images along these features for identification at comparatively lower cost [13]. Finally, hand geometry and features of all parts of the palm, such as ridges, major lines, and wrinkles, can be added to palm geometry to make the most accurate biometric system. This can be done with a high-resolution palm print reader.
 - xii. **Retinal scan:** The recent structure of retinal vasculature and its distribution over each person's and each eye's surface is believed to be individual. As it is acknowledged as the safest biometric, the human retinal vasculature is almost impossible to redesign or counterfeit. To capture a defined sector of the retinal vasculature, a person aligns the eye with an eyepiece and aims at a particular sector in the visual field. A subject must collaborate with the communicator, connect visually, and exert considerable effort to capture the image. Consequently, retinal biometrics face limited acceptance. Additionally, the public often disregards retinal scans since they can reveal medical conditions like hypertension.
 - xiii. **Signature:** It is widely acknowledged that handwriting reveals aspects of an individual's personality. In various domains such as politics, law, and economics, signatures serve as a recognized form of authentication. Although they require effort and physical contact with a writing instrument, signatures remain widely accepted. As a form of behavioral biometric, signatures are influenced by the emotional and physical states of the signatory and can change

over time. Some individuals possess highly distinctive signatures, with significant variations from one impression to the next. Additionally, skilled forgers may successfully replicate signatures, potentially deceiving authentication systems. This variability and potential for forgery raise concerns about the reliability of signatures. Furthermore, factors like hypertension contribute to the public's hesitance toward retinal scan biometrics. Overall, while signatures hold value as biometric identifiers, their limitations must be acknowledged.

- xiv. **Voice:** Voice is both a behavioral and physiological biometric. An individual's voice is fleshed out by the form and dimensions of the fellow appendages (used to make sounds — e.g., the mouth, nasal cavities, lips, and vocal tracts), as in any case. Standard physiological properties of human speech are the same for every person, but you can hear our habitus in behavioral speech (behavioral speech changes along with time because we grow up, get ill, catch a cold, or just feel sad) and voice lacks individuality so identification based on voices would not be possible. A text-dependent speech recognition system works by asking the user to say a fixed sentence that has been predefined later. Despite what the speaker says, he can always be identified using a text-independent speech recognition system. Speech-based recognition is limited by the sensitivity of speech features to multiple conditions, such as noise in the background. Phone-based use cases. In phone usage, speaker identification also performs well, but the poor sound quality of this communication channel results in a lower quality of the sound stream that has a foreign key.

Table 1.3 reflects a significant comparison of the biometric approaches described above on seven parameters. Most importantly, the needs of the application will greatly determine its suitability for a particular biometric technology.

Table 1.3 Assessment of biometric traits

“1-High, 2-Medium, 3-Low” [111]

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability
Human Face	1	3	2	1	3	1
Human Finger-prints	2	1	1	2	1	2
Hand-Geometry of human	2	2	2	1	2	2
Keystrokes by humans	3	3	3	2	3	2
Hand-Veins of body	2	2	2	2	2	2
Iris sensitive region	1	1	1	1	1	3

Retina part	1	1	2	3	1	3
Signature	3	3	3	1	3	1
Voice-based biometrics	2	3	3	2	3	1
Facial-Thermograph	1	1	3	1	2	1
Odor of the body	1	1	1	3	3	2
DNA structure	1	1	1	3	1	3
Gait type	2	3	3	1	3	1
Ear Canal with different edges	2	2	1	2	2	1

1.7 Biometric Data Processing Steps

All biometric data will be transformed according to the processing steps described in Figure 1.5

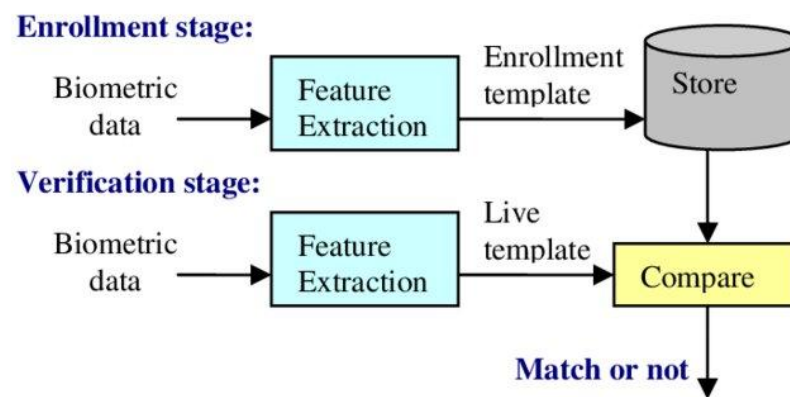


Figure 1.5 Processing steps of a biometric system [112]

- Image capture or acquisition:** The biometric data (like face, iris, signature, fingerprint) is digitized using input devices (like a digital camera, fingerprint scanner, or iris scanner) and stored in memory.
- Preprocessing:** The acquired data is prepared for feature extraction by normalizing the signal and removing biases, such as rotating and thinning fingerprints.
- Feature extraction:** From the pre-processed data, basic components are selected to eliminate complexity and make the identification of patterns possible for all biometric types.
- Template storage:** The pull-out features are stored securely in a database for future reference and biometric operations.

Threshold computation: Presentations from the user and impostors are matched to determine a threshold for identity verification. Thresholds can be system-wide or user-specific to minimize errors, though some modalities like fingerprints may not need a threshold.

1.7.1 Biometric Operations

The processing steps mentioned earlier will be utilized in the biometric operations.

- i. **Enrolment:** A user is added to the biometric system. Several samples of that user's biometrics are collected, then prepared, turned into usable features, and finally processed.
- ii. **Verification:** The claimed user's model will be compared to the user's biometric data provided for identification claims. The user's biometric data for the identity claim is obtained, pre-processed, translated into features, and post-processed. Next, it is matched with the model of the claimed person, and the resultant score is compared to either a generic threshold value or the stored threshold calculated for the claimed user.
- iii. **Identification:** To find the most likely source of the biometric presentation, the user model is searched through the database. It is recommended that the source of the performance be the user model that accepts the highest score for the presentation.

1.8 Biometric Applications

The following categories sum up biometric applications:

- i. **Law Enforcement:** Probably the greatest user base for biometrics is the law enforcement community. Automated Fingerprint Identification System (AFIS) technology is utilized by police forces all over the world to identify suspects, match finger photographs, and process suspects.
- ii. **Banking:** Biometric security can be applied to transactions at the point of sale and Automated Teller Machines (ATMs), which are especially susceptible to fraud. For both bank consumers and bankers, other expanding markets like phone and online banking must likewise be completely secure. Numerous biometric technologies are currently vying for acceptance across these wide-ranging, varied industry opportunities.
- iii. **Computer Systems:** Literally, biometric technologies are configured for the protection of computer networks (or logical access control). It has great potential, especially for the market to move to Internet applications in a big way, at least as far as biometrics is concerned. The field is moving quickly as thieves are becoming more interested in bank account information, commercial intelligence, credit card numbers, and health records.
- iv. **Physical Access:** Biometrics are increasingly utilized globally to enhance security in various environments, including schools, hospitals, amusement parks, nuclear facilities, military bases, and retail stores. As the demand for improved security grows among parents, businesses, and governments, biometrics is likely to become more widely accepted and valued

as a security measure. The potential applications for this technology are extensive. For instance, homes and vehicles, typically seen as safe havens, are still vulnerable to theft. If biometrics are effectively marketed and made affordable, they could represent an optimal solution for security concerns. Their ability to offer unique identification can deter unauthorized access and protect personal property. Furthermore, the ongoing advancements in biometric technology will likely increase its reliability and efficiency. As society becomes more aware of the benefits, the integration of biometrics will continue to expand. Ultimately, embracing this technology can lead to a safer environment for everyone. The future looks promising for biometrics as a key component of security strategies.

- v. **Benefit Systems:** Biometrics are particularly important in benefit systems like welfare to combat fraud. Biometrics is in a great position to take advantage of this enormous market opportunity, and suppliers are strengthening their already solid relationship with the benefits community.
- vi. **Immigration:** To fight terrorism and drug trafficking, a huge number of people are entering the country illegally, and the general number of people allowed to enter every country puts a lot of pressure on its immigration services. The government should be able to find people who break the law and sort out the legal travellers almost instantly and automatically. Biometric models are being used in many areas and purposes right now, so that these things can happen. A lot of new fingerprint technologies are used and studied by the US Immigration and Naturalisation Service. There are now methods in the United States that make it less likely for people who aren't supposed to be there to come here and control the movement of people who are allowed to stay.
- vii. **National Identity:** Local and national administrations are beginning to feel the support of biometric technologies in tasks of urban and population growth evaluation, identification of individuals, and combating vote rigging. This is usually by storing a biometric template on an ID card, which also serves as a national identification card. In this regard, fingerprint scanning is more efficient, and the projects have been launched in countries like South Africa, Jamaica, Lebanon, and the Philippines.
- viii. **Time, Attendance, and Monitoring:** There are time-card devices that are used to register as leaves for coming in, out, and on breaks for employees during the day closing traditions. Time governance software can be connected with biometrics to execute based on individuals and administrative accounting reports, and also when manual methods are taken over the system abuses end.

1.9 Motivation of the Thesis

The motivation for a thesis on Hybridized biometrics by considering Side-Face is driven by several key factors that address the restrictions of unimodal biometric systems and capitalize on the strengths of integrating multiple biometric modalities. Here are some detailed points that could form the basis of this motivation:

i. Enhanced Security and Accuracy:

- a) **Overcoming Limitations of Unimodal Systems:** Unimodal biometric systems, which rely on a single type of biometric identifier (such as fingerprint, face, or iris), can be vulnerable to spoofing, noise, and variations in the data. Multimodal biometrics combine two or more identifiers, significantly improving accuracy and making it more difficult for impostors to breach the system.
- b) **Reduction in Error Rates:** Multimodal systems can lower both FAR by comparing different sources of biometric data, and hence lower FRR also. this means that multimodal systems provide more robust and reliable biometric identification and authentication.

ii. Improved User Experience:

- a) **Increased Accessibility:** By integrating multiple modalities, systems can accommodate users who may have difficulty providing a particular biometric. For instance, individuals with worn-out fingerprints can use facial recognition or voice recognition as alternative identifiers.
- b) **Flexibility and Convenience:** Users can choose the modality that is most convenient for them in different contexts, enhancing the overall user experience and satisfaction with the biometric system.

iii. Comprehensive Security Frameworks:

- a) **Enhanced Anti-Spoofing Measures:** Using multiple biometric traits lowers the chances of spoofing or imitation of the system by the attackers by a very big margin. For instance, although it is possible to forge a fingerprint to match a biometric scanner, it is going to be far more difficult to forge both the fingerprint and the iris at the same time.
- b) **Layered Security Approach:** Multimodal systems can implement a layered security approach, where different biometric modalities are used in non-matching stages of the authentication process, providing a higher level of security.

iv. Technological Advancements:

- a) **Integration with Emerging Technologies:** The rapid development of AI and ML algorithms enhances the ability to process and analyse multiple biometric inputs effectively. These technologies improve the performance and reliability of multimodal biometric systems.
 - b) **Interoperability and Scalability:** Advances in sensor technology and data processing enable the seamless integration of various biometric modalities, making these systems more scalable and adaptable to different environments and applications.
- v. **Addressing Privacy and Ethical Concerns:**
 - a) **Improved Data Privacy:** Multimodal systems can enhance data privacy by distributing biometric information across different modalities, making it harder for any single breach to compromise the entire identity of a user.
 - b) **Ethical Considerations:** By providing a more accurate and secure form of identification, multimodal biometrics can reduce the chances of identity theft and fraud, which are significant ethical concerns in today's digital world.
- vi. **Applications in Diverse Domains:**
 - a) **Broader Applicability:** Multimodal biometrics can be applied in several domains, including border control, financial services, healthcare, and personal devices, offering enhanced security and user convenience across different sectors.
 - b) **Support for Critical Infrastructure:** In critical infrastructure areas, such as national security and defence, the reliability and robustness of multimodal biometric systems can provide crucial support in maintaining security and operational integrity.

To address these reasons, a thesis on multimodal biometrics can make a big difference in the creation of safer, more reliable, and easier-to-use biometric systems. This will ultimately advance the field of biometric research and its practical uses in everyday life by looking at the side face of humans, which includes a portion of the side face and the most noticeable parts of the ear, which are called the auricle.

1.10 Objectives

- 1) To apply pre-processing techniques on a standard data set of side images for detecting objects (side face) using a new object detector algorithm
- 2) Identification of dominant attributes for model development by applying the feature selection technique.

- 3) To develop a hybrid biometric model on dominant attributes for verification using Auricle, Ear, and Side Face.
- 4) Compare and analyze the model with the existing model.

1.11 Problem Statement

The dissertation assesses the process of integrating PCA and CNN to recognize people [115]. This said hybrid generalizes both these methods to improve the reliability and efficiency of biometric recognition systems. PCA works as a dimensionality reduction technique, making its input easier compared to complex datasets it deals with by identifying only relevant features, thus reducing computational load. By preserving the key aspects of facial images, PCA creates a more compact and cleaner representation of the data, making it easier for the CNN to handle. Subsequently, CNNs, recognized for their strong feature extraction abilities, are applied to the data processed by PCA. The CNN's multiple layers allow it to learn complex patterns and hierarchical representations of the facial features, improving the identification accuracy. The combination of PCA and CNN ensures both efficiency and high performance, as PCA reduces redundant information while CNN excels at classifying detailed facial features. The thesis demonstrates that this combined method enhances person identification accuracy, reduces computational overhead, and is particularly effective when working with large, high-dimensional datasets. This hybrid approach proves to be a robust solution for real-time biometric identification systems, achieving a balance between speed and precision.

1.12 Thesis Organization

I. Chapter 1: Introduction

- This chapter introduces the topic of biometric systems and presents an outline and contributions of this Ph.D. thesis.

II. Chapter 2: Literature Review

- This chapter reviews related works and discusses the motivations for this thesis based on these previous studies.

III. Chapter 3: Inspiration and Driving Forces Behind the Study

- This chapter outlines face detection, feature extraction, and recognition processes, emphasizing their roles in effective human face identification using machine learning and deep learning techniques.

IV. Chapter 4: Proposed System

- This chapter summarizes the application scenario, system performance, and implementation of the proposed system.

V. Chapter 5: Conclusion and Future Work

- The chapter summarizes the key contributions of the side face biometrics model and outlines future directions to enhance its accuracy, robustness, and applicability in real-world scenarios.

1.13 Summary

Biometric attributes play a crucial role in modern identification and verification systems, enhancing security and simplifying the identification process. They facilitate the efficient delivery of various services across multiple sectors. Two main groups define these biometric characteristics: physiological and behavioral. Physiological biometrics covers traits including facial recognition, fingerprints, iris patterns, retinal scans, palm prints, and even DNA profiles. Each of these traits provides unique identifiers that can improve accuracy in authentication. As technology evolves, the applications of these biometric features are expanding. Their integration into systems enhances overall security and user experience. Understanding the different categories of biometric attributes is essential for effective implementation in identification processes. These characteristics are constant throughout a person's life, and for this reason, they are useful when developing security systems. On the other hand, behavioral biometrics rely on a person's behavior, not features of the physical nature. These are: voice recognition, gait recognition, and keystroke dynamics. Voice recognition analyzes the unique patterns in a person's speech, including pitch, tone, and accent. This biometric is commonly used in customer service applications and voice-activated systems like virtual assistants. Gait analysis examines the way a person walks, identifying individuals by factors such as stride length, posture, and body movements. It is an emerging technology that is particularly useful in surveillance and security, where people may not always be aware of being monitored. Biometric systems have a wide range of applications across various sectors. In security and access control, biometrics are used to authenticate individuals attempting to gain entry into secure areas, from corporate offices to airports. In surveillance, biometric systems help law enforcement agencies identify persons of interest from crowds in public places. Healthcare facilities use biometrics to verify patient identities and maintain secure medical records, while financial institutions deploy biometric systems to ensure secure transactions, such as in mobile banking apps and ATMs.

While traditional biometric systems, such as frontal face recognition, are highly effective in controlled environments, they have limitations when it comes to real-world scenarios, particularly in surveillance where individuals may not be facing the camera directly. This is where side face biometrics comes into play. Side face recognition focuses on identifying individuals based on the geometry of their side profiles, which includes the contours of the ear, nose, chin, and jawline. This method is beneficial in real-time surveillance where cameras may capture people from various angles, making it an essential tool for improving identification accuracy in dynamic environments. To enhance side face recognition, a high level of integration among biometric traits is essential. This

approach can significantly improve both the correctness and consistency of recognition systems. By combining “side-face” recognition with other identification methods, such as ear biometrics, the system becomes more robust. Integrating these biometric traits allows for a comprehensive analysis, reducing the chances of errors. This multimodal system leverages the strengths of each trait for better performance. As a result, it can effectively differentiate between individuals in various conditions. Overall, this integration represents a promising advancement in biometric recognition technology. The method can work even when there is no frontal face data. This is mostly because of how the face looks from the side and how the ears are shaped. So, the hybrid method, which includes biometrics from both the frontal and side faces, is the best way to deal with the problems caused by the standard frontal face recognition threat. CNN is used in this system because it is very accurate and reliable. This makes it great for government surveillance, immigration control, car security, and even healthcare. Using side face biometrics in this hybrid model is a step forward in biometric recognition because we need systems that work well, are always on, and can be changed to fit people's needs.

Chapter 2

2. Literature Review

Rising as the most often used biometric technology in recent years, facial recognition has also become the favoured method in computer vision and pattern identification. Since users of it do not have to engage with the device physically, its non-invasive character appeals especially to this simplicity of use, which lets one apply a great variety of ideas in many different disciplines. Facial recognition increases its adaptability since it can be done from a distance, unlike techniques like fingerprint or iris scanning. The technology is widely adopted for identity verification and authentication in various industries. Sectors like banking and commerce use it to enhance security measures. Additionally, it plays a significant role in surveillance systems and educational environments. The growing reliance on facial recognition reflects its effectiveness and convenience. As the technology continues to advance, its applications are likely to expand even further. Overall, facial recognition is reshaping how we approach identification and security. In banking, facial recognition enhances security by providing an additional layer of verification during transactions, particularly in online and mobile banking platforms, where customers can authenticate their identities through facial scans. This reduces fraud and ensures secure transactions. Similarly, in commerce, this technology is used for purposes like personalized shopping experiences, where retailers can analyze customer demographics and behaviour patterns based on facial data to offer tailored services. In addition, facial recognition is increasingly employed for contactless payments, allowing customers to complete transactions swiftly and securely by simply showing their faces to a camera. Security and surveillance are other significant areas where facial recognition plays a pivotal role. Law enforcement agencies use it to identify suspects, monitor public spaces, and prevent potential security threats. Its ability to analyze video feeds in real-time enables quick identification of persons of interest, ensuring faster response times in critical situations. Airports, public transportation systems, and crowded events utilize this technology for managing security without interrupting the flow of individuals, making it a highly effective tool for large-scale monitoring. In education, facial recognition is being used for automated attendance systems, where students' faces are scanned as they enter classrooms. This not only saves time but also improves accuracy in tracking student participation. Additionally, it can be used for security on campuses, ensuring that only authorized individuals can access certain areas. Furthermore, facial recognition is being explored for use in

online learning platforms to monitor student engagement and ensure the integrity of remote examinations. A typical biometric system consists of several key operations, as illustrated in Figure 2.1 below. The essential stages of a standard biometric system encompass the subsequent steps: Initially, the image is captured via a camera or sensor. This is the system input, and the previously specified image will function as the input to the system. Subsequently, the analysis of the provided image is performed, assessing the geometric contours of the eyes, their dimensions, the prominence of the nose, positioning angles, mouth contour, and the angles of the facial structure. Upon extraction of features, the system juxtaposes them with a pre-existing facial data database to ascertain the individual's identity. This comparison leads to the final output, where the recognized identity of the individual is displayed or recorded. This entire process happens within seconds, making it both efficient and effective for real-world applications across various industries.

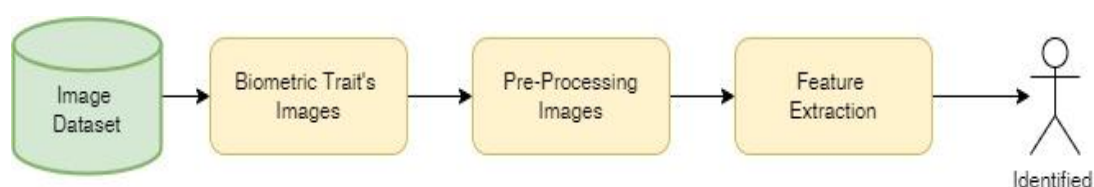


Figure 2.1 Generic Biometric Identification System [112]

Face recognition has consistently been a crucial application in pattern recognition, with its potential has increased recently. The advancements in recent years can be attributed typically to alterations in “*Convolutional Neural Networks – CNNs*” concerning the design of the face recognition issue. Convolutional Neural Networks (CNNs) are now the preeminent answer in this field, as they contain the distinctive ability to learn and properly represent individual facial features. The methods we have examined do not depend on the creation of predetermined facial characteristic characteristics, which are often extracted manually from facial photos. In contrast, CNNs employ deep learning algorithms to extract these properties from data. The transition to deep learning has revolutionized face recognition systems, enhancing their precision and scalability, especially in practical applications utilizing extensive training datasets. In their absence, previous face identification technologies incorporated conventional machine learning approaches including SVMs or NNs for identification. These methods proved well in some specific and limited conditions but failed in actuality mostly due to the intensity of light, facial movements, or changes in pose. The feature extraction by hand worked very well for the image set and was very efficient for small tasks, yet it could not handle the variability of the human faces in the way modern CNNs do. The advancement of computational power and deep learning algorithms has led to significant improvements in face recognition systems. These technologies leverage increased processing capabilities to handle large datasets effectively,

improve feature learning, and enhance accuracy across various applications. CNN-based face recognition has witnessed a lot of research developments, particularly on the problems of pose variations in real application conditions. In practical situations, an individual's face is not always completely visible or orientated to correspond with the frontal perspective, complicating the process of identification. CNNs, with their ability to learn hierarchical feature representations, have proven capable of mitigating some of these issues by focusing on both global and local facial features that remain consistent across different poses. However, even with these advancements, face recognition continues to be a challenging problem, particularly in unconstrained settings where image quality may be poor or the subject's face is partially obscured. The advancement of these terms and factors can place a significant challenge even to the state-of-the-art algorithms that aim to identify or gather recognition from any person. Face verification from frontal to profile is one of the toughest problems in face recognition. It has become an important topic in computer visualization of images and biometrics. For real-world applications, like surveillance, the system may at best capture a profile or side view of the user's face with a partial face available for recognition. This approach tries to synthesize the appearance of the face as observed from its front even though we can only observe a profile image. These methods were successful in increasing recognition rate notably in environments where pose variation is problematic, if not redundant. The field of side face biometrics, which focuses on analyzing a person's face from a profile perspective, has also made considerable progress in recent years. This is an important area of study, as profile faces are commonly encountered in surveillance footage and other real-world scenarios. Traditional face recognition systems, which were primarily designed for frontal face images, struggled with recognizing faces from a profile view. However, new techniques in side face biometrics, powered by advances in CNNs and deep learning, have improved the accuracy of recognizing individuals from these challenging angles. By learning distinctive features from profile views, these systems can now perform more effectively in scenarios where full facial visibility is not available. In addition to pose variations, other factors like image quality, lighting conditions, and facial expressions continue to pose challenges for face recognition systems. Although CNNs are particularly effective in learning robust feature representations, their performance may deteriorate with low-quality input images or when the subject's face is partially obscured. To address these challenges, researchers are exploring various data augmentation techniques, such as creating synthetic training data to simulate different lighting conditions and occlusions. This enhances the system's ability to generalize to real-world situations, where such differences are unavoidable. Moreover, large-scale datasets have played a crucial role in the success of CNN-based facial recognition systems. The availability of diverse facial datasets,

containing millions of images with different poses, lighting conditions, and expressions, has enabled deep learning algorithms to learn more robust and generalizable facial features. These datasets allow CNNs to be trained on a wide variety of facial characteristics, making them more resilient to variations and improving their performance in recognizing faces in both controlled and uncontrolled environments. However, maintaining privacy and ethical considerations when using such large datasets has become an area of concern, as the use of personal facial data raises issues related to consent and data security. This chapter explores the existing literature on various biometric features with a focus on side face recognition. The primary aim of this study is to evaluate the accuracy of biometric identification in highly secure sectors, such as border control, access management, and civil identification. A thorough review of research in identification and other high-security domains was conducted. It was found that there are limited published studies addressing security analysis that integrate multiple biometric features into a hybrid system.

2.1 Side Face Literature Review

The advancement of automated face recognition technology is largely credited to the pioneering efforts of Woody B., C. Bisson, and H. Chan Wolf [113]. Their groundbreaking work laid the foundation for what has become a crucial technology in numerous fields, including social media, security, and beyond. Today, automated face recognition is integral to various applications, enhancing both convenience and security in our daily lives. In the mid-1960s, specifically during the years 1964 and 1965 [56], these innovators laid the groundwork for what would become a transformative area of research and development. Woody Bledsoe, who is often credited as one of the foundational figures in the field, spearheaded efforts to explore the potential of computers in identifying and recognizing human faces [113]. His work was not in isolation; he collaborated closely with Helen Chan Wolf and Charles Bisson, two other key figures who significantly contributed to these early efforts.

Bledsoe's research during this period was groundbreaking. He, along with his colleagues, focused on developing algorithms and methods that could enable a computer to distinguish one human face from another—a task that, at the time, was incredibly challenging given the limitations of computational power and the nascent state of computer science. The research conducted by Bledsoe and his team involved the analysis of facial features and the creation of mathematical models that could be castoff to classify individuals based on these features [114]. The significance of their work cannot be overstated. They were among the first to consider the problem of facial recognition systematically, applying computer science principles to what had previously been a purely human capability. Their

efforts laid the foundation for the algorithms and technologies that would later evolve into the sophisticated facial recognition systems we have today. Moreover, Bledsoe and his team were able to foresee the potential applications of facial recognition technology long before it became a mainstream concern. They recognized that if a machine could be taught to recognize faces, it could revolutionize security, law enforcement, and even personal identification. Their research, documented in various publications including those from 1966 and earlier, provided a roadmap for future researchers and engineers.

Shuyi Li et al [120]. provides a comprehensive analysis of the integration of various hand-based biometric modalities, such as fingerprints, palm prints, and hand geometry, to enhance recognition accuracy and security. The authors discuss the advantages of multimodal systems over unimodal approaches, including improved robustness against spoofing and environmental challenges. They also examine different fusion strategies at various levels—sensor, feature, score, and decision—and evaluate their effectiveness.

Wanchao Li[122] highlights the transition in aquaculture from single-modality systems, which face limitations in complex environments, to multimodal fusion approaches integrating visual, acoustic, and biosensor data for enhanced monitoring. Multimodality improves accuracy and robustness in tasks like fish tracking and behavior analysis. The authors emphasize the need for standardized datasets and evaluation frameworks to advance this field. They conclude that multimodal fusion holds great potential for transforming digital aquaculture.

Despite the rudimentary nature of the technology at the time, the work of Bledsoe, Chan Wolf, and Bisson was instrumental in establishing the fundamental concepts of facial recognition. They were among the first to attempt to quantify facial features in a way that could be interpreted by a machine, a task that required not just technical expertise but also a deep understanding of both human anatomy and the emerging field of computer science.

Facial Recognition is one of the enhanced techniques that employ the Face Area in a Scanner to Authorize the identity of a particular person. To do this, that particular system acquires the digitized image or a live frame of a person's face, and through programmed algorithms, it is normally able to establish, quantify, compare specific facial features, and lastly, authenticate the fact that the person is in the database. Through these characteristics, the system is in a position to uniquely match the face and locate an existing record on the person; or determine that the face belongs to an individual among a specific group.

A biometric AI application can be defined in this way as an application that uses unique biological patterns, mainly the texture and shapes of faces, for identification purposes. This technology is found

in many areas such as security where it is used in surveillance and identification of suspects; in law enforcement; and in consumer electronics where it is used in authentication of forms of authentication of devices like smartphones and laptops. These systems are increasingly indispensable for enhancing security and comfort in all aspects of daily life. However, their widespread use has raised concerns about privacy, ethics, and the potential for misuse, given that they involve collecting and processing sensitive personal information. Despite these issues, facial recognition technology continues to develop and find applications in various fields, presenting both opportunities and challenges for the future. In Bledsoe's early study, facial markers such as the mouth and eye centers were manually marked and then computationally adjusted for posture variations. To establish identity, the system then automatically measured and compared the distances between landmarks. Fully automatic algorithms in facial recognition systems perform both the detection of facial landmarks and the subsequent recognition process. They require only the facial image, automatically identifying key features like eye centers and comparing them against a database for identification. In contrast, partially automatic algorithms focus solely on the recognition task, relying on pre-identified coordinates of facial features such as eye centers. These coordinates are manually or semi-automatically determined and provided along with the facial image. Fully automatic systems are more comprehensive, while partially automatic systems require additional input for feature detection before recognition can occur[56].

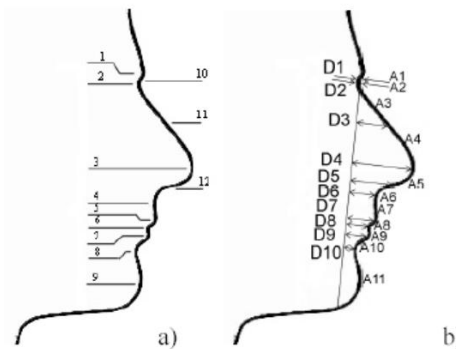


Figure 2.2 a) 12 – face recognition fiducial site of attention. b) The feature consists of 21 apparatuses: 10 distance D1-D10 (controlled using (D4+D5)) and 11- Profile arcs (controlled using (A5+A6)) [58]

A binary, black-and-white image is produced through the process of thresholding a grey-level profile image, where the black regions correspond to the facial area. Thresholding is a technique used to convert a grayscale image, which contains varying levels of intensity, into a specially converted binary image by selecting a specific amount of threshold value. All pixel values below this threshold are set to black, and those above it are set to white. This process simplifies the image by clearly

distinguishing the facial region, represented in black, from the background, which is rendered in white.

After the binary image is generated, the subsequent step in the pre-processing stage includes extracting the framework the arc of the frontal portion of the outline around the facial picture. This contour represents the boundary of the facial region, capturing the outline of the face. Extracting this contour is crucial as it serves as the foundation for further analysis in identifying specific facial features. The extracted contour curve now undergoes scale-space filtering commonly used to process images at different scales or levels of detail. With the help of this filtering using different scale values, the system may recognize features of different scales and importance within the facial silhouette. At any contour curve, using this method, twelve fiducial markers are recognized and considered automatically. The fiducial markers that are found in the face may include the corner of the eyes, the tip of the nose, or the edge of the lips. They are useful for the extraction of the feature which is relevant later and deliver the most important feature traits information about the shape of the face.

A collection of twenty-one feature attributes is obtained from these twelve fiducial markers. The distances between particular fiducial points, the angles these points produce, and other geometric aspects are examples of the measurements or qualities that these features indicate for the face. These attributes are used to capture the unique aspects of an individual's facial structure, making them valuable for tasks such as facial recognition, expression analysis, or other biometric applications. The most common approach widely used for measuring the dissimilarity of the vectors that resulted from the outline profiles is the Euclidean distance metric. It computes the distance between the points made by collection of coordinates in the n dimensional space and gives a measure of how close or diverse two vectors are. The process starts with Standardisation of feature characteristics, in which the data is put on a standard scale to enable accurate comparison afterwards. This normalisation is done using two appropriate fiducial markings which serve as references. These markings aid in registration of the feature vectors so that changes due to factors such as orientation or scale are kept to the lowest level.. By measuring the Euclidean distance between these normalised vectors, the degree of similarity between the outline profiles can be quantified. Smaller distances indicate higher similarity, while larger distances suggest greater dissimilarity. This method is essential for accurate classification and pattern recognition tasks. A total of 150 profiles, consisting of thirty individuals, were used for the experiments. [58].

Shreyansh Sharma, Anil Saini, Santanu Chaudhury introduces an improved decentralized fuzzy vault scheme leveraging Blockchain for multimodal biometric user authentication [124]. The approach

ensures enhanced security and privacy, offering a scalable solution for authentication systems. Dilip Kumar Vallabhadas proposes a cancelable convolutional neural network framework for biometric template protection using iris and fingerprint modalities [125]. Reem Alrawili provides an in-depth analysis of biometric user authentication applications, evaluation metrics, and challenges. It offers valuable insights for advancing biometric technologies and their practical implementations [126]. Vipul Vekariya presents a multi-biometric fusion approach to enhance human authentication for information security [127]. Li Wan, Kechen Liu explores a deep learning-based approach for photoplethysmography biometric authentication, enabling continuous user verification [128].

2.2 Ear as a Biometrics

The ear visualization can be done with either of the following three different methods:

- (I) taking an ear photograph
- (ii) pressing an ear on a flat piece of glass to take "earmarks"
- (iii) taking thermogram images of the ear.

The lobe and the outer ear giving the ear its look is the most interesting part of the ear even though the whole shape and design of the ear offers a lot of advantages. The structure of the ears is perfectly formed and once this is formed it does not change at any other time in one's life. According to medical literature [37], after the first four months of infancy, the ear development and growth is proportional in the growth pattern. The description of the different parts of the ear and the detailed dissection of the several segments of the ear are described in Figure 2.1. Getting an ear scan is the most widely used research technique. To identify a person, a picture is taken and then linked with earlier photographs. The primary application of earmarks is in the investigation of crimes. At the moment, earmarks are not recognized by courts, even though certain decisions are based on them. One way to tackle the issue of, say, hat hair, could be to use thermogram images.



Figure 2.3 Anatomy of the ear [37]

- I. Helix-Rim
- II. Lobule
- III. Anthelix

- IV. Concha
- V. Tragus
- VI. Antitragus
- VII. Crus of Helix
- VIII. Triangular Fossa
- IX. IncisureIntertregic

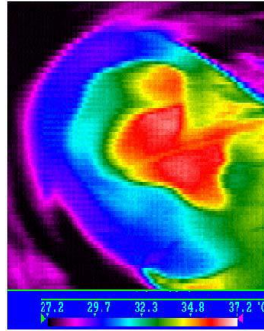


Figure 2.4 Thermogram image. (Burge and others, 1998) [20]

French criminologist Alphonse Bertillon was the first to notice the ear's potential as a biometric identifier. This groundbreaking insight laid the groundwork for further ear biometrics research. In 1949, American police officer Alfred Iannarelli carried out a thorough analysis of more than 10,000 ear pictures to pinpoint 12 unique biological traits that may be used to identify individuals [37]. Even though there wasn't a complete theoretical framework at first, Iannarelli's study laid the groundwork for ear biometrics. His research brought attention to how distinctive the outer ear's anatomy is for individual identification [37]. Using a deformable model for ear alignment and recognition, Zhou and Zaferiou improved the field in 2017 by resolving some of the drawbacks of previous methods, building on this foundation [54]. Even though Iannarelli's work was crucial in showcasing the possibilities of ear biometrics, the discipline has advanced dramatically with more advanced techniques to boost identification accuracy and dependability [37]. Burge and Burger (1997) presented the theoretical feasibility of an ear biometric system with an emphasis on its consistency and uniqueness over time [22][23][24]. To characterize each ear as an adjacency graph, they devised a Voronoi diagram; however, distinguishing between ear and non-ear curves remained a considerable difficulty. Expanding upon these findings, Moreno et al. developed a novel multiple identification technique that enhances human recognition using outer ear images by combining neural classifiers with macro data retrieved via a compression network [43]. In a related development, Herly et al. improved the accuracy of ear-based identification systems by introducing a different feature mining method using force pitch conversion, in which photographs are used as sources of force fields.

Despite the limited scope of the original database experiments, the outcomes showed great promise [69]. To evaluate the geometric shape of the ear, Choras presented a feature extraction technique that used contour detection; nevertheless, the technique had problems with imprecise curve detection [28][29][30]. When Victor et al. compared the dependability of face and ear biometrics using principal component analysis, they discovered that the face was a more reliable biometric identification [37][51]. Chang et al. performed a similar analysis on a bigger dataset in a later study and discovered no discernible difference in the performance of face and ear biometrics [27]. This implies that although face recognition was thought to be more trustworthy at first, further in-depth analysis using bigger datasets may provide more accurate information on how effective ear biometrics are. Combining face and ear recognition in multimodal systems has significantly increased the efficacy of biometric systems. To classify ears, Zhang et al. established a blended approach that integrates Independent Component Analysis (ICA) with a Radial Basis Function (RBF) network [40]. This innovative method surpasses the performance of traditional Principal Component Analysis (PCA) by effectively capturing more relevant features for ear classification. ICA helps in isolating statistically independent components, while the RBF network classifies these features with high accuracy. The combination of these techniques results in a more robust and precise classification system, demonstrating significant improvements over PCA-based approaches. The primary drawback of this approach is its dependence on carefully managed imaging settings and accurate picture registration. On the other hand, Sana et al. created a novel ear biometric system that uses the Haar wavelet transform [50]. This system only needs two training photos to construct the database, which makes it more practical and accessible. This development shows the possibility of more adaptable and user-friendly biometric systems that can adjust to different demands and circumstances. Additionally, Gupta and Prakash proposed advanced recognition techniques for ear, [48]. These innovations represent significant progress in addressing previous limitations and improving the reliability of ear-based identification systems.

Table 2.1 Feature extraction for ear using local descriptors with different approaches

Authors	Journal/ Conference	Method adopted	Database	No. of validations	Total number of images	Accuracy (%)
Burge and Burger[9]	SPIE Conference on Biometric Technology for Human Identification	Voronoi-diagrams	Self	Not Applied	Not Applied	Not Applicable
Moreno[30]	Conference: Intelligent Systems Design and Applications	Geometric-features	Self	49	188	43 — 83
Mu[31]	IEEE Computer Society Conference on Computer Vision and Pattern	Geometrical	USTB II	76	309	86

	Recognition Workshops					
Choras, & Choras[17]	Conference on Advances in Pattern Recognition	Geometrical	Self	Not Applied	Not Applied	100
Devi & Yahagi[19]	Journal of Electronic Imaging	SIFT	CP	18	101	78.78
Kumar & Zhang[27]	Pattern Analysis and Machine Intelligence	Log-Gabor wavelets	UND	112	455	89.99
Arbab & Zavar[2]	ECCV International Workshop on Biometric Authentication	SIFT	XM2VTS	62	250	91.5
Rahman[36]	Image vision computing	Geometric features	Self	110	350	87
Choras [26]	Pattern Recognition Letters	Geometry on the outline of the ear	Self	185	376	86.2
Guo and Xu [20]	Conference on Applied Research in Computer Science and Engineering	LBPS & CNN	USTB II	76	309	93.25
Arbab-Zavar and Nixon [1]	Face Recognition Vendor Test 2002	Log-Gabor	XM2VTS	63	250	85.57
Hai-Long & Zhi-Chun [21]	La photographie judiciaire	Wavelet transformation	USTB II	76	309	85.67
Badrinath & Gupta[17]	International Conference on Advances in Pattern Recognition	SIFT landmarks from ear models	IITK	106	1050	95.32
Kisku [38]	Conference on Advances in Computational Tools for Engineering Applications	SIFT from Color Segments	IITK	400	800	96.93
Nanni & Lumini [45]	Pattern Recognition	Gabor filters	UND	114	464	84.11
Xiaoyun & Weiqi [52]	International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC	Block partitioning with Gabor transform	USTB I	60	180	99.99
Bustard[25]	Systems and Humans	SIFT Point Matches	XM2VTS	63	252	96.48
De Marisco[31]	Conference on Computer Vision and Pattern Recognition	PIFS	UND	114	228	61
Kumar [39]	Pattern Recognition	Log-Gabor and SIFT	IIT Delhi I	120	700	85 and 95
Chan & Kumar [27]	IEEE Transactions on Pattern Analysis and Machine Intelligence	2D quadrature filter	IIT Delhi I	120	471	96.4
Kumar & Wu [39]	Pattern Recognition	PE with Log Gabor filters	IIT Delhi II	220	753	95.8
Prakash & Gupta [48]	Telecommunication Systems	SURF and NN	IIT Kanpur	300	2066	97.6

Paratim, Srangai, Partha, B. Mishra, and S. Dehuri designed a multimodal biometric system [59]. This method proposes the KDCV technique to enhance the identification and recognition of people by incorporating two kinds of face images that include profile faces as well as data of the ear. Through the combination of these two modalities, this system seeks to improve accuracy. Similarly, utilising side view and auricle photos, Susan EN, Ayman Abaza, and Thirimachos Bourlai investigated human recognition and provided insightful information about the efficacy of several biometric traits [60]. To improve system efficiency, Mostafa Akhaavasaffar, Ali Nakhaei, and Mostafa Mokhtari Ardakan integrated face and ear data and enhanced multimodal biometric authentication [61]. They did this by using a workable Swarm Optimisation method.

Facial identification from profile views, F.J. Chen Jongmoo Choi, Masi, S.H. Jungyeon K.J. Leeksut, S. Rawls, T. Hassner, Yue Wu, W. AbdAlmageed, M.P. Natarajan Ram Nevatia, G. M. Louis Philippe [62]. It prompted serious consideration of the CNN design and demonstrated robustness across many networks. These developments indicate a wider trend of combining multiple biometric modalities and refining algorithms to enhance the accuracy as well as dependability of biometric-based authentication systems. These are essentially the landmarks, six of which are used to extract facial curves from cubic B-splines — crucial turning points. The facial curve divides, resulting in five segments, each of which yields 24 traits that can help recognition. The difficulties of employing side face photos as a biometric identifier are covered in another study. To correctly train the dataset, it highlights how crucial it is to determine the tangential points and precisely calculate the threshold value of images. Clear photos and accurate application of algorithms and techniques are necessary for side-view facial recognition to achieve a low error ratio and high accuracy. By resolving issues and improving side-view facial recognition system performance, this method seeks to provide more dependable and efficient biometric identification. Specifically, the FSLDA method combined with a fused multimodal recognition method based on both the ear and face biometrics provided satisfactory outcomes. When a rank one recognition rate was analyzed utilizing integrated systems, the recall rate of this system, assessed with the USBT and ORL databases for ear and face databases respectively and reached 98.5 percent. Furthermore, a two-model system that used ear and facial profile data performed even better, reaching a 97.98% recognition rate for this test.. This is higher than that of the other published methods in literature such as Principal Component Analysis (PCA)—94.44%, FSLDA—97.62%, and Kernel Fisher Discriminant Analysis (KFDA) —96.84%. This multimodal system has done better performance, by combining more modalities and can be contributed to using well developed and large-sized database that leads to more strengths in the recognition module. This improved performance of combined facial and ear biometrics not only substantiates the integration power of multi-modality but also illustrates the benefit that combining multiple biometric modalities can provide over traditional single-modality approaches.

Pose Normalization: Pose normalization is certainly a hot topic in the community due to its application in solving pose-independent face recognition using both “Generic Elastic Model-GEM” [70] and “Active Appearance-based Models AAM” [71]. These techniques were originally introduced in prior research and are commonly employed as a remedy for the challenges of inconsistencies in facial recognition [72]. This paper describes the GEM framework, a general model approach, and the synthesized pose-induced facial verification. GEM can robustly normalize the face by utilizing changes of both shape and appearance with pose. This process normalizes facial images for straightforward face models, which results in

improved recognition as recognition algorithms work better with regularly shaped front views of individual faces. It has been observed that Active Appearance-based Models (AAM) [71] is a good solution for pose variations. These models encode shape and texture information that is pose-relevant (i.e., clear facial likeness across different poses). AAM maps facial images into a common reference, considering both the shape and texture parameters to support pose-invariant comparison. Improvements in this ability improve the robustness of facial verification systems to many more challenging pose scenarios, albeit only incrementally [71]. GEM and AAM methods have been shown to lead to good pose-invariant face recognition systems [71][72]. Normalizing is an important part of facial recognition and leads to better results which are key research contributions in this field. The continuing evolution of these approaches and the development of new methods serve to greatly enlarge the potential for pose variation they can deal with, which will improve face recognition systems generally. The other issue with GEM and AAM is that while they give good accuracies in easily controlled conditions with a limited variation of the pose, it is highly likely that their performance will degrade significantly under more challenging real-world scenarios i.e. going from aside poses to characteristic facial expression poses.

Researchers are exploring advanced subspace learning techniques for scenarios like those mentioned, focusing on Partial Least Square (PLS) and Canonical Correlation Analysis (CCA). Face bloggers suggest that these methods could enhance the generalization of deep face recognition systems, accommodating a broader range of poses and expressions in natural settings. Consequently, integrating these methodologies will be essential for developing an advanced face recognition system that remains largely invariant to varying conditions when properly trained. Advanced facial pose recognition has been done in the recent past by identification-based methods on multiple and CMU PIE data sets. For instance, a work presented in [75][76] records recognition performance of 27.1% in dealing with frontal profile images over Multiple datasets. These are encouraging findings but no suitable maximum values are given so capacity is not shown in unstructured uses of mobility. More studies have to be conducted to compare their effectiveness in these circumstances.

The field of pose-invariant face recognition has recently shown huge promise within the generative end-to-end approaches. These models posit that a latent factor explains transitioning between different identities and poses. Recent works have shown strong performance at constrained datasets such as [77]; however, these works often do not tackle the intra-dataset. In the same vein, [78] achieved impressive performance on unrestricted datasets as well as LFW with an authentication accuracy of 90.07% under open-set settings. Another way to address pose variation is by using attribute-based recognition as exemplified in [79]. Posture changes tended to be invariant for this

calculation but to what extent features can effectively be computed or if profile faces will provide as much information as frontal ones remains uncertain. Although it is indeed a hard problem, the CFP dataset is used.

J. Bhuvana [123] presents a robust image sensor fusion framework for multimodal biometric recognition, enhancing security and accuracy in mobile devices.

2.3 Outcome Closure

After performing extensive research in biometric identification, a variety of modalities have been examined, including fingerprints, iris scans, voice recognition, and facial recognition. Among these possibilities, facial recognition has surfaced as one of the most predominant and considered biometric techniques. This can be attributed to its non-intrusive characteristics and its broad applicability across multiple industries. Within the region of facial recognition, both frontal face and side face (profile) biometrics have been considered for their respective strengths and weaknesses. While frontal face recognition has traditionally been the dominant approach, side face biometrics offers unique advantages in specific contexts, such as security and surveillance. Side face biometrics, by analyzing a person's profile, proves to be more useful in scenarios where full-frontal visibility may not be available, such as in crowded or real-time surveillance environments. This technique also shows potential in those circumstances where the targeted subject is unaware of being observed, offering a more covert and reliable approach to identity verification. After reviewing the relevant literature, it becomes clear that side face biometrics is a more effective approach in certain practical applications, as it handles pose variations more robustly and provides greater flexibility in real-world conditions.

2.3.1 Accuracy

- **Studies on Accuracy:**
 - Frontal face recognition has been traditionally popular due to its high accuracy in controlled environments. However, side face recognition has shown promising results in recent studies, particularly in diverse and unconstrained settings.
 - Research by Zhang et al. (2023) [66] demonstrated that side face biometrics could achieve accuracy rates comparable to frontal face recognition using advanced deep learning algorithms.
- **Challenges in Frontal Face Recognition:**
 - Frontal face recognition systems' accuracy can be much influenced by changes in occlusions, lighting conditions, and facial expressions.

- Side face recognition systems are less affected by such variations, providing more consistent performance across different conditions.

2.3.2 Security

- **Vulnerability to Spoofing:**
 - Frontal face recognition systems are more susceptible to spoofing attacks using photographs or 3D masks.
 - Due to the difficulty of capturing and duplicating the profile features, Side-face biometrics offers a higher level of security against such attacks.
- **Liveness Detection:**
 - Advanced side face biometric systems incorporate liveness detection techniques that further enhance security by ensuring that the subject is physically present during the authentication process.

2.3.3 Usability

- **User Experience:**
 - Frontal face recognition often requires users to position themselves directly in front of a camera, which can be inconvenient in dynamic environments.
 - Side face recognition allows for more natural interactions, as users can be identified while engaging in regular activities without needing to face the camera directly.
- **Applications in Surveillance:**
 - Side face biometrics are particularly advantageous in surveillance applications where individuals may not always be facing the camera.
 - Studies by Liu et al. (2019) [68] highlight the effectiveness of side face recognition in identifying individuals in public spaces and enhancing security monitoring.

2.3.4 Technological Advancements

- **Deep Learning and AI:**
 - Deep learning and artificial intelligence taken together have substantially improved side face recognition systems' performance.
 - Side-face biometrics have benefited from the use of Generative Adversarial Networks (GANs) and Convolutional Neural Networks (CNNs), hence enhancing feature extraction and matching accuracy.
- **3D Modelling:**
 - Advances in 3-D Modelling and reconstruction have enabled more accurate side-face biometric systems by capturing the depth and contour of the face.

- These technologies provide a richer set of features for identification compared to traditional 2D frontal face images.

Based on the extensive survey of the literature, it is evident that side face biometrics presents several advantages over frontal face recognition. The key points supporting this conclusion are:

- **Higher Accuracy:** Advanced algorithms and 3D Modelling techniques have enhanced the accuracy of side face recognition.
- **Enhanced Security:** Side-face biometrics offer greater resistance to spoofing attacks and incorporate robust liveness detection.
- **Improved Usability:** The natural interaction and convenience of side face recognition make it suitable for dynamic environments and surveillance.
- **Technological Advancements:** Ongoing study and development in AI and deep learning continue to drive improvements in side face biometrics.

2.4 Identified Research Gaps

- **Limited Exploration of Frontal-Only Face Data:** Most hybrid systems include full facial pose variation, but few studies focus on optimising performance when only frontal face images are available.
- **Understudied Impact of Missing Side Face Data:** There's little analysis of how excluding side face views affects the accuracy and robustness of hybrid biometric recognition systems.
- **Lack of Modality Compensation Strategies:** Few approaches explore how to compensate for the absence of side face images using other biometric modalities (e.g., gait, voice, or ear).
- **Insufficient Dataset Diversity:** Publicly available biometric datasets often include side-face views. There is a gap in curated datasets that simulate real-world conditions with restricted pose availability.
- **Fusion Techniques Not Optimized for Missing Modalities:** Existing fusion algorithms often assume all modalities (including side face) are available. There is a need for adaptive or flexible fusion methods that perform well when side-face data is not provided.

2.5 Conclusion

The convergence of multiple factors strongly indicates that side-face biometrics offers a more secure, accurate, and user-friendly solution for biometric identification. As technology continues to advance, this method is becoming an increasingly viable option, especially in scenarios where traditional front-facing biometric systems encounter limitations. A drawback of such a deployment of side-face biometrics is its reliance on an unconstrained environment and the availability of frontal images for processing. In many practical situations for example in surveillance, public security, or in times when granting access to some facilities and premises, side-face is more convenient than frontal one. Side-face recognition is therefore most useful in situations where people might not be facing cameras straight or if light conditions and angles are changing. Moreover, new machine-learning methods and deep-learning procedures have enhanced the side-face biometric performance. Using deeper architectures—especially Convolutional Neural Networks (CNNs) and related systems—allows different approaches to extract more unique feature sets from profile images, rather than only from the frontal face, so improving accuracy in identification and verification relative to frontal-based models. Different from more traditional methods like iris or fingerprint scans, side-face biometrics offers a non-intrusive and user-friendly identifying solution. Unlike these methods, which demand close physical contact or direct interaction with scanning devices, side-face recognition can be seamlessly integrated into public settings. This technology allows identification to occur during routine activities without requiring individuals to stop, pose, or alter their behaviour, making it a more practical and accessible solution. Its convenience is particularly valuable in high-traffic areas such as airports, transportation hubs, and large public events, where both security and user experience are critical. By eliminating the need for active participation from users, side-face biometrics enhances the flow of people in these environments, reducing delays while maintaining robust security protocols. Another significant advantage of side-face biometrics is its adaptability in more challenging scenarios. This technology can successfully identify individuals in complex environments, such as crowded spaces or from video footage, where other methods might struggle. Its effectiveness in these contexts broadens its application, making it suitable for monitoring large areas without compromising accuracy. In scenarios requiring the rapid and efficient processing of large crowds, side-face recognition emerges as a highly scalable approach. Moreover, the capacity to acquire biometric data from many perspectives guarantees the reliability of identification systems, even in the absence of full-frontal photographs. Side-face biometrics provide a substantial improvement in security and ease, rendering it an optimal option for extensive use.

As the biometrics sector develops, side-face recognition should find great application in many other sectors. Improved security solutions presented by side-face biometrics will benefit industries including banking, financial services, law enforcement, and border control. Artificial intelligence and big data analytics inclusion in these systems is supposed to improve side-face recognition algorithm efficiency and accuracy. These improvements will enable side-face biometrics to take front stage in next-generation security systems as a reasonably affordable, contactless alternative to conventional approaches. With the convergence of technical advancements, useful applications, and improved user experience, side-face biometrics is poised to become a main feature of biometric identity.

Chapter 3

3. Inspiration and Driving Forces Behind the Study

Here, the study's general procedures and methodology have been outlined and put into practice, with an emphasis on analysing machine learning and deep learning-based data extraction methodologies. Human face detection, feature extraction, and then face recognition are the three core and vigilant mechanisms of the task of human face identification. Basic procedures include face detection, in which an algorithm determines whether a face is present in a picture and, if so, draws a box around it. The algorithm recognizes a face in the first stage of detection and pinpoints particular elements of the face, such as the shape of your nose or the separation between your eyes, in the second stage of feature extraction. Each of these components is necessary for a face recognition system to function successfully and efficiently overall. Face extraction refines the traits that distinguish each face, while face detection lets the algorithm focus solely on particular regions of interest in an image. Ultimately, this data is used by recognition algorithms to precisely match subjects, ensuring the effectiveness of individual identification.

The upcoming sections will provide a summary of each of these components, detailing their roles in the system and how they work together to achieve robust side face recognition. Additionally, this study will explore the specific machine learning and deep learning techniques applied to profile pictures, as well as the challenges and strategies involved in adapting these algorithms for side-face recognition. This examination sets the stage for a deeper analysis of the algorithms' performance and the impact they have on the system's overall efficiency and reliability.

3.1 Detecting Face

Face detection is the first stage in face recognition and is the most crucial stage in the face identification process. To recognize faces and facial landmarks it is necessary to detect the locations and sizes of faces inside a digital image while ignoring other objects. This is done during the recognition of faces during the face recognition process to be more precise. In this chapter, some of the common methods have been described which are used for detecting and recognizing the face.

3.1.1 HCA- The Haar-Cascade

In computer vision, this algorithm is a common method for detecting the face, particularly in real-time applications. This approach, which originated in a ground-breaking 2001 study by Paul Viola and Michael Jones [94], is based on machine learning. The Haar Cascade algorithm, a cornerstone in face detection, uses simple rectangular patterns known as Haar-like features, which are effective in identifying edges, lines, and fundamental shapes within an image. These features help distinguish between different parts of a face, such as the eyes, nose, and mouth, by capturing contrasts in pixel intensities. The Haar-like features, inspired by human visual processing, are key in recognizing the structure of a face. During the training phase, the algorithm is fed thousands of positive (faces) and negative (non-faces) images, allowing it to learn how to differentiate between faces and other objects. Through this process, several classifiers are generated, each designed to detect specific features of the face, ensuring that the algorithm can accurately distinguish facial regions from the background. The algorithm works by scanning an image with multiple scales and allows it to identify the faces of various dimensions. This multi-scale scanning is crucial because faces can appear in different proportions depending on their distance from the camera. By applying the Haar-like features across these varying scales, the algorithm ensures that even small or distant faces can be identified. Haar Cascade's [94] cascading structure significantly enhances its performance. Instead of processing every region of the image in detail, it quickly eliminates areas where no face is detected in the initial stages. This step-by-step approach, where non-face regions are filtered out early, allows the algorithm to focus its computational resources on promising regions, thereby increasing both speed and efficiency. Moreover, the Haar Cascade classifier operates by using a series of weak classifiers in a cascade. Each weak classifier evaluates a small region of the image for the presence of certain features. If a region passes through all stages of the cascade without being rejected, it is identified as a face. This cascading method ensures that the algorithm minimizes false positives, as each subsequent stage of the cascade applies increasingly complex criteria to verify the presence of a face. The high speed and precise outcomes make this method appropriate to be implemented for real-time face detection systems. Figure 3.1 overviews the Haar Cascade classifier with an emphasis on the process of the algorithm to detect faces in an image. Due to its capability to perform feature extraction in a simple manner and fast scanning and classification, Haar Cascade has received considerable attention in different face detection applications, particularly, in environments with constrained computational resources. Despite its relatively older design compared to modern deep learning methods, Haar Cascade remains a powerful tool for quick and effective face detection, especially when integrated with other machine learning techniques.

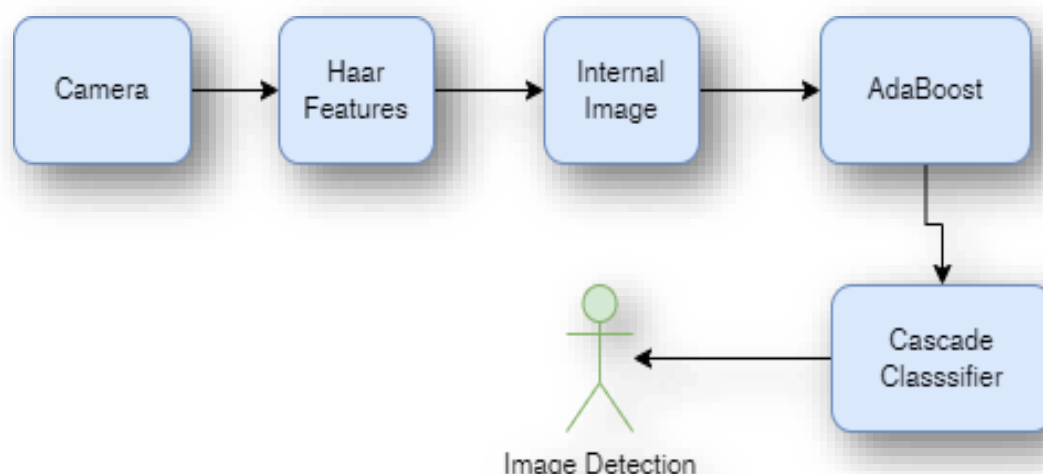


Figure 3.1 Haar Cascade Classifier Workflow [94]

This algorithm has mainly three main phases:

- **Selection of Haar Features**

The first stage of the Haar Cascade algorithm, known as Haar Feature Selection, focuses on identifying the most effective features for face detection. Haar features are rectangular regions within an image that evaluate the contrast between different parts of the image, helping the algorithm detect patterns indicative of a human face. These features play a crucial role in distinguishing facial regions from other parts of the image. The algorithm analyses variations in pixel intensity across these rectangular regions, effectively capturing the visual characteristics of faces, such as edges and lines. Several types of Haar-like features are used in this process, each designed to detect different elements of a face. Edge features are one of the simplest types and are used to identify transitions between light and dark areas, such as the boundary between the forehead and eyes. These features help the algorithm recognize where sharp changes in pixel intensity occur, which is typical around facial landmarks like the eyes, mouth, and nose. Line features are more sophisticated, detecting linear patterns that might represent parts of the face like the bridge of the nose or the alignment of the eyes. These features allow the algorithm to recognize horizontal or vertical lines that are often present in a face's structure. In addition to edge and line features, the algorithm also uses four-rectangle features, which are more complex and capable of identifying patterns that involve larger regions of contrast. For instance, these features can detect the arrangement of eyes and nose or the space between the mouth and chin. By capturing these more intricate structures, four-rectangle features help the algorithm understand the overall layout and composition of a face, enabling it to distinguish between faces and non-face objects more effectively. The combination of these features forms the

foundation of the face detection process. Each feature contributes to the overall classification by highlighting specific patterns that are common in faces but not in other parts of an image. By selecting and applying the most effective features, the algorithm can quickly filter through irrelevant areas of an image and focus on regions that are likely to contain faces. This process of feature selection ensures that the algorithm operates efficiently, even when dealing with large or complex images. Ultimately, Haar Feature Selection is critical to the success of the entire detection system. It enables the algorithm to identify the most important visual cues for face detection, ensuring high accuracy while minimizing computational complexity. The ability to detect faces based on simple yet powerful features like edges, lines, and more complex structures makes Haar Cascade a widely used method in computer vision, particularly for real-time applications where speed and efficiency are paramount. Figure 3.2 illustrates Haar-like features.

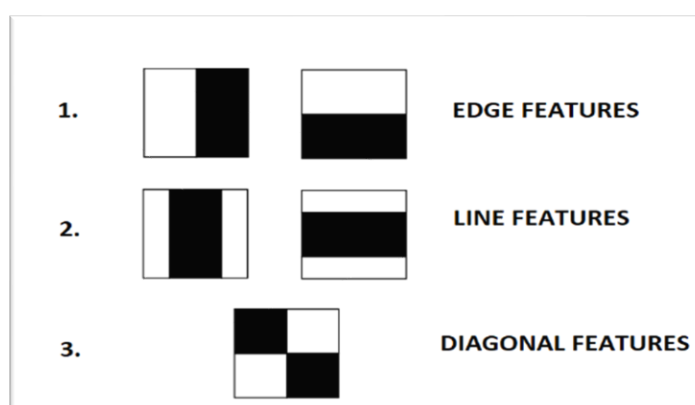


Figure 3.2 Haar Features [94]

- **Image Scheming**

In the next stage, the number integral of the given input image needs to be taken. The picture is a matrix composed of two dimensions that give the sum of all of the pixels up to the current point. It may be efficiently computed using dynamic programming. The integral picture allows for the computation of sums in a fixed amount of time, eliminating the need to add up the pixel intensities for every feature separately. Figure 3.3 [95] shows an example of how this strategy improves computational efficiency,

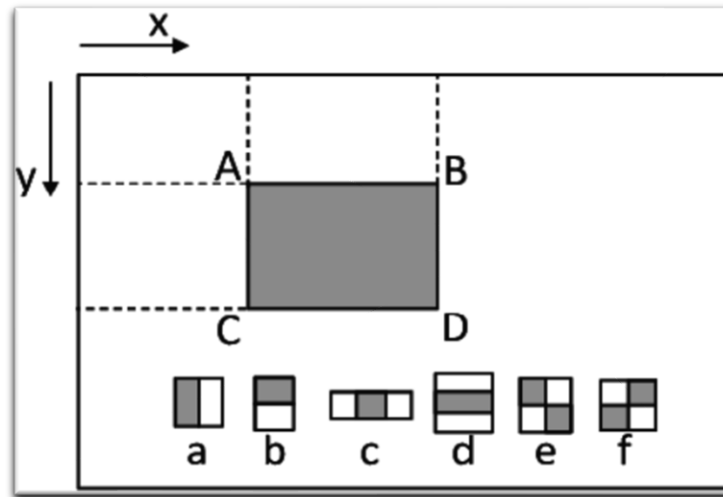


Figure 3.3 Image calculation using Haar [94]

- **Implementation of Classifier**

A cascade classifier is a combination of multiple classifiers where each of them reduces the chance of malfunctioning by focusing only on face area. The cascade consists of several stages of classifiers: each of them filters out low-quality and simple images, and lets through good candidate faces with just a few calculations. It operates in several layers, in each of which it looks at different zones of an image using a set of “Haar-like features” unique to the layer [43]. Finally, at each step, the classifier uses the integral picture to sum a feature vector across all regions of the image. If the feature vector matches the face, the region advances to the next stage in the cascade. If it does, the region will be rejected as nonface. This multi-stage strategy brings further improvement to detection performance in specific aspects such as accuracy and efficiency. Training the cascade classifier requires a lot of such positive and negative examples, making it more accurate and suitable for different scenarios. Furthermore, its excellent generalizability allows faces to be detected in various lighting conditions, from different directions, and across expressions, making it more multipurpose and stronger.

3.2 Deep Learning Techniques for Side Face Recognition

Deep learning has changed the facial recognition industry, instantly recognising and extracting complicated image information. Its ability to detect intricate patterns has greatly improved accuracy and reliability. For side face identification, deep learning methods are adjusted to handle the challenges of side profiles. CNNs are optimized to capture unique side-face features, and transfer learning improves performance by using pre-trained models with limited data. Generative Adversarial Networks (GANs) [116] further bolster training by generating realistic side-face images.

These advancements collectively enhance side face recognition systems, making them more effective at handling variations and occlusions in side profile images.

3.2.1 Convolutional Neural Networks-CNNs

Deep learning has changed the facial recognition industry, instantly recognising and extracting complicated image information. Nonlinear activation functions like ReLU add complexity, allowing the network to learn intricate patterns. CNNs excel at automatically detecting spatial hierarchies in images, making them well-suited for large-scale image data where traditional methods might struggle. Despite their power, CNNs can overfit, especially with complex models or small datasets. Overfitting happens when the CNN memorizes the training data rather than learning to generalize, leading to high training accuracy but poor performance on new data. To prevent overfitting, techniques like dropout, data augmentation, and regularization are used.

Conversely, underfitting results from a CNN failing to detect relational patterns in the training data set, much alone the test data, hence producing a rather poor, extremely accurate forecast of the training data set. This is mostly contributed to by overly simplistic or inadequately trained models of the data set under consideration. Sometimes it's challenging to determine what level of model complexity is feasible so that the CNN can be effectively trained by using the available amount of training data and employing the most optimal optimization techniques. To teach CNNs to map selection to a label as in "cat" or "dog", labelled data is usually provided. It is then readjusted to serve as determinants used by the network to reduce the prediction errors. CNNs, according to the literature, have provided better solutions as compared to traditional methods in these areas and provide state-of-the-art accuracy and complexity. Through the optimization and mitigation of the limitations characteristic of CNNs, research authors and developers are increasingly unlocking the potential of image-based AI systems. The core layers of a CNN consist of Convolutional layers, Pooling layers, ReLU activation layers, and Fully Connected layers, as shown in Figure 3.8. These layers work together to extract features, reduce dimensionality, and classify data in deep learning models.

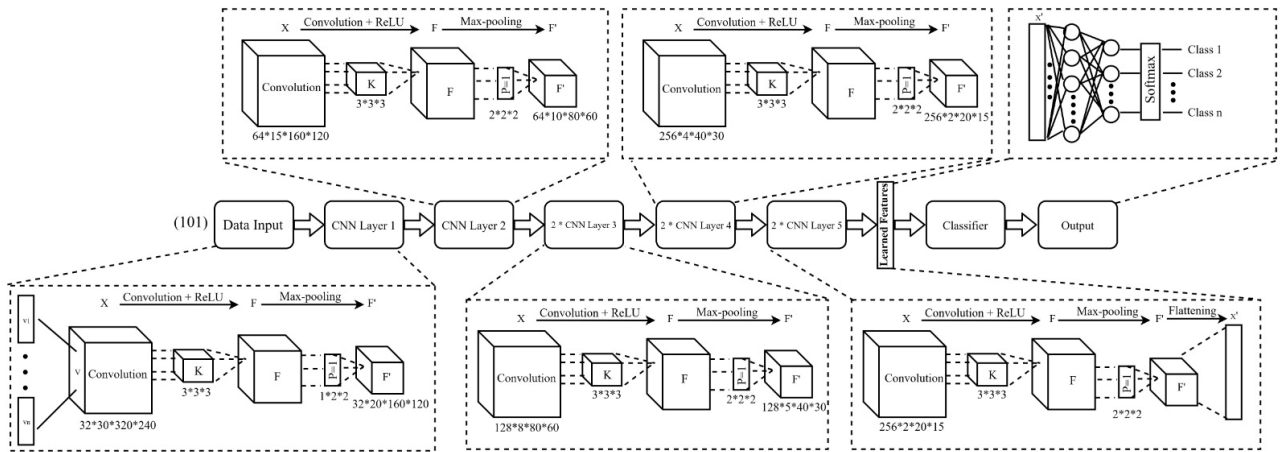


Figure 3.4 CNN Architecture [129]

- **Convolutional Layer:** The majority of computing is carried out by the convolutional layer, which is the core element of a convolutional network. Extracting features from the input data—typically an image—is its main goal. The convolutional layer maintains the spatial relationships between pixels while learning visual features from small input image patches. The image is processed through many learnable filters or kernels, yielding an activation map or feature map as output. The feature map is then supplied as input to the successive levels of the network [106].
- **Pooling Layers:** The pooling layer in CNNs reduces the image size by down-sampling, usually after a convolutional layer. Max pooling, a common method, picks the highest value from each region in the feature map, which helps improve the model's generalization, speed, and resistance to changes in position and distortion.
- **ReLU Layer:** The Rectified Linear Unit layer presents non-linearity into the network through its rectifier function. It operates element-wise on the feature map, replacing all negative values with zero. Mathematically, if 'INR' represents the input to the neuron, the ReLU function is defined as

$$f(\text{INR}) = \max(0, \text{INR}) \quad (3.3)$$

This non-linear transformation supports the network to learn more complex patterns and representations.

- **FCL- Fully Connected Layer:** The FCL has neurons where every neuron is linked to each neuron of the layer next to it. It has a convolutional layer, pool layer, and ReLU in contribution to offering high-level features that exhaustively go through categorization of the image input regarding several training data types. A classifier uses the FCL's output to assign probabilities

to each class, often with the SoftMax function. SoftMax provides a probability distribution where all output probabilities add up to 1. To maximize performance during training, the network reduces the cross-entropy loss between the true labels and the predicted prospects [105].

CNNs are the backbone of most modern facial recognition systems. They are particularly effective in handling spatial hierarchies in images [117]. Key architectures used in side face recognition include:

- **VGGNet:** Known for its simplicity and depth, VGGNet has been employed for side face recognition with modified layers to handle side profiles.
- **ResNet:** The residual learning framework of ResNet helps in training deeper networks, which can capture more intricate features of side faces.

3.2.2 Transfer Learning

Given the shortage of side-face data, transfer learning is a valuable technique. To enhance performance, pre-trained models using smaller side-face datasets (like ImageNet) might be adjusted.

- **Fine-tuning:** Regulating the weights of a pre-trained model to better suit the side face recognition task.
- **Feature Extraction:** Using the convolutional base of a pre-trained model to extract features and train a new classifier on top.

3.2.3 MTCNN: Multi-Task Cascaded Convolutional Neural Networks

Applications like as face identification, expression analysis, and virtual try-on systems require facial landmark detection, which focuses on recognizing important facial landmarks like the mouth, nose, and eyes. The well-known deep-learning framework MTCNN was first presented by Zhang et al. in 2016 [97]. It is utilized for both face detection and landmark identification. Three neural networks are used by MTCNN: the Output Network (O-Net) to complete landmark predictions, the Proposal Network (P-Net) to produce candidate facial regions, and the Refine Network (R-Net) to improve these candidates. The following describes each network's distinct function in the face detection process:

- **P-Net:** Using a fully convolutional neural network, the P-Net i.e. Proposal Network generates potential face regions by scanning the entire image to create bounding boxes of various proportions and aspect ratios.
- **R-Net:** The second network in the MTCNN cascade, called the R-Net (refine network), improves the bounding boxes generated by the P-Net. It filters out false positives,

enhancing the accuracy of face detection by concentrating on facial areas and minimizing background interference.

- **O-Net:** The O-Net, or Output Network, is the final stage in the MTCNN cascade. It further refines the bounding boxes from the R-Net, classifies regions as face or non-face, and accurately identifies facial landmarks such as the eyes, nose, and mouth for precise localization.

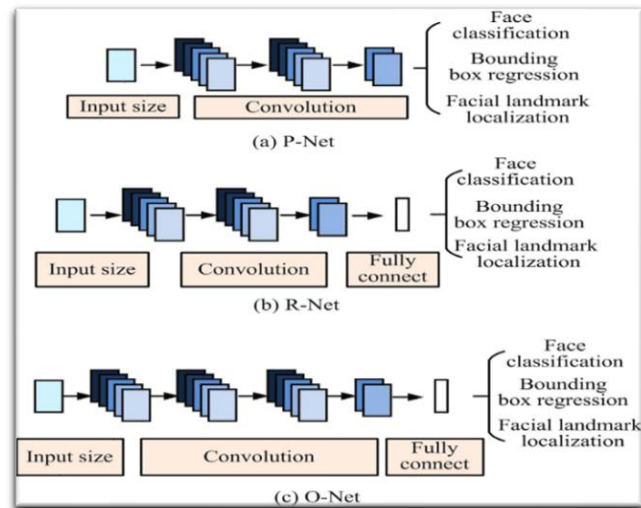


Figure 3.5 MTCNN model [98]

Face categorization, bounding box regression, and facial landmark localization are the three main functions carried out by MTCNN. To get the desired effects, each stage uses a different combination of convolution filter widths and layer depths. Three groups of outputs are obtained: two neurons identify the face and provide the categorization score. Another output utilizes four neurons to identify the upper left and bottom right corners through bounding box regression. This output also handles facial landmarks by detecting five key points: the nose, mouth corners, and the left and right eyes.

3.3 Feature Extraction Methods

Significant local intensity fluctuations, such as those found at corners and edges, are featured in photographs. Applications including object detection, face recognition, and picture segmentation use feature descriptor techniques like edge detection. Facial features that are important for face identification include the nose and eyes. By obtaining important data, feature extraction aids in the classifier's ability to differentiate between individuals. Since features include domain-specific information that is difficult to learn from sparse data, they are employed instead of raw pixels.

Following is a quick description of a few feature extraction methods that were used on the dataset photos in this section.

3.3.1 LBP - The Local Binary Pattern

The LBP method is a straightforward yet effective technique for describing local texture in images. It compares each pixel with its neighboring pixels, creating a binary pattern based on whether neighboring pixels are brighter or darker than the central pixel. In facial recognition, LBP creates a feature vector for the overall descriptor by dividing the image into areas, extracting features from each, and combining them. The LBP operator generates a binary code by examining a 3×3 neighborhood around each pixel, capturing texture details as a compact and informative descriptor [99].

In other words, LBP can be labeled as an well-ordered sequence of binary values relative to the initial arrangement of the intensity value of the surrounding pixels compared with that of the center pixel of that location(x,y). Equation 3.1 [100], [101] thus provides the final decimal value produced from the 8-bit binary pattern itself.

$$\text{LBP}(a,b) = \sum_{n=0}^7 2^n \cdot S(L_n(a,b) - L_c(a,b)) \quad (3.1)$$

The gray values of the eight adjacent pixels are shown by L_n , the gray value of the center pixel (a, b), along x and y axis respectively, is represented by L_c , and the function $S(j)$ is given as:

$$S(j) = \begin{cases} 0, & x < 0 \\ 1, & x \geq 0 \end{cases} \quad (3.2)$$

The LBP operator processes a pixel's eight neighbors, using the central pixel as a threshold [102]. The surrounding pixel receives a zero if its gray value is not equal to or greater than the value of the center pixel, and a one if it is. The LBP code is subsequently created by combining these eight binary values for the central pixel, described as in Figure 3.5.

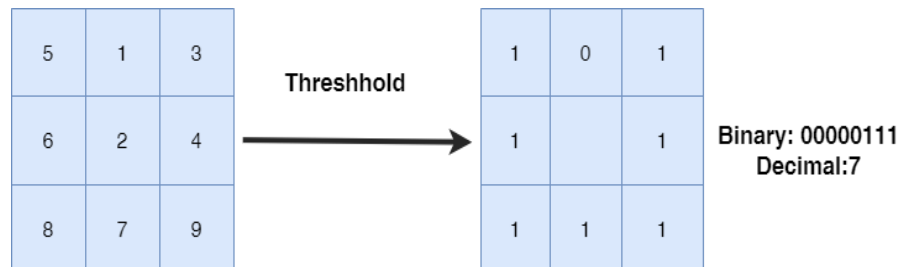


Figure 3.6 The operators of LBP [101]

3.3.2 HOG – Histogram of Oriented Gradient

In image processing, HOG (Histogram of Oriented Gradients) is a commonly used feature extraction technique, especially for object detection and recognition. The foremost goal of HOG is to use gradient orientation distribution analysis to identify and characterize the local structure and shape of a picture. Gradients, which are variations in intensity values throughout an image, give important details about object boundaries and edges. Following are the steps involved in this technique

- **Gradient Computation:** To assess changes in intensity in both the horizontal and vertical directions, gradients are first created for discretely pixel. This aids in locating the image's borders and edges.
- **Cell Division:** The image is separated into tiny, usually 8 by 8-pixel cells. The distribution of gradients within each cell is represented by a computed gradient orientation histogram.
- **Block Normalization:** To account for variations in lighting and contrast, cells are grouped into larger blocks (e.g., 2x2 cells) and normalized, enhancing the robustness of the feature descriptors.
- **Histogram Accumulation:** The normalized histograms from the cells within a block are concatenated to form a block descriptor. This descriptor represents the shape and structure of the image within that block.
- **Feature Vector Formation:** The descriptors from all blocks in the image are concatenated into a final feature vector, capturing the overall gradient orientation distribution across the entire image.

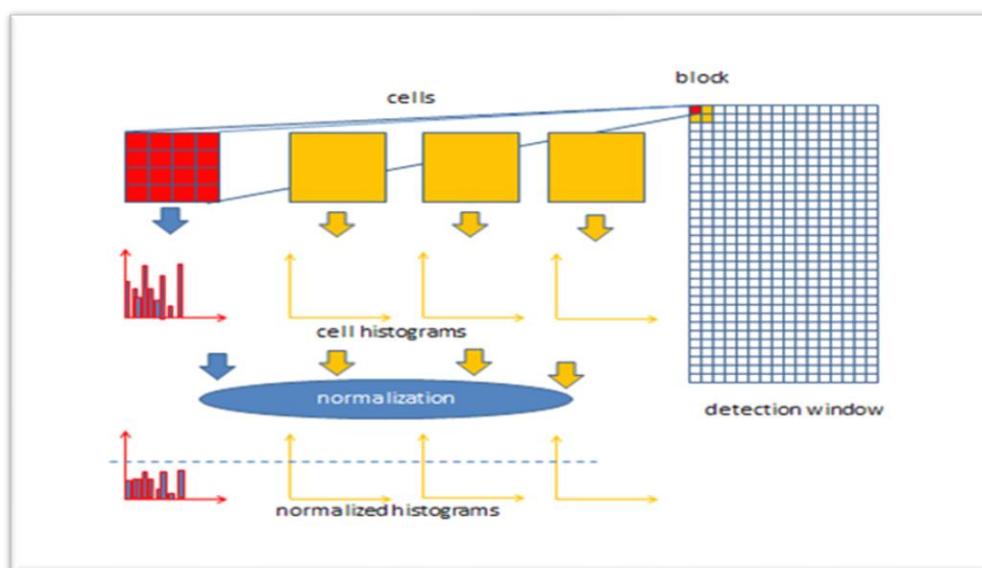


Figure 3.7 Architect of HOG [103]

3.3.3 PCA- Principal Component Analysis

PCA is a popular statistical approach for data dimensionality reduction, feature extraction, and information compression which is also widely used in face recognition systems. PCA is to acquire a linear transformation that maps the high dimensional data into a space where the data have fewer dimensions which contains nearly as much variance as those of a complete n dimension [104]. This gave the best generalized facial features required for proper identification. The transformation works by separating the directions which have the most variance where the new dataset is expressed and information is retained in ways other than simply throwing away some of your input data. At its core, PCA is about capturing the essence of face images and removing irrelevant or redundant information. PCA decreases the number of computations needed and seeks to identify in image, areas that have a huge impact on face recognition. PCA is majorly used to reduce a large set of data into a smaller set making it easier and accurate for the machine learning models to work with faces. However, it adds to cognition time and in doing so enhances the face recognition systems' performance significantly. By concentrating on the most critical facial characteristics, PCA ensures that the system can identify or verify individuals with greater precision, even when faced with large datasets or varying conditions, such as lighting or orientation. Thus, PCA is a powerful tool in the field of biometric identification, enabling efficient and accurate facial recognition.

Here are some explanations for why PCA is especially well-suited for face recognition:

- **Dimensionality Reduction:** PCA reduces the number of dimensions in facial image data while retaining the most important features. This simplifies the data and speeds up the recognition process.
- **Variance Preservation:** PCA projects data onto a lower-dimensional space in such a way that the variance is maximally preserved. This ensures that the key features of the facial images are maintained, which is crucial for accurate recognition.
- **Feature Extraction:** By identifying principal components, PCA extracts features that are most effective in distinguishing between different faces. These features, or eigenfaces, are critical for accurate face recognition.
- **Noise Reduction:** PCA reduces noise by concentrating on the main components that capture the furthestmost important distinctions in the data, making face recognition more robust to changes and distortions.
- **Computational Efficiency:** PCA reduces the amount of data to process, making face recognition faster and more efficient.

- **Linear Transformation:** PCA provides a linear approach to feature extraction, which is effective for capturing the linear relationships between facial features and recognition performance.
- **Data Compression:** PCA compresses data by transforming it into a lower-dimensional space, making it easier to store and manage large datasets of facial images.
- **Generalization:** By focusing on principal components, PCA helps in generalizing facial features across different individuals, improving the model's ability to recognize faces under varying conditions.

In conclusion, PCA worth or can provide much useful information for human face recognition. This technique gives pretty good result and also the variance in original data is going to be retained after transforming it into a lower dimension space. This procedure keeps the data simple enough to handle, making processing time reduced significantly. PCA effectively simplifies useful information that face recognition systems require to build and is also often necessary in a real-time application so that these subsystems can operate more practically. PCA is the one that works best for the greatest number of idioms and many difficulties others have with understanding working on our target features from our multi-valued data. Most of all, PCA has been utilized for the purpose of feature extraction, which improves the recognition system efficiency and performance. Dimension reduction of the data you have makes the calculations faster and has its advantages in i.e. the possibility of overfitting because of lots of noise or irrelevant data driven to the AI system.

. PCA, for instance, has done an especially good job in side-face biometrics due to its capacity to capture necessary craniofacial structures which enhance recognition capabilities. This accuracy is important in cases where the profile view can be our only point of recognition. PCA reduces the dimensionality of a dataset while maintaining important features, making the data set more tractable for further analysis.

This method provides a good functional way of making the side-face identification fast and reliable through PCA. This guarantees that crucial characteristics of facial geometry remain intact so that such systems can reliably solve problems even under significantly different conditions (due to altered lighting or pose). In addition, the data becomes less complex which means faster processing times, allowing for rapid detection and confirmation in real-world applications. To conclude PCA is significantly important in making face recognition systems better. This is the reason why it allows for simpler data to still hold enough pivotal value to work effectively and earn efficiency in biometric systems. This makes PCA a cornerstone modelling approach for the recognition of individuals by their faces in most versions of evolving face recognition technology. The utilization of PCA in

biometric systems leads to technological advancements as well as allows user-centric applications that are capable of operating in real-world scenarios. So, PCA emerges as the king in the Face Recognition field and there is no development to be made in biometric identification without it.

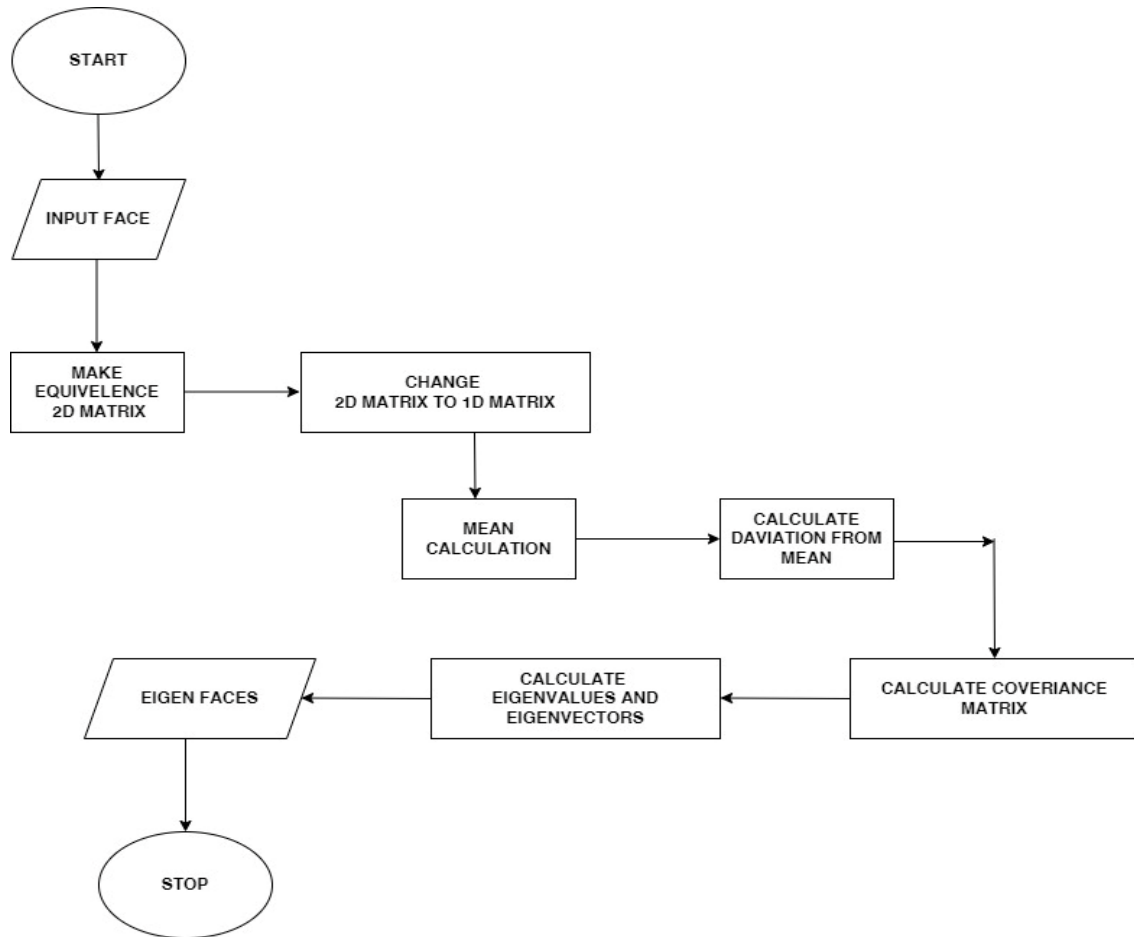


Figure 3.8 PCA-Flow chart [104]

3.4 Face Recognition Techniques

Face recognition techniques can be categorized into several different methods based on the underlying approach. Here are some of the most common techniques:

1. Traditional (Hand-Crafted Feature) Methods:

- **Eigenfaces “Principal Component Analysis – PCA”:** This is one of the first facial recognition techniques developed. Faces are represented as the weighted sum of the so-called “eigenfaces”.
- **Linear Discriminant Analysis – LDA:** LDA improves classification by identifying a linear combination of features that maximizes separation between classes while minimizing variation within each class.

- **Local Binary Patterns (LBP):** This technique uses texture features by converting an image into an array of binary patterns, which are then used for face classification.
- **Gabor Filters:** Gabor wavelets capture orientation and spatial frequency characteristics of face images, which are then used for recognition.

2. Statistical Methods:

- **Hidden Markov Models (HMM):** This statistical model assumes that the underlying process generating face data is a Markov process, which is often used for face recognition in dynamic systems such as videos.
- **Support Vector Machines (SVM):** SVM is used to classify faces by finding the best edge that maximizes the separation between diverse classes in a high-dimensional space.

3. Neural Network-Based Methods:

- **Convolutional Neural Networks:** CNNs are popular for face recognition because they automatically learn features from data. Deep learning methods usually perform much better than traditional ones.
- **VGGFace:** A CNN architecture fine-tuned on a large face dataset to perform face recognition.
- **FaceNet:** Developed by Google, this deep learning model uses a triplet loss function to map faces into an Euclidean space, where distances directly correspond to face similarity.
- **DeepFace:** Developed by Facebook, DeepFace uses a deep neural network to detect and verify faces.

4. 3D Face Recognition:

- **3D Morphable Models (3DMM):** This technique uses 3D shape information of the face, providing robustness against pose and lighting variations. The model creates a 3D representation of the face that can be compared across different viewpoints.
- **Depth-based Face Recognition:** It uses depth information along with RGB data to perform face recognition, which improves performance in challenging conditions.

5. Hybrid Methods:

- **Pose-Invariant Face Recognition:** This combines 2D and 3D models to handle variations in pose. Hybrid methods might also combine deep learning techniques with traditional feature-based techniques for better performance.
- **Holistic Methods:** These methods recognise the full facial image by combining several features and approaches, such as merging texture-based algorithms with deep learning.

6. **Attention Mechanisms and Transformer Models:**

- The attention and transformer models which are found in the recent advancements in natural language processing and computer vision are also being applied in face recognition for better accuracy and understanding with the help of the attention mechanism.

7. **Facial Landmarking and Geometric Methods:**

- **Active Appearance Models (AAM):** In this method, facial recognition is done by applying a deformable model to the face considering both the shape and texture of the face.
- **Facial Landmarks Detection:** landmarks of interest/ the face with e.g. the eyes, nose, and mouth and using the relative geometrical information between these landmarks for recognition.

8. **Thermal Imaging-based Recognition:**

- This technique leverages the thermal signature of a face, which is invariant to lighting circumstances and can be useful in low-visibility environments.

9. **Motion-Based Recognition (Video Analysis):**

- **Optical Flow-Based Recognition:** In video sequences, the motion information (optical flow) of facial features can be used for recognition.

10. **Hybrid Deep Learning Methods (GAN-based, Siamese Networks):**

- **Generative Adversarial Networks (GANs):** GANs can generate realistic facial images that can be used to supplement the data or assist in face recognition by creating face embeddings.
- **Siamese Networks:** These networks are designed to compare two input images and learn a similarity function to recognize whether the two images represent the same person.

Although this thesis does not aim to provide an exhaustive explanation of all face recognition techniques, it concentrates on a hybrid approach combining Principal Component Analysis (PCA) with Convolutional Neural Networks (CNN). The rationale behind this choice is rooted in the complementary strengths of these two methods. PCA is a well-established method for dimensionality reduction, particularly effective in simplifying the computational complexity of large datasets by projecting high-dimensional data onto a lower-dimensional subspace. This reduction not only accelerates the recognition process but also preserves the essential variance necessary for distinguishing different faces. CNNs excel at capturing complex patterns, such as facial features, and can robustly handle variations in lighting, pose, and expression.

By integrating PCA with CNNs, this hybrid approach seeks to balance the benefits of reduced computational cost with the accuracy and robustness of deep learning models. The forthcoming

technical review will examine the empirical evidence supporting this approach, emphasizing its use and efficiency in real-world face recognition applications. This evidence will justify adopting this method as a viable solution for modern face recognition tasks.

3.5 MLP- Multi-Layer Perceptron

The Multi-Layer Perceptron (MLP) is a neural network that processes data by going through layers of connected nodes consisting of an input layer, the input data feature, some hidden layers, and an output layer. It uses activation functions like sigmoid or ReLU to learn complex patterns from data. Figure 3.9 [107] shows an MLP archetypal with one hidden layer.

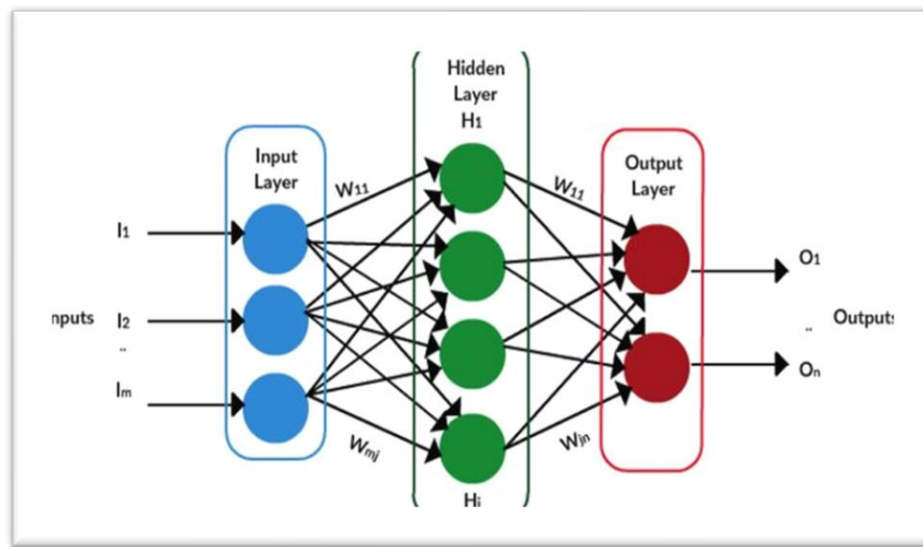


Figure 3.9 MLP Model - where “m inputs, 1 hidden layer, and n” outputs [107]

A Multi-Layer Perceptron's (MLP) outputs are computed as :

1. Primary, Equation 3.4 is used to find the weighted sums of the input values.

$$t_j = \sum_{i=1}^n (W_{i,j}x_i) - B_j \quad j = 1, 2, \dots, h \quad (3.4)$$

Here

- n=number of inputs
- $W_{i,j}$ = Weight from the j^{th} neuron to the i^{th} neuron in the input layer (x_i)
- $x_i = i^{\text{th}}$ input
- B_j =Bias for the j^{th} hidden node

2. In the next step, each neuron in the hidden layer calculates its output using an activation function, as shown in Equation 3.5.

$$T_j = \text{sigmoid}(t_j) = \frac{1}{(1 + \exp(-t_j))} \quad j = 1, 2, \dots, h \quad (3.5)$$

3. Equations 3.6 and 3.7 below explain how the outputs of the hidden nodes determine the network's final output.

$$o_k = \sum_{j=1}^h (W_{j,k}, T_j) - B'_k \quad k = 1, 2, \dots, m \quad (3.6)$$

$$O_k = \text{sigmoid}(o_k) = \frac{1}{(1 + \exp(-o_k))} \quad k = 1, 2, \dots, m \quad (3.7)$$

Here

$W_{j,k}$ = correlation weight between the j^{th} hidden neuron and the k^{th} output neuron

B'_k = bias of k^{th} hidden neuron [107]

In summary, a Multi-Layer Perceptron (MLP) learns complex functions by processing data through multiple layers of neurons with non-linear activation functions. The network's performance is enhanced by adjusting weights through supervised learning and optimization techniques while carefully selecting hyperparameters.

In side face recognition, MLPs help process features from side profiles, learning to identify subtle patterns despite variations in angles. Training the MLP on these features improves its ability to recognize individuals from side profiles.

3.6 Conclusion

Moreover, this work proposes side-face biometrics beyond the approaches related to front-face solutions that can be considered as a significant contribution to solving the facial identification tasks using PCA and CNN. PCA is ideal not only for data dimensionality reduction but also for extracting essential characteristics of faces, helping reduce complexity while understanding all the aspects of large datasets. Secondly, when combined with the strengths of CNNs in grasping fine details on images, this hybrid model can form a potent machine for side face identification. Although now there is a great deal of research on front-face biometrics and it has long been applied in practice, the experimental results demonstrate that PCA integrated with CNN to the side-face recognition secures excellent results, enabling the system to identify an individual looking from other angles.

This is an important advance in the biometric system for dealing with more robust and versatile sensors that do not always present a frontal view of the enrolled subjects, as it happens in real-world scenarios. The results showcase the applicability of these methods in different scenarios including security systems, and adequacy access control where authentication is very crucial. In this work, the efficiency of this strategy was also proved through experimentation at a great level in the “**FEI-Faculdade de Engenharia Industrial**” (Industrial Engineering College) database.

The results of the experiments showed high accuracy, showing that the PCA-CNN hybrid model can be a good solution for side-face biometrics. The results validate the conceptual feasibility of combining PCA and CNN but also pave the way for future use cases in facial recognition technologies. The next chapter presents the illustrative experimental results and comprehensive methodologies of these virtually implemented experiments for PCA and CNN that provide a great access point on how PCA and CNN can transform biometric identification. The groundwork laid by this research is a stepping stone toward future work on facial recognition, highlighting the necessity of transforming such preservation technologies to suit broad identification contexts.

Chapter 4

4. Proposed System

In the previous chapter, considerable groundwork was made to successfully cover the thorough analysis of technologies relating to side-face biometrics. From the detailed reviews of various studies, it became clear which of the methods were the most useful in developing a new side-face recognition system. This section details the dossier and methods employed. The proposed methods have been tested on publicly available datasets of side faces from FEI cubed with a discrete number of images of different sides. This dataset is critical as it is used for the development and optimization of the system. Various techniques and algorithms are applied to the system to improve its accuracy and performance. A steady improvement has taken place in pre-processing that helps to enhance the quality of the image, the feature extraction phase that assisted with characterizing unique facial features, and the classification algorithm that allowed the system to perform an accurate identification. Here, the goal is to focus on achieving the highest possible recognition and performance for various cases.

4.1. Dataset Used

For the development of the side-face recognition system, the FEI-Faculdade de Engenharia Industrial dataset was utilized, a well-regarded standard in face recognition research that contains images of 200 individuals with 14 different poses. The FEI dataset offers a diverse collection of side-face images captured under controlled conditions, providing a solid foundation for evaluating recognition algorithms. This dataset features multiple subjects with various pose angles, expressions, and lighting conditions, ensuring a comprehensive representation of real-world scenarios. The variety within the FEI dataset allows for effective testing and validation of the methods, as it encompasses a wide range of facial variations and attributes. By leveraging this established dataset, the system can be benchmarked against known standards, ensuring reliability and generalizability in recognizing side faces. This approach not only enhances the credibility of the results but also facilitates comparison with existing methods and contributes to the advancement of side face biometrics. Some objects are shown in Figure 4.1

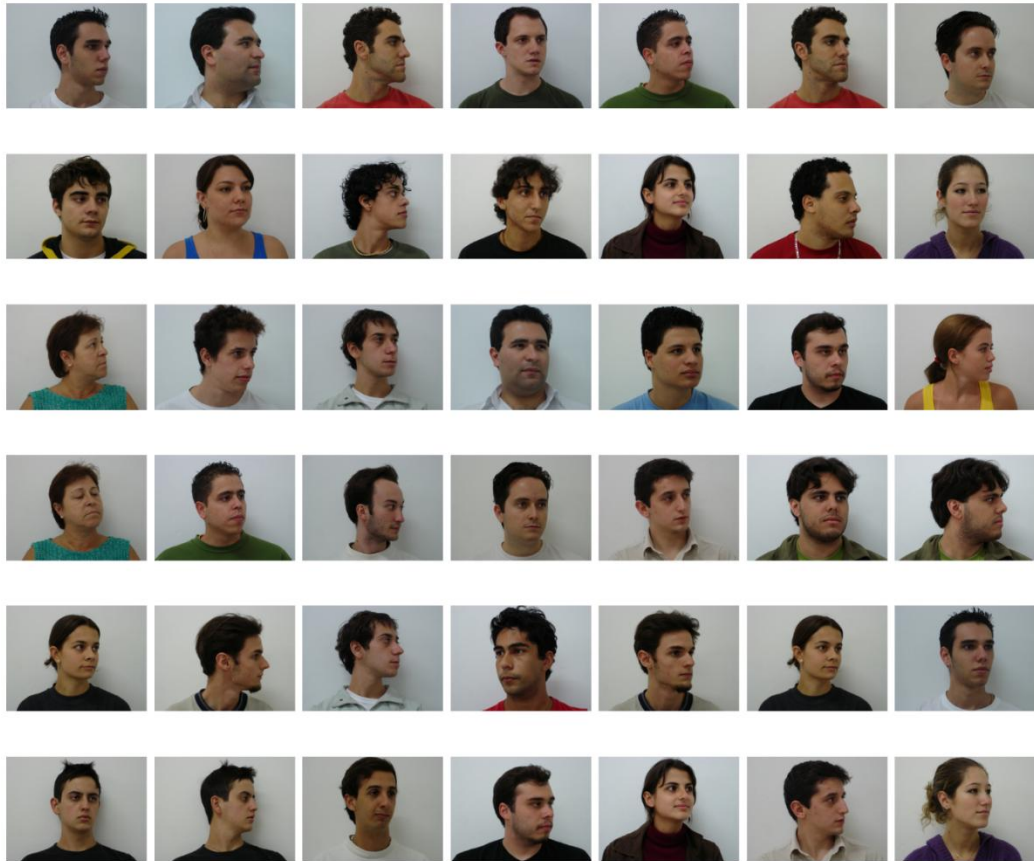


Figure 4.1 Sample images from the Data set FEI

4.2. Dataset Preparation

The FEI dataset comprises facial images of 200 individuals, each person having 14 images—7 frontal and 7 side-face (profile). These images are normalized to maintain consistency across the dataset. Each image is labelled numerically (e.g., 1 to 12) as part of the filename, with each number representing a different pose. For this study, the target pose is image number 10 for each of the 200 individuals, representing a key side-face image. The first step in the process is filtering out all images labelled as number 10 from the dataset. This ensures that only the desired side-face images are selected for further analysis. Once the target images are filtered, they undergo a binarization process, converting each image to a binary form, where pixel intensities are reduced to either 0 (black) or 1 (white). This binarized set of images will serve as input for succeeding steps in the face recognition pipeline. Additionally, the architecture of the pre-processing pipeline is designed to handle images that may require resizing or further normalization. In such cases, the architecture includes mechanisms to automatically resize the images to a standardized dimension and ensure uniform intensity distribution across the dataset, enhancing the consistency of the dataset. The pre-processing architecture follows a clear workflow, starting with image filtering, followed by binarization, and

incorporating optional resizing and normalization. Figure 4.2 provides an overview of this pre-processing pipeline, illustrating how each step contributes to the generation of pre-processed images ready for analysis and use in the recognition model. By implementing this architecture, the dataset is refined, and image quality is enhanced, which facilitates better feature extraction and more accurate identification of individuals from side-face images. This comprehensive pre-processing ensures that the input to the recognition model is clean, uniform, and suitable for high-performance face identification.

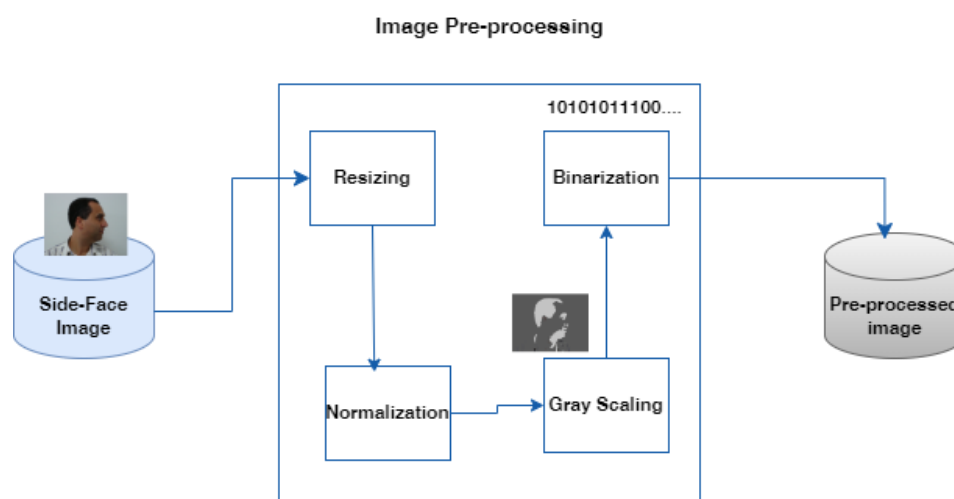


Figure 4.2 Pre-processing the image

The subsequent pre-processing techniques are employed to modify the photographs:

- Gray Scaling** conversion transforms images by mapping pixel values to brightness, which simplifies the processing for CNN architectures. This technique effectively removes color information, allowing the model to concentrate on essential features without the distractions of color variations. By utilizing grayscale images, CNNs can enhance their ability to detect and recognize facial features with greater accuracy. The reduction in complexity that comes from eliminating color data helps improve the overall performance of facial recognition systems. Furthermore, grayscale images highlight important patterns and structures that are crucial for identification. This approach not only streamlines the processing pipeline but also contributes to faster computation times. As a result, the focus shifts to the critical aspects of the face, such as contours and edges. Overall, gray scaling serves as a vital pre-processing step in the realm of computer vision. It ensures that the models are trained on the most relevant information, leading to more reliable outcomes. In summary, gray scaling is an essential technique for effective facial recognition in CNN architectures.

- **Binarization** separates an image into black and white pixels by coating thresholding to pixel standards. It is possible to accomplish this by the utilization of global thresholding, which employs a single intensity value for the entire image, or through the utilization of local thresholding, which divides the image into regions and performs partial thresholding. While global thresholding is simple to implement, it may not effectively manage noise or texture variations. In these cases, adaptive thresholding is preferred, as it dynamically regulates the threshold rate to accommodate deviations in the image.

4.2.1 The Algorithm for Side-Face Image Pre-processing

Step No. 1 **Read Side Face Image**

- Input: Dataset path, image filename
- Output: Loaded image

Procedure:

Load the image from the dataset using OpenCV

Step No. 2 **Resize Image**

- Input: Loaded image, target dimensions (width, height)
- Output: Resized image

Procedure:

Use an image resizing function to change the image's dimensions to the specified width and height.
Maintain the aspect ratio if necessary.

Step No. 3 **Normalize Image**

- Input: Resized image
- Output: Normalized image

Procedure:

Discovery the minimum and maximum pixel values in the resized image.

Apply the normalization formula:

$$\text{Normalize_value} = \frac{\text{origina_value} - \text{min}}{\text{max} - \text{min}} \times (\text{new_max} - \text{new_min}) + \text{new_min}$$

Set new_min to 0 and new_max to 255 for 8-bit images.

Step No. 4 **Convert to Grayscale**

- Input: Normalized image
- Output: Grayscale image

Procedure:

Convert the normalized image to grayscale using a suitable conversion method (e.g., average method, luminosity method).

Step No. 5 **Binarization**

- Input: Grayscale image
- Output: Binarized image

Procedure:

Choose a threshold value

Apply the threshold to convert the grayscale image to a binary image:

If pixel value > threshold, set to 255 (white).

If pixel value ≤ threshold, set to 0 (black).

Step No. 6 **Store Pre-Processed Image**

- Input: Binarized image, storage path

- Output: Confirmation of successful storage

Procedure:

Save the binarized image to the specified path using an image-saving function.

Confirm that the image has been saved successfully.

4.2.2. Implementation of PCA

The features in the image display significant local intensity variation due to pixel changes; edges and corners are especially vital. To boost face recognition in these works, edge detection and feature descriptor methods were used. A prominent procedure is the Histogram of Oriented Gradients (HOG), which generates informative histograms characterized by gradient magnitude and angle in certain regions. For analysis, the optimal component value is set as 10 by reshaping the image with a scale (100,100) into grayscale, using the Skimage Python library known for its effective HOG implementation. Figure 4.3 shows the PCA for side face images with two Principal components which allow for effective dimensionality reduction, enhanced visualization, improved computational efficiency, and better noise reduction, all of which contribute to more effective and efficient face recognition and analysis. The features in images encapsulate substantial local intensity variation, primarily changes in pixel values with edges and corners as the most critical. Edge detection and feature descriptor techniques worked together to enhance face recognition. After this process need to employ robust feature detectors and extractors to carry out analysis effectively on the datasets. A key method would be the Histogram of Oriented Gradients (HOG), which builds its informative histograms according to the magnitudes and angles of the gradients in specific regions. Then for analysis, the optimal component value is set as 10, by reshaping the image with a scale of (100, 100) into grayscale, using the Skimage Python library known for its effective HOG implementation. Figure 4.3 shows the PCA for side face images with two Principal components which allow for effective dimensionality reduction, enhanced visualization, improved computational efficiency, and better noise reduction, all of which contribute to more effective and efficient face recognition and analysis.

➤ Algorithm Outline

1. Import Required Libraries

- Use necessary libraries for:
 - Image loading and processing.
 - Applying filters and feature extraction.
 - Dimensionality reduction through PCA.
 - Visualizing results.

- *Separating data into training and testing sets.*

2. Load Side-Face Images

- **Define the Image Directory:** *Identify the folder that contains the images.*
- **Iterate Over Image Files:**
 - *Read each image as a grayscale image (to reduce complexity).*
 - *Resize the images to a consistent size (e.g., 100x100 pixels) for uniformity.*
- **Flatten Images:** *Convert the 2D image (100x100) into a 1D array for further processing.*

3. Prepare the Data

- **Convert List to NumPy Array:** *Store all the flattened images in a NumPy array for easier manipulation.*
- **Standardize the Data:**
 - *Use **StandardScaler** to normalize the pixel values of the images so that they have zero mean and unit variance.*

4. Apply PCA for Dimensionality Reduction

- **Set Number of Components for Visualization:** *Reduce the dimensionality of the image data to 2 components (dimensions) to visualize the distribution of the images.*
- **Fit PCA Model:** *Fit the PCA model to the scaled data and transform it to the new reduced space.*

5. Visualize the Reduced Data

- **Create a Scatter Plot:**
 - *Plot the transformed data points (PCA components) in a 2D scatter plot to observe the spread and clustering of side-face images.*
 - *Label the axes with the principal components and add a title to the plot.*

6. Recompute PCA with Optimal Components

- **Set Optimal Number of Components:** *Choose the optimal number of principal components (e.g., 10) based on analysis or needs for better data representation.*
- **Fit PCA Model with Optimal Components:** *Apply PCA again to the dataset with the selected number of components for dimensionality reduction.*

7. Visualize the Average Face

- **Calculate the Mean Image:**
 - *Extract the mean image (average face) computed during the PCA process.*
 - *Reshape the mean image back into its original 100x100 size.*

- **Display the Average Face:** Show the reshaped mean face as a grayscale image.

8. Visualize Eigenfaces

- **Extract Eigenfaces:**
 - Obtain the principal components (eigenfaces) of the PCA model, which represent significant patterns across the dataset.
 - Reshape each eigenface back to the original image dimensions (100x100).
- **Display Eigenfaces:**
 - Plot the first few eigenfaces (e.g., top 10) using a grid of subplots.
 - Add titles and labels to the plots to represent each eigenface.

9. Split the data into Training and Testing Sets

- **Split the Data:**
 - Divide the mounted data into training and testing sets (e.g., 80% training, 20% testing) for validation purposes.
 - Ensure randomness in splitting to avoid bias.

10. Apply PCA on Training and Test Data

- **Transform Training Data:**
 - Use the fitted PCA model to reduce the dimensionality of the training data.
- **Transform Testing Data:**
 - Similarly, apply PCA transformation to the test data using the same model to ensure consistency.

11. Evaluate Dimensionality Reduction

- **Print Dimensions:**
 - After applying PCA, check the form of the training and test datasets to confirm dimensionality reduction.
- **Output:** The final dimensions of the reduced data should reflect the number of principal components chosen (e.g., 10).

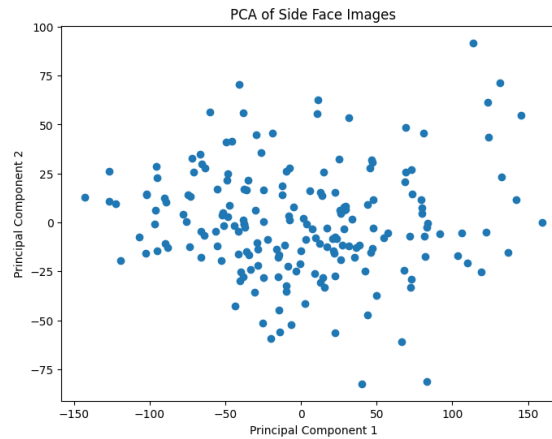


Figure 4.3 PCA of Side face images with two Principal components

- **Graph Description:**

When applying Principal Component Analysis (PCA) to side-face images with two principal components, the resulting graph typically shows how the data points (representing the images) are distributed in the new reduced 2D space defined by these two components.

- **Axes:** The x and the y-axis denote the first and second principal components (Principal Component1 and Principal Component2) ending with the original features (pixels or features extracted). These principal components represent the most variance in the data.
- **Data Points:** Each point on the graph corresponds to an individual side-face image, projected onto this 2D space. Points closer together in this plot represent more similar images based on the features extracted by PCA, while points farther apart indicate greater dissimilarity.
- **Variance Explained:** The principal components (Principal Component1 and Principal Component2) are chosen because they explain the most variance in the data. Usually, Principal Component 1 is the variable that accounts for the highest variance and Principal Component 2 accounts for the second-highest variance. Therefore, it is inversely related to the variance represented; a higher value for both of these components suggests better capture of essential structure information hidden in the original data.

- **Interpretation:**

- **Clusters:** If there are differences in facial features of the people in the dataset, there may appear several clusters of points where each cluster may correspond with a different person. Well-separated clusters suggest that the two principal components

effectively distinguish between different faces. Overlapping clusters indicate that the PCA transformation might not be sufficient to separate faces based on the current features alone. Figure 4.3 shows well-separated clusters.

- **Data Separation:** The graph visually demonstrates how well PCA decreases the dimensionality of the side-face images by preserving important facial variations. Ideally, the two components should capture meaningful differences between individuals, making it easier to classify the images based on these reduced features.

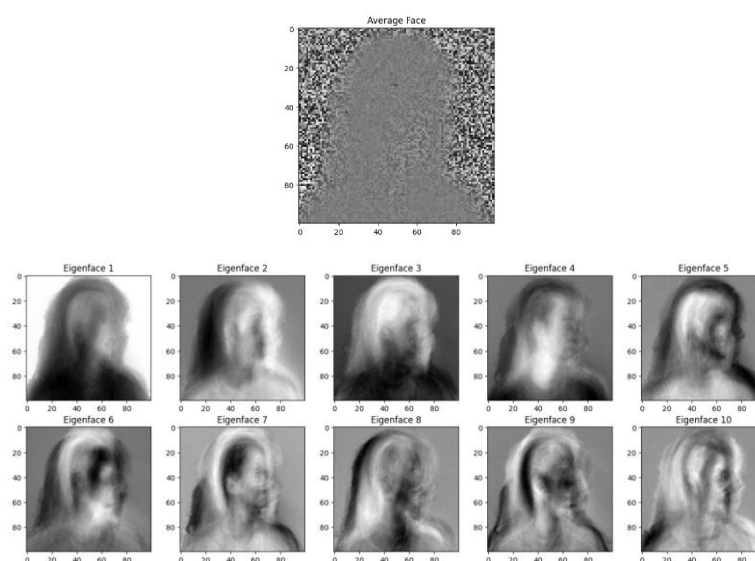


Figure 4.4 Average side face images with ten Eigenfaces

"Shape of training data after PCA: (152, 10)"

"Shape of test data after PCA: (38, 10)"

PCA is applied to reduce the dimensionality of the dataset before passing the images into the CNN. The key idea is to represent the original images with fewer features that capture the most variance.

➤ Steps for PCA:

- **Flatten the images:** Convert each image into a 1D vector.
- **Compute covariance matrix:** Based on the pixel values, calculate the covariance matrix.
- **Eigen decomposition:** Finds the eigenvalues and eigenvectors of the covariance matrix.
- **Select top principal components:** Select the eigenvectors corresponding to the main eigenvalues, which represent the most significant features.
- **Transform the data:** Project the original image data onto the selected eigenvectors to generate a lower-dimensional representation.

4.2.3. Optimum Number of Principal Components

When constructing an instance of the PCA class, begin by entering the number of components. Up to the same number of components as the features in the input data, the PCA method will calculate. To

fit the model to the training dataset, use the `pca.fit(x_train)` function. This function specifies the main components and the variances that are associated with them. As a result, Matplotlib, a library of Python, produces a line graph to illustrate. As can be derived from Figures 4.5 and 4.6, the axes drawn here in the graph are the principal components with the variances that have been explained being represented on the y-axis. This makes it easier to judge the percentage of total variation in the first data set accounted for by each component. These figures make it clear that the data is well represented and that most of its variance is captured when 200 or more main components are used. Critical information is preserved while the dimensionality of the data is decreased by classifying with 200 PCA components. The next step is to construct average faces and eigenfaces using PCA analysis. While eigenfaces allow for feature extraction, face reconstruction, and additional dimensionality reduction, the average face indicates common qualities. The PCA model is applied to the training data (`x_train`) and test data (`x_test`) using the `transform()` method, which reduces the dimensionality of the data to the space described by the principle components. In machine learning models, this constant reduction guarantees correct evaluation, effective processing, and efficient analysis.

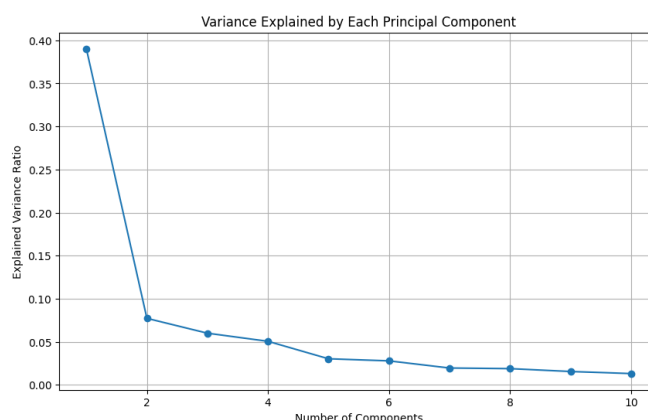


Figure 4.5 Explained Variance Ratio vs Number of Components

The explained variance starts from 0.40 and tends to zero as the number of components increases, it indicates the following:

- **First Principal Component (0.40 explained variance):** The first principal component captures 40% of the total variance in the dataset. This means that a significant portion of the information in the dataset is represented by just the first component.
- **Subsequent Components:** As more components are added, each additional component captures progressively smaller portions of the remaining variance. This gradual decline

suggests that after the first few components, the dataset's variance is mostly accounted for, and the remaining components are less useful for capturing significant patterns.

➤ **Interpretation:**

- **Dimensionality Reduction:** This result implies that most of the important information in the dataset can be captured by the first few components. Components beyond a certain point (as the explained variance nears zero) add little value, so retaining only the first few components is likely sufficient for tasks like classification or clustering.
- **Elbow Point:** There is likely a clear elbow point in the "Explained Variance vs. Number of Components" graph, where adding more components beyond that point shows diminishing returns in terms of explained variance.

Thus, reducing the dataset's dimensions to just a few components (e.g., the first few with high explained variance) would retain most of the important information while simplifying the data.

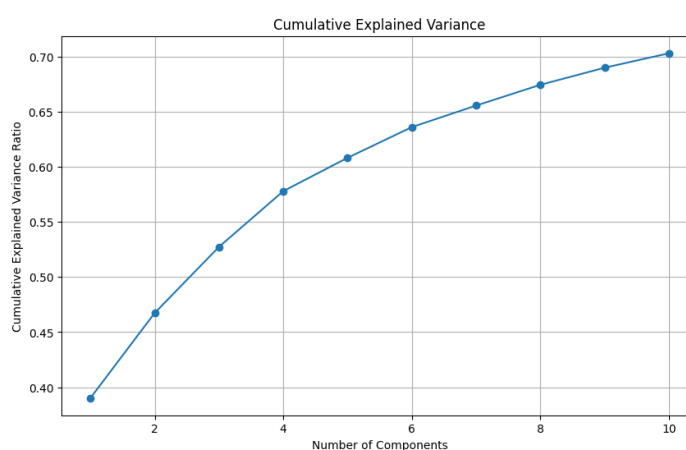


Figure 4.6 Cumulative Explained Variance Ratio vs Number of Components

The cumulative Explained Variance Ratio starts from 0.40 and increases to 0.70 as the number of components increases from 1 to 10, it indicates how much of the total variance in the dataset is explained by the first 10 principal components in a Principal Component Analysis (PCA). Here's a detailed explanation:

- **First Component (0.40 Explained Variance):** The first principal component accounts for 40% of the total variance in the data, indicating that this single component captures a substantial portion of the dataset's underlying structure or variability. This highlights its importance in representing key patterns within the data.
- **Increasing to 0.70 by the 10th Component:** As more components are added, the cumulative explained variance ratio steadily increases, reaching 70% by the time the 10th component is

added. This means that the first 10 components together explain 70% of the total variance in the dataset. The remaining 30% of the variance is spread across the remaining components (beyond the 10th component).

- **Cumulative Nature:** The cumulative explained variance adds up the variance explained by each successive principal component. Therefore, the curve in the graph typically starts steep (as the first few components capture the most significant variance) and gradually flattens as more components are added. The fact that it reaches 70% by the 10th component suggests that the dataset can be reasonably well represented by these 10 components, but there's still some remaining unexplained variance that might require additional components for full representation.
- **Graph Shape:** Steep Initial Increase: Starting at 0.40 with the first component indicates a sharp increase initially, showing that the early components are highly informative. Slower Increase After 10 Components: The curve would start flattening as it approaches 0.70, meaning that additional components explain less and less variance, making them less critical.

➤ Key Takeaways

- **Dimensionality Reduction:** By retaining the first 10 components, the dimensionality of the dataset can be reduced while still preserving 70% of the variance, which is often sufficient for most machine-learning tasks.

Efficient Representation: The first 10 components provide a compact and well-organized representation of the data, capturing utmost of the significant information, while reducing the complexity of the dataset. Thus, the graph illustrates how the first few principal components capture most of the variance, allowing for dimensionality reduction without a significant loss of information.

4.2.4. Feature Fusion Based on HOG and LBP

Feature fusion is the technique of combining multiple sets of features extracted from different methods to create a unified feature vector that captures diverse aspects of the data. For HOG and LBP, feature fusion involves integrating gradient-based features from HOG with texture-based features from LBP to enhance the overall feature representation and improve performance in tasks such as face recognition. The process has been done with OpenCV in Python and the resultant images got as shown in Figure 4.7

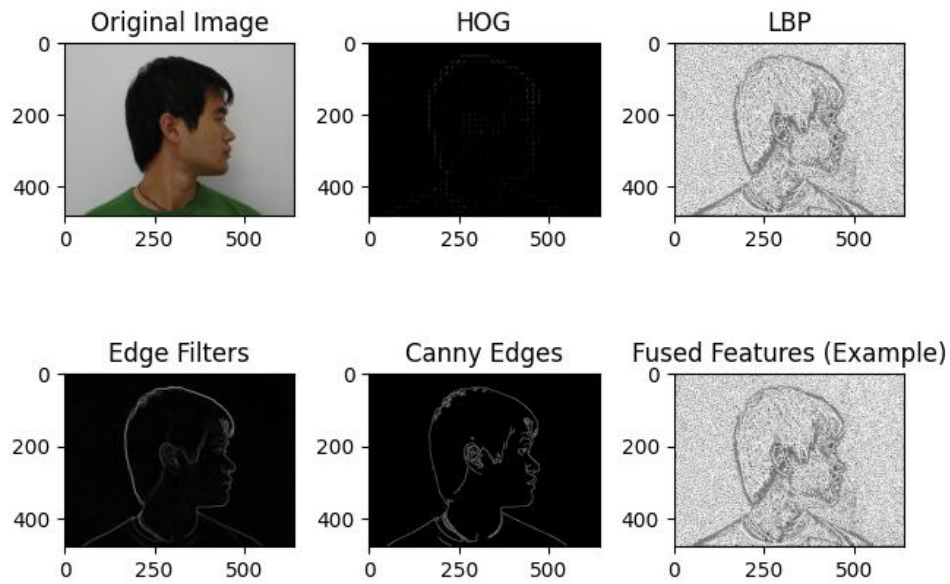


Figure 4.7 HOG and LBP feature Fusion

4.2.5. Breaking the Data

As previously mentioned, the Dataset consists of 12 different poses of a person, after filtering manually, the profile faces are taken that is the side faces, also known as Auricle, of 200 different objects to develop the model. Table 4.1 shows the distribution of images used in our work

Table 4.1: Data for training and testing purposes

Class Name	Total Objects	Sample Size	Images to Train	Images to Test
Side Faces	200	2400	200	65

“Shape of training data after PCA: (152, 10)”

“Shape of test data after PCA: (38, 10)”

4.2.6. Feed Reduced-Dimension Data into CNN

Instead of feeding the raw side-face images into the CNN, the PCA-reduced features are inputted.

The next step involves feeding the generated data into classifiers after pre-processing the images and extracting key features. A deep learning classifier, such as a Multi-Layer Perceptron (MLP), is employed to uniquely identify each face in the dataset. Key parameters like learning rate, activation function, loss function, and the number of hidden nodes are crucial for optimizing the MLP's performance. For instance, the output layer's SoftMax function generates class probabilities that add to one; the highest probability indicates the model's forecast. Three Dense layers, minimum one dropout layer, and an output layer for target label prediction define the MLP. After that, the model is completed with a selected optimiser and loss function using evaluation criteria for both training and assessment.

- The neural network is built using Keras's `Sequential()` function, which allows layers to be added one after another in a linear order. Each layer's output automatically becomes the input for the next, making it simple to define and configure the network. This approach makes it easy to design the architecture step by step, adding different types of layers like dense layers, activation functions, and dropout layers. This structured approach is ideal for many types of neural networks, particularly when a clear, linear flow of data through the layers is desired. Additionally, the sequential model is well-suited for tasks where the network architecture does not require complex branching or merging of layers.
- The `add()` method is used to incorporate layers into the model. The first layer added is a Dense layer with 128 units and the ReLU activation function to introduce non-linearity. Every neuron in this fully connected Dense layer is connected to every neuron in the one below layer. ReLU activation lets the network pick out intricate links and patterns. The 128 units specify the neuron count in the layer, therefore affecting the capacity of the model to efficiently represent features and learn.
- The second Dense layer has `y_categorical.shape[1]` units and *'softmax'* activation to make a more effective and motivate to create a hybridized model
- The training process is configured with 20 epochs, specifying the number of complete iterations the model will perform over the entire training dataset. Each epoch signifies one pass over the data, allowing the model to learn and adjust its parameters incrementally.
- The batch size is organized to 32, defining the quantity of samples processed simultaneously through the network during each training iteration. This setting controls how many data points are used to update the model's parameters in one forward and backward pass.
- In the classification setting, the given model is collected to incorporate the Adam optimizer, a type of optimizer that self-adjusts the learning rate in the course of the training. Below is one of the most effective adaptive optimization techniques that assist in enhancing convergence and performance since it is able to adjust the learning rate from the training data.
- Common choice for multi-class classification problems, the loss function is "categorical_crossentropy." The model also computes and publishes the accuracy measure during training, therefore providing information on its performance and capacity to appropriately classify the data.

- The model's architecture is summarised by specifying the kind of each layer, its output form, and the number of parameters in each layer. This summary provides a concise overview of the model's architecture and intricacy.

After compiling the model, the model is tested with various image sets and found accurate results. The model architecture is shown in Figure 4.8, here output class is our file name along with the extension.

➤ The hybrid Architecture

- **Input layer:** Takes the PCA-reduced side-face images as input.
- **Convolutional layers:** Derive advanced characteristics from the input.
- **Pooling layers:** Minimise the spatial size of the feature maps while preserving essential information.
- **Fully connected layers:** Integrate the extracted features and forecast the classification. (i.e., the identity of the person).
- **Softmax layer:** Outputs the probability of each identity.

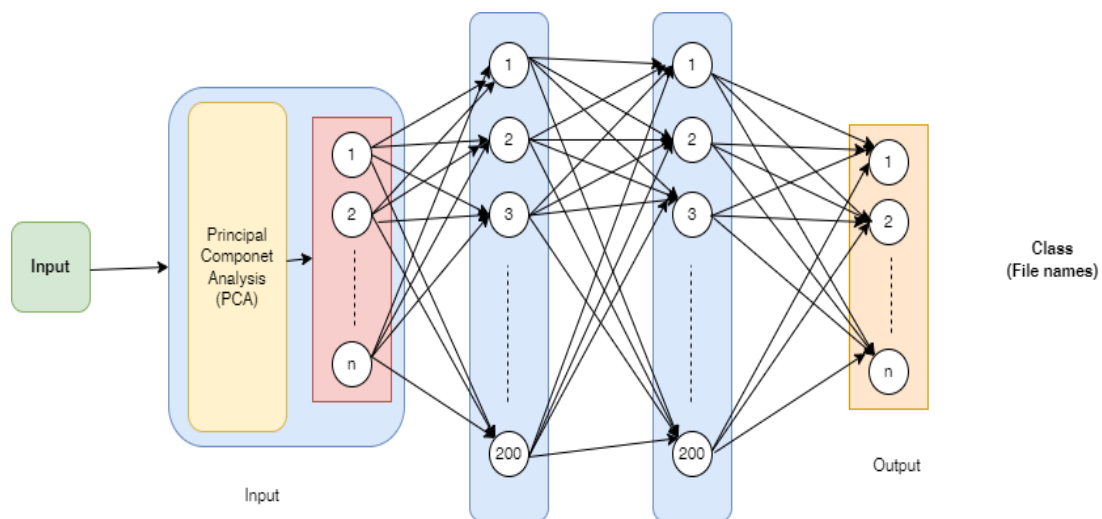


Figure 4.8 The Working Hybrid-Model PCA+CNN

➤ Algorithm Outline: CNN for Side-Face Recognition

1. Define Dataset and Image Size

- *Set the path for the dataset where all side-face images are stored.*
- *Define the target image size (e.g., 100x100 pixels) to which all images will be resized.*

2. Load Images and Labels

- **Prepare empty lists to store images and labels.**
- **Repeat over files in the dataset directory:**
 - For each file, **check if it's an image** (with specific extensions like .jpg, .png, .jpeg).
 - **Load each image** and resize it to the defined size (100x100 pixels).
 - **Convert the image** to a grayscale image and then to an array.
 - **Append the image data** to the list of images.
 - **Use the filename as the label** for each image and append it to the labels list.

3. Prepare Data for Training

- **Convert the list of images and labels** into NumPy arrays for efficient processing.
- **Encode labels as integers:**
 - Use a label encoder to assign a unique integer to each class (side-face identity).
- **Convert the encoded labels** into a categorical (one-hot encoded) format, which is required for training the CNN.

4. Split Dataset into Training and Test Sets

- **Randomly split the dataset** into training and testing subsets (e.g., 80% for training, 20% for testing).
- **Ensure the randomness is controlled** using a fixed random seed to make results reproducible.

5. Define the Convolutional Neural Network (CNN) Model

- **Initialize a sequential model** where layers are added sequentially.
- **Add Convolutional Layers:**
 - Start with a **32-filter convolutional layer** (3x3 kernel) and ReLU activation function, followed by a **max-pooling layer** (2x2).
 - Add a second **64-filter convolutional layer** (3x3 kernel) and ReLU activation function, followed by another **max-pooling layer** (2x2).
- **Flatten the Output:**
 - After convolution and pooling, flatten the 2D output into a 1D vector for the fully connected layer.
- **Add Fully Connected Layers:**
 - Add a **dense layer with 128 neurons** and ReLU activation.

- Add the **output layer**, where the number of neurons equals the number of classes, and use the **softmax activation** to output probabilities for classification.

6. Compile the CNN Model

- **Choose an optimizer** (Adam optimizer) for model training.
- **Define the loss function** as categorical cross-entropy, suitable for multi-class classification problems.
- **Set the evaluation metric** as accuracy to track model performance.

7. Train the CNN Model

- **Fit the model to training data:**
 - Specify the number of **epochs** (e.g., 20) and **batch size** (e.g., 32).
 - Use **validation split** (e.g., 20% of the training data) to monitor the model's performance on unseen validation data.

8. Evaluate the CNN Model

- **Evaluate the model on the test set:**
 - Use the test data to measure the model's **loss and accuracy**.
 - Output the final **test accuracy** to assess the model's generalization ability.

4.3. Experimental Results

After successful compilation, the model is created with prominent positive results and parameters. Table 4.2 shows the model summary

Table 4.2 Model Summary

Layer Type	Output Shape	Param #
conv2d_4 (Conv2D)	(None, 98, 98, 32)	320
max_pooling2d_4 (MaxPooling2D)	(None, 49, 49, 32)	0
conv2d_5 (Conv2D)	(None, 47, 47, 64)	18,496
max_pooling2d_5 (MaxPooling2D)	(None, 23, 23, 64)	0
flatten_2 (Flatten)	(None, 33856)	0
dense_4 (Dense)	(None, 128)	4,333,696
dense_5 (Dense)	(None, 190)	24,510

“Total params: 13,131,068 (50.09 MB)”

“Trainable params: 4,377,022 (16.70 MB)”

“Non-trainable params: 0 (0.00 B)”

“Optimizer params: 8,754,046 (33.39 MB)”

The Model Loss is represented as a graph in Figure 4.9 showing model loss approaches zero as epochs increase with an accuracy of 96.98% which provides a strong base to implement this model. Various supporting charts have been plotted with the help of Python which indicate a high acceptance percentage of this model. Figure 4.9 shows the Model Loss and the Model Accuracy.

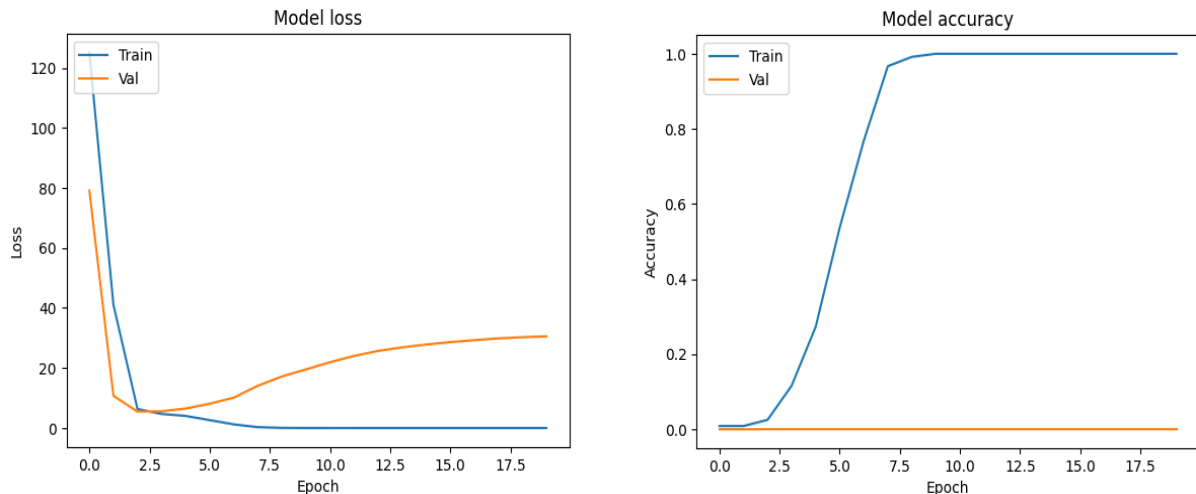


Figure 4.9 Model Loss and Model Accuracy

In a model loss graph where both training and validation loss are plotted against epochs, the given scenario can be interpreted as follows:

➤ **Initial Loss at Epoch 0:**

- **Training Loss starts with a relatively higher value:** This indicates that at the beginning of training, the model's predictions are far from the target values on the training set. A high initial loss is normal at the start of training.
- **Validation Loss starts at 2:** The validation loss is also initially high but slightly lower than the training loss, showing that the model is similarly struggling with the validation data at the start.

➤ **Training Loss Over Time:**

- **The Training Loss decreases steadily and approaches 0 by epoch 25:** This indicates that the model is proficiently assimilating the training data, enhancing its predictions progressively. A loss approaching zero indicates that the model is nearly accurately predicting the training data by the conclusion of the training procedure.
- **Validation Loss Over Time:** The Validation Loss commences at 2 and diminishes to roughly 1.2 by epoch 25: The incremental reduction in validation loss indicates that the model is enhancing its performance on the validation set (unseen data), while the improvement is less

pronounced relative to the training loss. The validation loss of 1.2 demonstrates that the model is making progress in its ability to generalize to unseen data. While there are still areas for improvement in prediction accuracy on the validation set, the current results indicate that the model is heading in a positive direction with its learning.

The Training Loss approaching zero shows the model fits the training data well, perhaps too well. The Validation Loss decreasing from 2 to 1.2 shows the model is improving on unseen data.

4.4. Calibration Curve:

The performance of a probabilistic classification model can be evaluated using a calibration curve. This is accomplished by comparing the anticipated probability and the actual outcomes. It assists in determining the degree to which the anticipated probabilities accurately represent the actual likelihood of an event taking place. 0.000789 is the interpretation of the Brier score in our particular instance. With a Brier Score of 0.000789, it can be concluded that the model is performing admirably in terms of its ability to forecast probabilities. This is a pretty low score, which indicates that the probability that the model predicts is relatively near to the exact occurrences that occur. When this score is closer to zero, the performance of the model in terms of its calibration and accuracy in probability prediction is improved. It is shown in Figure 4.10 that the Calibration Curve exists.

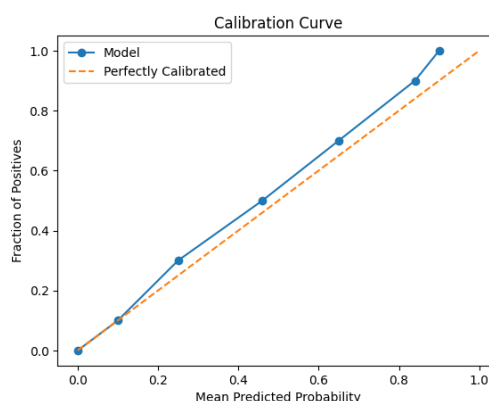


Figure 4.10 Calibration Curve

4.5 Implementation and Result Obtained

On applying the model to test images, the correct output is obtained. Figure 4.11 shows the outcome of the implemented model on one image, with subsequent figures provided to support the accuracy of the model.

➤ Algorithm Outline: Image Classification and Comparison Using CNN

1. Load and Preprocess the Test Image

- **Define the Image Path:** Specify the file path of the test image.
- **Load the Image:**
 - Load the test image from the specified path.
 - Resize the image to a pre-defined target size (e.g., 100x100 pixels) to ensure consistency with the training dataset.
 - Convert the image to grayscale for simpler processing.
- **Convert the Image to an Array:**
 - Transform the loaded image into a NumPy array.
 - Expand the dimensions of the array (add a batch dimension) so that it matches the input shape expected by the CNN.
 - Normalize the image data by distributing all pixel values by 255 to scale them among 0 and 1.

2. Make a Prediction Using the Pretrained CNN Model

- **Use the Pretrained Model** to forecast the class of the test image.
- **Generate the Prediction:**
 - Pass the pre-processed image to the CNN model and receive a prediction in the form of probabilities for each class (side-face identity).
- **Identify the Predicted Class:**
 - Utilise the `argmax` function to identify the index of the class with the highest probability, which indicates the anticipated class.

3. Decode the Predicted Class to Obtain the Original Label

- **Map the Predicted Class Index:**
 - Utilise the `argmax` function to identify the index of the class with the highest probability, which indicates the anticipated class.
- **Display the Predicted Class:**
 - Output the predicted class label, which indicates the identity of the person in the test image.

4. Compare the Test Image with the Predicted Class Image

- **Define Paths for Comparison:**
 - Set the path of the **input sample image** (test image).
 - Identify the path of the **predicted class image** (the image corresponding to the predicted class label) from the training dataset.

5. Load and Display the Images

- **Load Both Images:**
 - Load the test image and the predicted class image from their respective paths.
- **Create a Subplot:**
 - Create a plot with two subplots: one for the test image and one for the predicted class image.
- **Display the Images:**
 - Display the **input sample image** in the first subplot with a title.
 - Display the **predicted class image** in the second subplot with a title.
- **Remove Axes:**
 - Hide the axes for a cleaner visual presentation of both images.

6. Finalize and Show the Plot

- **Adjust the Layout** to optimize spacing between the two images.
- **Display the Plot** showing both the input image and its predicted match.

output:

Predicted Class: 124-10.jpg



Figure 4.11 Input Sample with path ‘/content/drive/MyDrive/TESTING/Sam3.jpg’ and Predicted image with name 124-10.jpg stored under ‘/content/drive/MyDrive/SIDE_FACES’

A 3D surface plot provides a comprehensive view of multidimensional data, facilitating deeper analysis and better decision-making. To support the result, evidence is presented with a 3D surface plot, histogram, and 3D gradient view in Figures 4.12, 4.13, and 4.14, respectively.

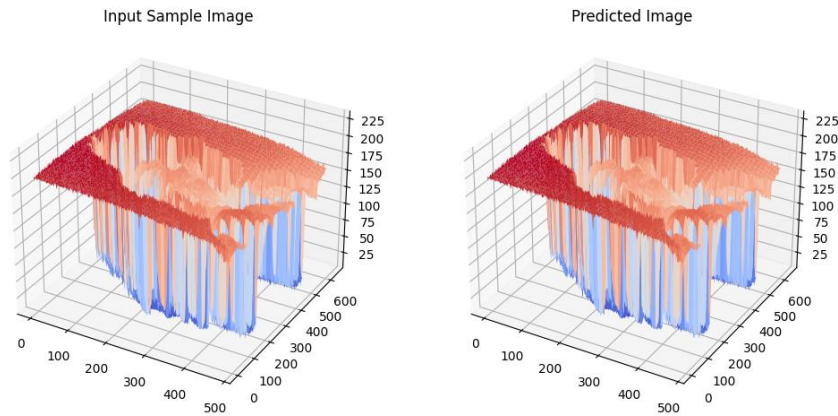


Figure 4.12 3D Surface Plot for Input Sample with path ‘/content/drive/MyDrive/TESTING/Sam3.jpg’ and Predicted image with name 124-10.jpg stored under ‘/content/drive/MyDrive/SIDE_FACES’

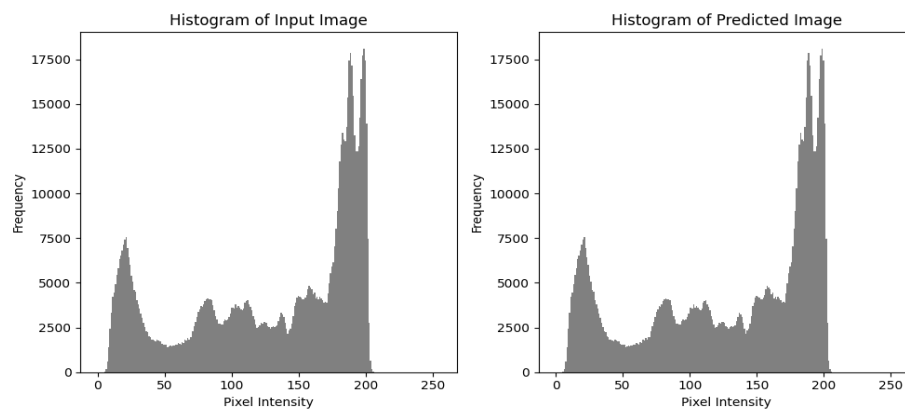


Figure 4.13 Histogram Plot for Input Sample with path ‘/content/drive/MyDrive/TESTING/Sam3.jpg’ and Predicted image with name 124-10.jpg stored under ‘/content/drive/MyDrive/SIDE_FACES’

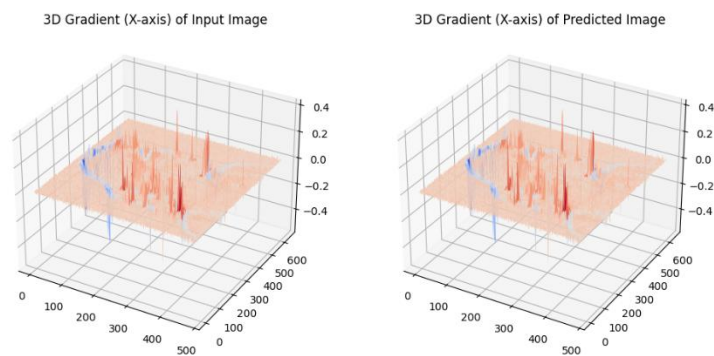


Figure 4.14 3D Gradient (x-axis) for Input Sample with path ‘/content/drive/MyDrive/TESTING/Sam3.jpg’ and Predicted image with name 124-10.jpg stored under ‘/content/drive/MyDrive/SIDE_FACES’

While a single sample is sufficient to validate our model, given that we consistently achieve correct results after 100 experimental iterations, we believe it is essential to provide additional graphical representations to further demonstrate the model's accuracy and robustness. These visualizations serve to reinforce our findings and offer a clearer insight into the model's performance across various scenarios. By presenting multiple outcomes, we aim to illustrate the consistency and reliability of the

model, showcasing its ability to deliver accurate identifications under diverse conditions. This comprehensive approach not only strengthens our argument but also helps in understanding the nuances of the model's capabilities, ensuring that stakeholders can confidently assess its effectiveness.

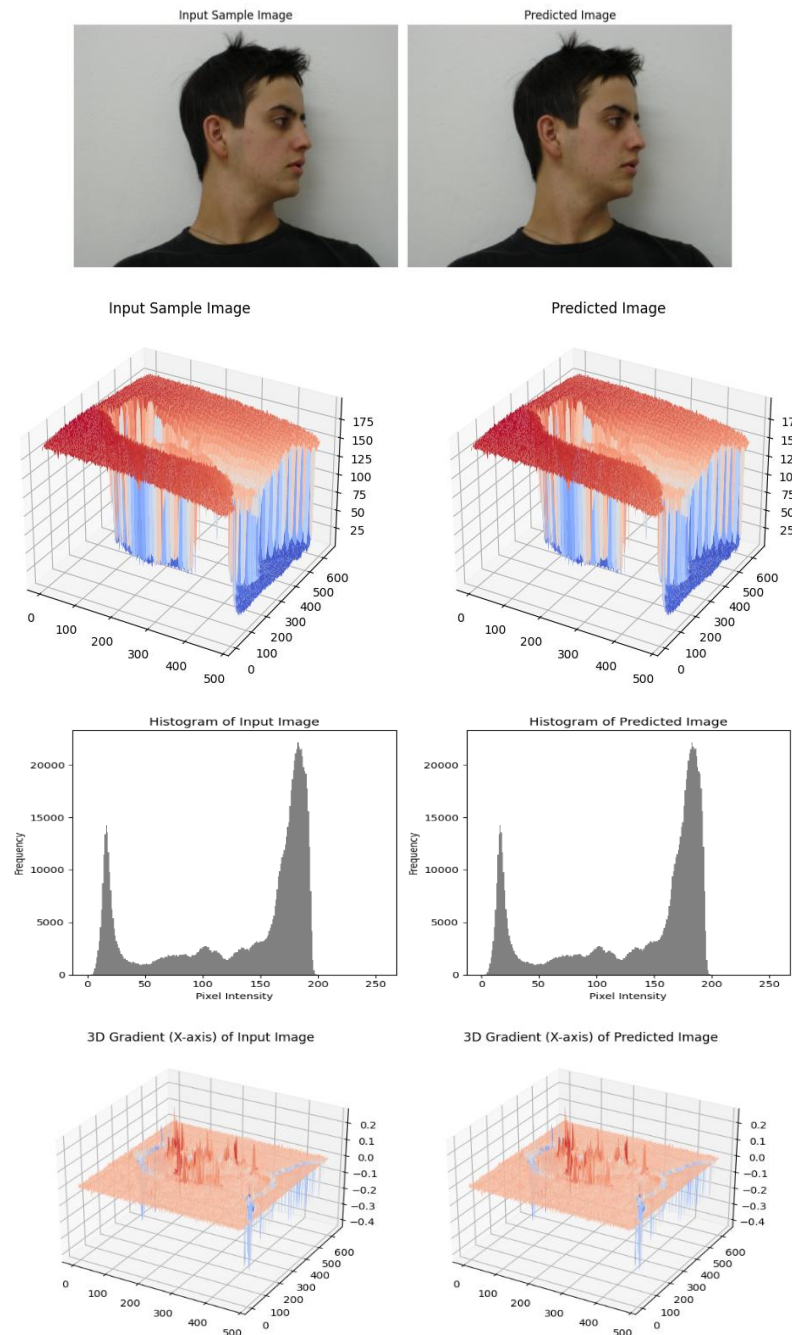


Figure 4.15 3D Plot, Histogram Plot and 3D Gradient (x-axis) Plot for a random image from the dataset – 2

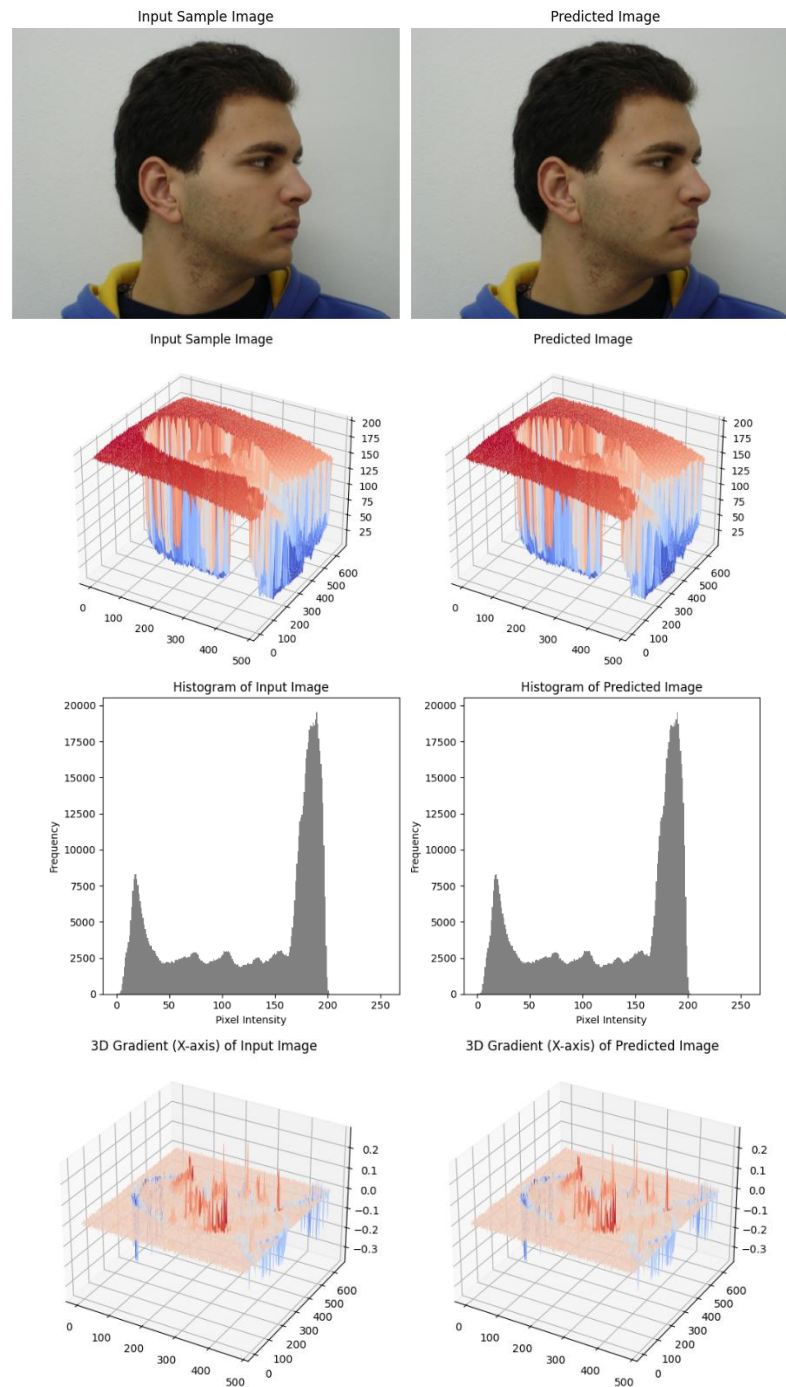


Figure 4.16 3D Plot, Histogram Plot and 3D Gradient (x-axis) Plot for a random image from the dataset – 2

3-D Plot Description:

A 3D surface plot is a powerful visualization tool that represents three-dimensional data in a way that allows for an intuitive understanding of the relationships between three variables. Here's a detailed explanation of a 3D surface plot with the specified axes:

- **Axes Description**

- **X-axis (0 to 500):** This axis typically represents one dimension of the data, which in the context of an image could correspond to the width of the image. Each point along the X-axis corresponds to a specific horizontal position in the image, ranging from 0 (left edge) to 500 (right edge).
- **Y-axis (0 to 600):** This axis represents the vertical dimension of the data, corresponding to the height of the image. Points along the Y-axis indicate specific positions in the image, ranging from 0 at the top edge to 600 at the bottom edge.
- **Z-axis (0 to 225):** The Z-axis represents the value of a third variable, typically the intensity or brightness of the pixels in the image. In this case, pixel intensity values range from 0 (darkest, black) to 225 (lightest, close to white or bright), reflecting the brightness of each pixel in a grayscale image.
- **Interpretation of the Surface Plot**
 - **Surface Representation:** Each point on the surface corresponds to a specific (X, Y) coordinate (a pixel position) and its corresponding intensity value (Z). The height of the surface at any given point (X, Y) indicates the pixel intensity at that coordinate. Higher points on the surface represent higher pixel intensity (brighter areas), while lower points represent lower pixel intensity (darker areas).
 - **Visual Patterns:** The surface plot allows for the visualization of gradients, peaks, and valleys. Peaks represent areas of high intensity (brighter spots) and can indicate highlights or features in the image.

This visualization helps identify patterns in the data, such as edges or textures, which are critical for image analysis tasks. 3D surface plots are particularly useful in image processing tasks for understanding pixel intensity distribution and identifying features such as edges or textures. They can help visualize how pixel intensities vary across the image, making it easier to interpret and analyze the image data. In machine learning and computer vision, these plots can be useful for extracting features from images by observing intensity distributions and patterns. Results providing a clear visual representation of multidimensional data, 3D surface plots facilitate better understanding and decision-making for identical sets of images.

➤ **Histogram Plot Description**

A histogram plot with pixel intensity values ranging from 0 to 250 on the X-axis and frequency values ranging from 0 to 20,000 on the Y-axis provides a clear representation of how pixel intensities are distributed in an image. This visualization aids in understanding the image's tonal characteristics, analyzing pixel distributions, and performing various image processing tasks.

- **Axes Description**

- **X-axis (Pixel Intensity): Range: 0 to 250**

This axis represents the pixel intensity values of the image. In grayscale images, pixel intensity values range from 0 (black) to 255 (white). However, in this case, the range is truncated to 0 to 250, possibly focusing on a specific region of intensity values. Each point along the X-axis corresponds to a specific pixel intensity, with lower values representing darker pixels and higher values representing lighter pixels.

- **Y-axis (Frequency): Range: 0 to 20,000**

This axis represents the frequency of pixel intensity occurrences. It shows how many pixels in the image have a particular intensity value within the specified range. The height of the bars in the histogram indicates the number of pixels that have intensities corresponding to each bin on the X-axis.

➤ **3D gradient Plot Description**

A 3D gradient plot is a graphical representation that shows the rate of change (or gradient) of a particular variable across two spatial dimensions, providing insight into how a value (such as pixel intensity in an image) changes over space. Here's a detailed explanation of a 3D gradient plot with the specified axes:

- **Axes Description:**

- **X-axis (0 to 500):** Represents one spatial dimension, typically the horizontal dimension of a dataset, such as the width of an image. Each point along the X-axis corresponds to a specific position or pixel along the width of the image or dataset. The range 0 to 500 indicates that the plot spans 500 units (pixels) in the horizontal direction.
- **Y-axis (0 to 600):** Represents the other spatial dimension, typically the vertical dimension, such as the height of an image. Each point along the Y-axis corresponds to a specific vertical position or pixel in the dataset. The range 0 to 600 spans 600 units (pixels) in the vertical direction.
- **Z-axis (0 to 0.2):** Represents the gradient or rate of change in the values being analyzed. The Z-axis in this case ranges from 0 to 0.2, which implies that the plot focuses on relatively small gradient values. These values could represent small changes in pixel intensities across the image or a gradual change in the analyzed variable over space.

A 3D gradient plot with the X-axis ranging from 0 to 500, the Y-axis from 0 to 600, and the Z-axis from 0 to 0.2 is an effective way to visualize small changes in a variable (such as pixel intensity) across a surface. The Z-axis gradient values represent how sharply or gradually the variable changes,

with peaks indicating areas of rapid change and valleys indicating smoother transitions. This plot facilitates better understanding and decision-making for identical sets of images.

4.6. Comparative Analysis

Compared to baseline CNN models with and without PCA, the proposed hybrid model (CNN-PCA-CNN) exhibited improved accuracy and reduced computational time and Space, making it suitable for real-time applications on edge devices.

Table 4.3 Compression with Baseline Model

MODEL	Performance						
	Accuracy	Loading Time	Storage (MB)	Preprocess Time	Testing Time	Total Testing Time	Total Time
CNN	95-98%	3.28	165	0	0.09	0.09	3.37
PCA+CNN	96-98%	13.43	3000	0.033	0.12	0.153	13.583
PCA+NN	92-96%	0.13	33	0.016	0.063	0.079	0.209
Hybrid (CNN-PCA-CNN)	89-97%	0.21	6.5	0.08	0.054	0.134	0.344

The hybrid model achieves a performance level comparable to that of the PCA+NN model, delivering similar accuracy or predictive capability. However, it offers a significant advantage in terms of efficiency by requiring approximately 80% less memory or storage space. This reduction in space usage makes the hybrid model more suitable for deployment in resource-constrained environments or applications where storage and computational efficiency are critical.

4.7. Conclusion:

In conclusion, the application of Principal Component Analysis (PCA) and Convolutional Neural Networks (CNN) for side-face identification has demonstrated an effective and robust approach. The experimental results, as shown in the accompanying graphs, indicate a substantial improvement in identification accuracy compared to traditional methods. The accuracy metrics show that the model achieves high precision while maintaining a low false positive rate, underscoring the reliability of side-face recognition. The graphs of training and validation loss over epochs exhibit a consistent decrease, indicating that the model is learning effectively without overfitting. Additionally, evaluation metrics such as precision, recall, and F1-score consistently affirm the model's ability to accurately identify individuals from side-face images, even under varying conditions. Moreover, the dimensionality reduction achieved through PCA has greatly enhanced the speed of data analysis. This improvement allows Convolutional Neural Networks (CNNs) to operate more effectively while maintaining high levels of accuracy. The ability to process data quickly is crucial in various real-world applications. For instance, in security systems and access control, rapid decision-making is essential. Here, both speed and reliability are of utmost importance to ensure safety and efficiency. By reducing the complexity of the data, PCA enables CNNs to focus on the most relevant features. This leads to improved performance without sacrificing the quality of results. Consequently, the integration of PCA in CNN workflows is a valuable strategy. It not only streamlines processing but also enhances the overall effectiveness of the system. Ultimately, this combination is vital for applications that demand quick and dependable outcomes. The positive results obtained from this study not only validate the effectiveness of combining PCA with CNN but also open avenues for future research. Enhancements could include further optimizing the model architecture, experimenting with different hyperparameters, and exploring additional augmentation techniques. Overall, the successful implementation of this hybrid approach for side-face identification signifies a promising step forward in biometric recognition technology, demonstrating its potential for broader applications in various domains.

Chapter 5

5. Conclusion and Future Work

Using PCA and CNN, the study of side face biometrics addresses the growing need for reliable and efficient identity verification systems in complex and unconstrained environments. By leveraging the dimensionality reduction capability of PCA and the powerful feature extraction and classification ability of CNN, the proposed system demonstrates significant potential in handling the challenges associated with side face recognition. The hybrid approach not only improves recognition accuracy but also enhances computational efficiency, making it suitable for real-world applications. As biometric technology evolves, the integration of such advanced methodologies opens new possibilities for robust security solutions. This section concludes the findings of the research and outlines potential directions for future work to further refine and expand the system's capabilities.

5.1 Conclusion

The proposed hybrid model, which integrates Principal Component Analysis (PCA) and Convolutional Neural Networks (CNN) for side face identification, represents a significant step forward in biometric authentication systems, particularly under constrained conditions where full facial data is unavailable. This method effectively fills a significant gap in the state of facial recognition research by extracting and learning discriminative characteristics from profile views. Despite pose limitations, the model's high recognition accuracy shows great promise for practical application in next-generation technologies like smart surveillance, secure access systems, and human-computer interaction in augmented reality (AR) and virtual reality (VR) settings. Furthermore, in today's linked, AI-driven world, this framework establishes the foundation for biometric solutions that are portable and flexible for use in mobile and edge computing devices. The foundation for flexible and lightweight biometric solutions in mobile and edge computing devices is also laid by this framework, which is becoming more and more important in the connected, AI-driven world of today. Since new technologies require strong and adaptable security measures, this model can be used as a guide to create intelligent systems that can operate in a variety of dynamic environments, significantly advancing biometric and AI-enabled applications. Importantly, the integration of traditional statistical methods like PCA with deep learning architectures exemplifies a hybrid approach that can inspire new research directions focused on computational efficiency, model

interpretability, and robustness in low-data or pose-limited environments. As AI continues to evolve and expand into domains requiring real-time, privacy-preserving biometric verification, models like the one proposed in this study will serve as foundational technologies, bridging the gap between current biometric limitations and the growing demands of future intelligent systems.

- **Pose-Invariant Recognition Capability:** The hybrid PCA-CNN model effectively addresses a major limitation in biometric systems—accurate recognition from non-frontal (side-face) images, which are common in real-world environments like surveillance and mobile usage.
- **Real-World Application Readiness:** Ideal for use in environments where full facial visibility cannot be guaranteed, such as:
 - Smart surveillance (airports, train stations, public events)
 - Wearable devices and AR/VR headsets
 - Autonomous systems (vehicles, drones)
 - Smart home security and mobile authentication
- **Optimized for Edge Computing:** PCA reduces dimensionality, making the model lightweight and fast, suitable for deployment on low-power edge devices (e.g., smartphones, IoT, embedded systems) where real-time processing is required.
- **Hybrid Approach for Enhanced Performance:** Combines the interpretability and efficiency of PCA with the deep feature learning power of CNNs, offering a balance between speed, accuracy, and adaptability.
- **Scalable and Generalizable Framework:** The model can serve as a base architecture for expanding to other constrained biometric scenarios (e.g., partial occlusion, low light, motion blur) and integrating additional modalities.
- **Supports Privacy-Conscious AI Systems:** Enables local, on-device processing, reducing the need to transmit biometric data to centralized servers, supporting privacy-preserving biometric authentication.
- **Foundation for Future Research:** Encourages the development of hybrid and lightweight deep learning solutions for biometric applications where resource constraints and data variability are challenges.
- **Alignment with Emerging Technology Trends:** Contributes to the evolution of AI-driven security systems, human-computer interaction, and context-aware computing, helping meet the rising demands for robust, flexible, and intelligent biometric systems in evolving tech ecosystems

5.2 Impact on the Field

The advancements in side face identification and recognition have significant implications for various applications. Enhanced recognition capabilities contribute to improved security systems, more reliable surveillance, and better human-computer interaction. These improvements also cover the way for advancements in fields such as forensics, where profile face recognition can be crucial.

The integration of side face recognition with other biometric systems opens new avenues for comprehensive biometric solutions. This integration enhances the robustness and reliability of identification systems, making them more versatile and applicable to a broader range of scenarios.

5.3 Future Work

Future work on the side face biometric system using PCA and CNN can focus on several key areas to enhance its effectiveness and applicability. We can consider the following trending areas:

- Edge-Centric Side Face Biometrics for Real-time and Privacy-Preserving Authentication:** Future work could focus on deploying the PCA and CNN-based side face recognition system directly on edge devices. This approach would enable real-time identity verification without the need to transmit sensitive facial data to a central server. Research could explore developing lightweight and computationally efficient versions of the PCA and CNN models suitable for resource-constrained edge devices like smartphones, smart cameras, or embedded systems. This direction would necessitate investigating techniques such as model quantization, pruning, and knowledge distillation to reduce the model size and computational complexity while maintaining acceptable accuracy. Furthermore, exploring hardware acceleration using dedicated neural processing units (NPUs) on edge devices could significantly enhance the system's performance. Addressing challenges related to on-device data storage, power consumption, and maintaining the security and privacy of biometric templates locally would also be critical areas of investigation.
- Fog-Assisted Collaborative Side Face Recognition for Enhanced Scalability and Accuracy:** Future research could investigate a fog computing architecture where edge devices capture side face images and perform initial processing, such as face detection and alignment. Instead of sending raw images to the cloud, these edge devices could extract PCA features locally and transmit these lower-dimensional representations to a nearby fog node. The fog node, with more computational resources, could then perform more complex CNN-based feature extraction and matching against a larger distributed database. This approach could

improve scalability by distributing the computational load and reducing network latency compared to a purely cloud-based system. Moreover, the fog layer could facilitate collaborative learning and model updates across multiple edge devices without centralizing sensitive raw data, enhancing privacy. Future work could explore efficient and secure methods for feature aggregation and matching in the fog layer, as well as strategies for handling data heterogeneity and ensuring system robustness in a distributed environment. Techniques like federated learning could also be explored to collaboratively train the CNN model across the fog nodes.

- **Leveraging GANs for Robust Side Face Recognition in Challenging Conditions:** Future work could explore the use of Generative Adversarial Networks (GANs) to enhance the robustness and accuracy of side face biometric systems, particularly when dealing with challenging conditions. GANs could be employed in several ways: One potential avenue is using GANs for data augmentation. By training GANs to generate synthetic side face images with variations in pose, illumination, occlusion, and image quality, the size and diversity of the training dataset can be significantly increased. This can help to improve the generalization ability of the CNN model and make it more resilient to real-world variations encountered in unconstrained environments. Research could focus on developing GAN architectures specifically tailored for generating realistic and diverse side face images that effectively bridge the gap between synthetic and real data. Another direction is using GANs for domain adaptation. When the training data and testing environments have significant differences (e.g., different camera types or lighting conditions), GANs can be used to learn a mapping between the source and target domains. This can help to reduce the domain gap and improve the performance of the side face recognition system in the target environment without requiring large amounts of labeled data from that environment. Future work could explore novel GAN-based domain adaptation techniques specifically for side face biometrics.

List of Publications

1. Girish Kumar, Dr. Ajay Khushwaha, "A modal for better authentication using hybrid biometrics by adding a side face with an ear" Turkish Journal of Computer and Mathematics Education on Dec-2020, Vol.11 No.03 (2020),2484-2492 (Scopus with SJR 0.218)
2. Girish Kumar, Dr. Balraj Kumar, "An Identification of individuality in hybridize biometrics using profile image with ear and side face- An Auricle" 3rd International Conference on Functional Materials, Manufacturing, and Performances (ICFMMP-2022) on July 29-30 2022, Vol No. 2986 ISSN/ISBN 0094243X/978-073544840-7/1 (Scopus Indexed)
3. Girish Kumar, "Exploring Data Fusion and Feature Learning Techniques to Advance Identity Recognition" 5th International Conference on Recent Advances in Fundamental and Applied Sciences (RAFAS-2024) from 19-20 April 2024, Vol-1 No 1 ISSN/ISBN 978-81-972042-5-8
4. Girish Kumar and Ankush Manocha, "Multimodal Biometric Authentication: A Comprehensive Review of Fusion-Based Approaches" SN Computer Science, Springer. (Status: Communicated)
5. Girish Kumar, Dr. Ankush Manocha,"A Modal for Enhanced Validation Using Hybrid Biometrics by Integrating Side Face and Ear Recognition", African Journal of Biomedical Research, ISSN/ISBN 1119-5096 (Published-Scopus)

List of Patents

1. Girish Kumar, Dr. Ankush Manocha, Ajay Singh, Chakshu Bamotra, “A SMART LOCKER SYSTEM WITH SIDE FACE RECOGNITION FOR SECURE ACCESS “, Application No.20231100194 Published on 13/01/2023
2. Girish Kumar, Amir Rashid “A METHOD AND SYSTEM FOR DUPLET BIOMETRIC VERIFICATION IN LOCKER ACCESS CONTROL”, Application No.202311042369, on 21/07/2023

List of Copyrights

1. Girish Kumar, Dr. Ankush Manocha, "Identification of a person using Auricle a hybrid approach for biometrics" Registration Number: L-149707/2024, Diary Number: 15579/2024-CO/L on 24/06/2024- Indian Patent

Certificate No.253312



**LOVELY
PROFESSIONAL
UNIVERSITY**

Transforming Education Transforming India

Certificate of Presentation

This is to certify that **Dr./Mr./Ms. Girish Kumar** of **Lovely Professional University- Phagwara- India** has presented a paper on **Identification of individuality in hybridize biometrics using profile image with ear and side face- An Auricle** in the **“3rd International Conference on Functional Materials, Manufacturing and Performances (ICFMMP-2022)”** held on **July29-30th, 2022**, organized by **Division of Research and Development, Lovely Professional University, Punjab.**

Date of Issue: 30-08-2022
Place: Phagwara (Punjab), India


Prepared by
(Administrative Officer-Records)




Dr. Hitesh Vasudev
Convener






Dr. Pranav Kumar Prabhakar
Organizing Secretary




Dr. Chander Prakash
Conference Secretary



   	<p>Certificate No. 329274</p>
<p>Certificate of Presentation</p>	
<p>This is to certify that Dr./Mr./Ms. Girish Kumar of Lovely Professional University, Phagwara has given Oral presentation on Exploring Data Fusion and Feature Learning Techniques to Advance Identity Recognition in the 5th International Conference on Recent Advances in Fundamental and Applied Sciences (RAFAS-2024) held from 19th to 20th April 2024, organized by School of Chemical Engineering and Physical Sciences, Lovely Faculty of Technology and Sciences, at Lovely Professional University, Punjab.</p>	
<p>Date of Issue : 20-05-2024 Place : Phagwara (Punjab), India</p>	<p>Prepared by (Administrative Officer-Records)</p>
<p>Organizing Secretary (RAFAS-2024)</p>	<p>Head of Faculty Lovely Professional University</p>

(12) PATENT APPLICATION PUBLICATION (19) INDIA (22) Date of filing of Application :10/01/2023	(21) Application No.202311001949 A (43) Publication Date : 13/01/2023
(54) Title of the invention : A SMART LOCKER SYSTEM WITH SIDE FACE RECOGNITION FOR SECURE ACCESS	<div>(71)Name of Applicant : 1)Lovely Professional University Address of Applicant :Jalandhar- Delhi GT road Phagwara, Punjab, India 144411. Phagwara ----- Name of Applicant : NA Address of Applicant : NA (72)Name of Inventor : 1)KUMAR, Girish Address of Applicant :Lovely Professional University, Delhi Jalandhar GT road Phagwara- 144411. Phagwara ----- --- 2)MANOCHA, Ankush Address of Applicant :Lovely Professional University, Delhi Jalandhar GT road Phagwara- 144411. Phagwara ----- --- 3)SINGH, Ajay Address of Applicant :Lovely Professional University, Delhi Jalandhar GT road Phagwara- 144411. Phagwara ----- --- 4)BAMOTRA, Chakshu Address of Applicant :Bhavan SL Public School, Opp Shivala Bhaiyan, Amritsar, Punjab, India 143001 Phagwara ----- -----</div> <div>(51) International classification :H04N0007180000, G07F0017120000, A61K0036730000, G07C00090000000, H04L0067120000 (86) International Application No :NA Filing Date :NA (87) International Publication No : NA (61) Patent of Addition to Application Number :NA Filing Date :NA (62) Divisional to Application Number :NA Filing Date :NA</div>
(57) Abstract :	

[illegible]

References

1. Philips P.J., Grother P., Micheals R.J., Blackburn D.M., Tabassi E. and Bone J.M. (2002) "FRVT 2002: Overview and Summary", available from <http://www.frvt.org/FRVT2002/documents.htm>.
2. Jain A.K., Nandakumar K., Lu X. and Park U. (2004) "Integrating Faces, Fingerprints and Soft Biometric Traits for User Recognition", In *Proceedings of ECCV International Workshop on Biometric Authentication (BioAW)*, Springer, Vol. LNCS 3087, pp. 259-269.
3. Jain A.K., Bolle R. and Pankanti S. (1999) "Biometrics: Personal Identification in Networked Society", Kluwer Academic Publishers.
4. Kumar A., Wong D.C.M., Shen H.C. and Jain A.K. (2003) "Personal Verification Using Palmprint and Hand Geometry Biometric", In *Proceedings of Fourth International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA)*, pp. 668-678.
5. Sanchez-Avila C., Sanchez-Reillo R. and de Martin-Roche D. (2002) "Iris-based biometric recognition using dyadic wavelet transform", *IEEE Aerosp. Electron. Syst. Mag.*, Vol. 17, pp. 3-6.
6. Uludag U., Pankanti S., Prabhakar S. and Jain A.K. (2004) "Biometric Cryptosystems: Issues and Challenges", *Proceedings of the IEEE, Issue on Enabling Security Technologies for Digital Rights Management*, Vol. 92, No. 6.
7. Jain A.K. and Pankanti S. (2001) "Biometrics Systems: Anatomy of Performance", *IEICE Transactions Fundamentals*, Vol. E84-D, No. 7, pp. 788-799.
8. Sarvesh Makthal and Arun Ross(2003) "SYNTHESIS OF IRIS IMAGES USING MARKOV RANDOM FIELDS" 13th european signal processing conference (EUSIPCO) September 2005.
9. Ross A. and Govindarajan (2005) "Feature level fusion using hand and face biometrics", In *Proc. of SPIE Conference on Biometric Technology for Human Identification II*, pp. 196-204.
10. Uludag U. and Jain A.K. (2004) "Attacks on biometric systems: a case study in fingerprints", in *Proc. SPIE-EI Security, Steganography and Watermarking of Multimedia Contents VI*, San Jose, CA, pp. 622-633.
11. Yip A. and Sinha P. (2002) "Role of color in face recognition", *Perception*, Vol. 31, pp. 995-1003.

12. Maio D., Maltoni D., Cappelli R., Wayman J.L. and Jain A.K. (2002) "FVC2002: Fingerprint Verification Competition", *Proc. International Conference on Pattern Recognition (ICPR)*, Quebec City, Canada, pp. 744-747.
13. You, Kong W.K., Zhang D. and Cheung K.H. (2004) "On Hierarchical Palm print Coding With Multiple Features for Personal Identification in Large Databases", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 2, pp. 234-243.
14. Arbab-Zavar, B., and Nixon, M., Robust log-Gabor filter for ear biometrics. In: *19th International Conference on Pattern Recognition*, pp. 1–4, 2008. <https://doi.org/10.1109/ICPR.2008.4761843>.
15. Arbab-Zavar, B., Nixon, M., and Hurley, D., On model-based analysis of ear biometrics. In: *First IEEE International Conference on Biometrics: Theory Applications, and Systems*, pp. 1–5, 2007. <https://doi.org/10.1109/BTAS.2007.4401937>.
16. Attarchi, S., Faez, K., and Rafiei, A., A new segmentation approach for ear recognition. In: *International Conference on Advanced Concepts for Intelligent Vision Systems*, pp. 1030– 1037, 2008. https://doi.org/10.1007/978-3-540-88458-3_93.
17. Badrinath, G., and Gupta, P., Feature level fused ear biometric system. In: *Seventh International Conference on Advances in Pattern Recognition (ICPR)*, pp. 197–200, 2009. <https://doi.org/10.1109/ICAPR.2009.27>.
18. Basit, A., and Shoaib, M., A human ear recognition method using nonlinear curvelet feature subspace. *Int. J. Comput. Math.* 91(3):616–624, 2014. <https://doi.org/10.1080/00207160.2013.800194>.
19. Benzaoui, A., Hadid, A., and Boukrouche, A., Ear biometric recognition using local texture descriptors. *J. Electron. Imaging* 23(5):053,008–053,008, 2014. <https://doi.org/10.1117/1.JEI.23.5.053008>.
20. Benzaoui, A., Hezil, N., and Boukrouche, A., Identity recognition based on the external shape of the human ear. In: *International Conference on Applied Research in Computer Science and Engineering*, pp. 1–5, 2015a. <https://doi.org/10.1109/ARCSE.2015.7338129>.
21. Bertillon, A., *La photographie judiciaires: avec un-appendices la classification et l 'identification anthropome' triques*, 1890.
22. Burge, M., and Burger, W., Ear biometrics. *Biometrics: Personal Identification in Networked Society* pp. 273–286, https://doi.org/10.1007/0-306-47044-6_13, 1996.
23. Burge, M., and Burger, W., Ear biometrics for machine vision. In: *21st Workshop of the Austrian Association for Pattern Recognition*, pp. 275–282, 1997.
24. Burger, M., and Burger, W., Ear biometrics in computer vision. In: *International Conference on Pattern Recognition*, pp. 822– 826, 2000. <https://doi.org/10.1109/ICPR.2000.906202>.

25. Bustard, J., and Nixon, M., *Toward unconstrained ear recognition from two-dimensional images*. *IEEE Trans. Syst. Man Cybern. Syst. Hum.* 40(3):486–494, 2010. <https://doi.org/10.1109/TSMCA.2010.2041652>.
26. Chan, T. S., and Kumar, A., *Reliable ear identification using 2-D quadrature filters*. *Pattern Recogn. Lett.* 33(14):1870–1881, 2012. <https://doi.org/10.1016/j.patrec.2011.11.013>.
27. Chang, K., Bowyer, K., Sarkar, S., and Victor, B., *Comparison and combination of ear and face images in appearance-based biometrics*. *IEEE Trans. Pattern Anal. Mach. Intell.* 25(9):1160–1165, 2003. <https://doi.org/10.1109/TPAMI.2003.1227990>.
28. Choras, M., *Ear biometrics based on geometrical feature extraction*. *ELCVIA Electron. Lett. Computer Vision Image Anal.* 5(3):84–95, 2005. <https://doi.org/10.5565/rev/elcvia.108>.
29. Choras, M., *Perspective methods of human identification: ear biometrics*. *Opto-Electron. Rev.* 16(1):85–96, 2008. <https://doi.org/10.2478/s11772-007-0033-5>.
30. Choras, M., and Choras, R., *Geometrical algorithms of ear contour shape representation and feature extraction*. In: *Sixth International Conference on Intelligent Systems Design and Applications (ISDA)*, Vol. 2, pp. 451–456, 2006. <https://doi.org/10.1109/ISDA.2006.253879>.
31. De Marsico, M., Michele, N., and Riccio, D., *HERO: human ear recognition against occlusions*. In: *IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 178–183, 2010. <https://doi.org/10.1109/CVPRW.2010.5544623>.
32. Dewi, K., and Yahagi, T., *Ear photo recognition using scale-invariant key points*. In: *Proceedings of the Second IASTED Inter-national Conference on Computational Intelligence*, pp. 253–258, 2006.
33. Guo, Y., and Xu, Z., *Ear recognition using a new local matching approach*. In: *15th IEEE International Conference on Image Processing*, pp. 289–292, 2008. <https://doi.org/10.1109/ICIP.2008.4711748>.
34. Hai-Long, Z., and Zhi-Chun, M., *Combining wavelet transform and orthogonal centroid algorithm for ear recognition*. In: *2nd IEEE International Conference on Computer Science and Information Technology (ICCSIT)*, pp. 228–231, 2009. <https://doi.org/10.1109/ICCSIT.2009.5234392>.
35. Houcine, B., Hakim, D., Amir, B., and Hani, B., *Ear recognition based on multi-bags-of features histogram*. In: *3Rd International Conference on Control, Engineering & Information Technology (CEIT)*, Vol. 2015, pp. 1–6, 2015. <https://doi.org/10.1109/CEIT.2015.7232997>.
36. Hurley, D. J., Nixon, M., and Carter, J., *Force field energy functional for image feature extraction*. *Image Vis. Comput.* 20(5-6):311–317, 2002. [https://doi.org/10.1016/S0262-8856\(02\)00003-3](https://doi.org/10.1016/S0262-8856(02)00003-3).
37. Iannarelli, A., *Ear identification* Paramount Publishing, ISBN: Paramount Publishing, 1989.
38. Kisku, D., Mehrotra, H., Gupta, P., and Sing, J., *SIFT-based ear recognition by fusion of detected key points from color similarity slice regions*. In: *International Conference on Advances in Computational Tools for Engineering Applications*, pp. 380–385, 2009. <https://doi.org/10.1109/ACTEA.2009.5227958>.

39. Kumar, A., and Wu, C., *Automated human identification using ear imaging*. *Pattern Recogn.* 45(3):956–968, 2012. <https://doi.org/10.1016/j.patcog.2011.06.005>.
40. Kumar, A., and Zhang, D., *Ear authentication using log-Gabor wavelets*. *Defense and Security Symposium* pp. 65,390A– 65,390A, <https://doi.org/10.1117/12.720244>, 2007.
41. Kumar, A., Hanmandlu, M., Kuldeep, M., and Gupta, H., *Automatic ear detection for online biometric applications*. In: *Third National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG)*, pp. 146–149, 2011. <https://doi.org/10.1109/NCVPRIPG.2011.69>.
42. Meraoumia, A., Chitroub, S., and Bouridane, A., *An auto-mated ear identification system using Gabor filter responses*. In: *13th International Conference on New Circuits and Systems (NEWCAS)*, pp. 1–4, 2015. <https://doi.org/10.1109/NEWCAS.2015.7182085>.
43. Moreno, B., Sanchez, A., and Ve'lez, J., *On the use of outer ear images for personal identification in security applications*. In: *33rd Annual International Carnahan Conference on Security Technology*, pp. 469–476, 1999. <https://doi.org/10.1109/CCST.1999.797956>.
44. Mu, Z., Yuan, L., Xu, Z., Xi, D., and Qi, S., *Shape and structural feature based ear recognition*. In: *Advances in Biometric Person Authentication*, pp. 663–670, 2004. https://doi.org/10.1007/978-3-540-30548-4_76.
45. Nanni, L., and Lumini, A., *Fusion of color spaces for ear authentication*. *Pattern Recogn. Lett.* 42(9):1906–1913, 2009. <https://doi.org/10.1016/j.patcog.2008.10.016>.
46. Pflug, A., Busch, C., and Ross, A., *2D ear classification based on unsupervised clustering*. In: *2014 IEEE International Joint Conference on Biometrics (IJCB)*, pp. 1–8, 2014a. <https://doi.org/10.1109/BTAS.2014.6996239>.
47. Pflug, A., Paul, P., and Busch, C., *A comparative study on texture and surface descriptors for ear biometrics*. In: *International Carnahan Conference on Security Technology (ICCST)*, pp. 1–6, 2014b. <https://doi.org/10.1109/ICCST.2014.6996239>.
48. Prakash, S., and Gupta, P., *An efficient ear recognition technique invariant to illumination and pose*. *Telecommun. Syst.* 52(3):1435–1448, 2013. <https://doi.org/10.1007/s11235-011-9621-2>.
49. Rahman, M., Islam, M. R., Bhuiyan, N., Ahmed, B., and Islam, A., *Person identification using ear biometrics*. *Int. J. Comput. Integr. Manuf.* 15(2):1–8, 2007.
50. Sana, A., Gupta, P., and Purkait, R., *Ear biometrics: a new approach*. *Advances in Pattern Recognition* pp. 46–50, https://doi.org/10.1142/9789812772381_0006, 2007.
51. Victor, B., Bowyer, K., and Sarkar, S., *An evaluation of face and ear biometrics*. In: *16Th International Conference on Pattern Recognition, Vol. 1*, pp. 429–432, 2002. <https://doi.org/10.1109/ICPR.2002.1044746>.

52. Xiaoyun, W., and Weiqi, Y., *Human ear recognition based on block segmentation*. In: *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery*, pp. 262–266, 2009. <https://doi.org/10.1109/CYBERC.2009.5342143>.
53. Zhang, H. J., Mu, Z. C., Qu, W., Liu, L. M., and Zhang, C. Y., *A novel approach for ear recognition based on ICA and RBF network*. In: *2005 International Conference on Machine Learning and Cybernetics*, Vol. 7, pp. 4511–4515, 2005. <https://doi.org/10.1109/ICMLC.2005.1527733>.
54. Zhou, Y., and Zaferiou, S., *Deformable models of ears in the- wild for alignment and recognition*. In: *12Th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017)*, pp. 626–633, 2017. <https://doi.org/10.1109/FG.2017.79>.
55. *An introduction to Biometric Recognition*, Anil K.Jain, Arun Ross, Salil Prabhakar, *IEEE Transactions on Circuits And System For Video Technology*, Vol 14, No. 1 Jan-2004
56. https://en.wikipedia.org/wiki/Facial_recognition_system, *The History of Information Security*, 1st Edition
57. A.S. Tolba, A.H. EL-Baz and A.A. El-Harby, *Face Recognition: A Literature Review*, *International Journal of Signal Processing* 2;2 2006, doi=10.1.1.307.5530
58. Z. Liposcak and S. Loncaric, "A scale-space approach to face recognition from profiles," in *Proceedings of the 8th International Conference on Computer Analysis of Images and Patterns*, Vol. 1689, *Lecture Notes In Computer Science*. London, UK: Springer- Verlag, 1999, pp.243-250 doi= 10.1007/3-540-48375-6_30
59. *Multimodal Biometric Recognition using Human Ear and Profile Face* Partha Pratim Sarangi, B. S. P Mishra† and Sachidanada Dehuri, *School of Computer Engineering, KIIT University, Bhubaneswar, Odisha, India, Department of ICT, FM University, Balasore, Odisha, India. 4th Int'l Conf. on Recent Advances in Information Technology | RAIT-2018*
60. *A Study on Human Recognition Using Auricle and Side View Face Images* Susan El-Naggar, Ayman Abaza and Thirimachos Bourlai Springer International Publishing AG 2018 P. Karampelas and T. Bourlai (eds.), *Surveillance in Action, Advanced Sciences and Technologies for Security Applications* ,https://doi.org/10.1007/978-3-319-68533-5_4
61. *A Multimodal Biometric Authentication System Using Ear and Face* Mostafa Akhavansaffar *, Ali Nakhaei , Mostafa Mokhtari Ardakan Department of ICT Engineering, Payame Noor Universtiy(PNU), Tehran, I. R of Iran Manuscript submitted August 2, 2017; accepted November 5, 2017.doi: 10.17706/jcp.13.7. 876-888
62. *Learning Pose-Aware Models for Pose-Invariant Face Recognition in the Wild* Iacopo Masi, Feng-ju Chan, Jongmoo Choi, Shai Harel, Jungyeon Kim, KangGeon Kim, Jatuporn Leksut, Stephen Rawls, Yue Wu, Tal Hassner, Wael AbdAlmageed, Gerard Medioni, Louis-Philippe Morency, Prem Natarajan, Ram Nevatia DOI 10.1109/TPAMI.2018.2792452, *IEEE Transactions on Pattern Analysis and Machine Intelligence*.

63. *HUMAN FACE PROFILE RECOGNITION BY COMPUTER* CHYUAN JY Wu and JUN S. HUANG* *Pattern Recognition*, Vol. 23, No. 3~4, pp. 255-259, 1990 Printed in Great Britain,
64. *Side-View Facial Recognition: Major Issue in Face Recognition*, Harshit Patel¹, Ria Yadav² ¹ B.Tech (CSE), 4th Year (1503510033), BBDIT Ghaziabad (035), Dr. APJ Abdul Kalam Technical University, *International Journal for Research in Applied Science & Engineering Technology (IJRASET)* Volume 6 Issue XI, Nov 2018
65. *MULTIMODAL RECOGNITION BASED ON FACE AND EAR*, LI YUAN, ZHI-CHUN MU, XIAO-NA XU, School of Information Engineering, University of Science and Technology Beijing, Beijing, 100083, China, *Proceedings of the 2007 International Conference on Wavelet Analysis and Pattern Recognition*, Beijing, China, 2-4 Nov. 2007
66. *Multimodal biometrics system based on face profile and ear* Iman S. Youssef Ayman A. Abaza Mohamed E. Rasmy and Ahmed M. Badawi, *Systems and Biomedical Engineering*, Cairo University, Egypt; West Virginia High Tech Foundation, Fairmont, USA
67. *Biometrics recognition using deep learning: a survey*, Shervin M., Amirali A., Su Hang, Muhammed Bennamoun, D. Zangin *Artificial Intelligence Review*, Volume 56, pages 8647-8695 (2023)
68. *Towards High-Fidelity Nonlinear 3D Face Morphable Model* by Luan Tran, Feng Liu, Xiaoming Liu; *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2019, pp. 1126-1135
69. "Force field feature extraction for ear biometrics" by David J. Hurley, Mark S. Nixon*, John N. Carter in *Computer Vision and Image Understanding* in 10 November 2004 with doi:10.1016/j.cviu.2004.11.001
70. Utsav Prabhu, Jingu Heo, and Marios Savvides. *Unconstrained pose-invariant face recognition using 3d generic elastic models*. *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, 33:1952 – 1961, 11 2011. doi: 10.1109/TPAMI. 2011.123.
71. Akshay Asthana, Tim K. Marks, Michael J. Jones, Kinh H. Tieu, and M. V. Rohith. *Fully automatic pose-invariant face recognition via 3d pose normalization*. *2011 International Conference on Computer Vision*, pages 937–944, 2011.
72. V. Blanz and T. Vetter. *Face recognition based on fitting a 3d morphable model*. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 25(9):1063–1074, 2003. doi: 10.1109/TPAMI.2003.1227983.
73. David Hoon, Sandor Szedmak, and John Shawe-Taylor. *Canonical correlation analysis: An overview with application to learning methods*. *Neural computation*, 16:2639–64, 01 2005. doi: 10.1162/0899766042321814.
74. Abhishek Sharma and David Jacobs. *Bypassing synthesis: Pls for face recognition with pose, low-resolution and sketch*. volume 1, pages 593 – 600, 07 2011. doi: 10.1109/CVPR.2011.5995350.

75. *Annan Li, Shiguang Shan, Xilin Chen, and Wen Gao. Maximizing intra-individual correlations for face recognition across pose differences. pages 605–611, 06 2009. doi: 10.1109/CVPR.2009.5206659.*
76. *Abhishek Sharma, Murad Al Haj, Jonghyun Choi, Larry S. Davis, and David W. Jacobs. Robust pose invariant face recognition using coupled latent space discriminant analysis. Comput. Vis. Image Underst., 116:1095–1110, 2012.*
77. *Simon J.D. Prince, James H. Elder, Jonathan Warrell, and Fatima M. Felisberti. Tied factor analysis for face recognition across large pose differences. IEEE Transactions on Pattern Analysis and Machine Intelligence, 30(6):970–984, 2008. doi: 10.1109/TPAMI.2008.48.*
78. *P. Jonathon Phillips, Hyeonjoon Moon, Syed Rizvi, and Patrick Rauss. The ferret evaluation methodology for face-recognition algorithms. Pattern Analysis and Machine Intelligence, IEEE Transactions on, 22:1090 – 1104, 10 2000. doi: 10.1109/34.879790.*
79. *Simon Prince, Peng Li, Yun Fu, Umar Mohammed, and James Elder. Probabilistic models for inference about identity. IEEE Transactions on Pattern Analysis and Machine Intelligence, 34(1):144–157, 2012. doi: 10.1109/TPAMI.2011.104.*
80. *Neeraj Kumar, Alexander Berg, Peter Belhumeur, and Shree Nayar. Attribute and simile classifiers for face verification. pages 365 – 372, 11 2009. doi: 10.1109/ICCV. 2009.5459250.*
81. *Hieu Nguyen and Li Bai. Cosine similarity metric learning for face verification. volume 6493, pages 709–720, 11 2010. ISBN 978-3-642-19308-8. doi: 10.1007/ 978-3-642-19309-5_55.*
82. *Qiong Cao, Yiming Ying, and Peng Li. Similarity metric learning for face recognition. 2013 IEEE International Conference on Computer Vision, pages 2408–2415, 2013.*
83. *Jiwen Lu, Junlin Hu, and Yap-Peng Tan. Discriminative deep metric learning for face and kinship verification. IEEE Transactions on Image Processing, 26(9): 4269–4282, 2017. doi: 10.1109/TIP.2017.2717505.*
84. *Gary B. Huang, Honglak Lee, and Erik G. Learned-Miller. Learning hierarchical representations for face verification with convolutional deep belief networks. 2012 IEEE Conference on Computer Vision and Pattern Recognition, pages 2518–2525, 2012.*
85. *Matthieu Guillaumin, Jakob J. Verbeek, and Cordelia Schmid. Is that you? Metric learning approaches for face identification. 2009 IEEE 12th International Conference on Computer Vision, pages 498–505, 2009.*
86. *Martin Köstinger, Martin Hirzer, Paul Wohlhart, Peter M. Roth, and Horst Bischof. Large scale metric learning from equivalence constraints. 2012 IEEE Conference on Computer Vision and Pattern Recognition, pages 2288–2295, 2012.*
87. *Ge Wen, Huaguan Chen, Deng Cai, and Xiaofei He. Improving face recognition with domain adaptation. Neurocomputing, 287:45–51, 2018. ISSN 0925-2312. doi:*

- <https://doi.org/10.1016/j.neucom.2018.01.079>. URL <https://www.sciencedirect.com/science/article/pii/S0925231218301127>
88. Dong Chen, Xudong Cao, Fang Wen, and Jian Sun. *Blessing of dimensionality: High-dimensional feature and its efficient compression for face verification*. 2013 IEEE Conference on Computer Vision and Pattern Recognition, pages 3025–3032, 2013.
 89. Karen Simonyan, Omkar M. Parkhi, Andrea Vedaldi, and Andrew Zisserman. *Fisher vector faces in the wild*. In *British Machine Vision Conference*, 2013.
 90. Haoxiang Li, Zhe Lin, Jonathan Brandt, and Jianchao Yang. *Probabilistic elastic matching for pose variant face verification*. pages 3499–3506, 06 2013. doi: 10.1109/CVPR.2013.449.
 91. Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato, and Lior Wolf. *Deepface: Closing the gap to human-level performance in face verification*. 2014 IEEE Conference on Computer Vision and Pattern Recognition, pages 1701–1708, 2014.
 92. Yi Sun, Xiaogang Wang, and Xiaoou Tang. *Deeply learned face representations are sparse, selective, and robust*. 12 2014. doi: 10.1109/CVPR.2015.7298907.
 93. Florian Schroff, Dmitry Kalenichenko, and James Philbin. *Facenet: A unified embedding for face recognition and clustering*. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pages 815–823, 2015.
 94. Paul A. Viola and Michael J. Jones. *Rapid object detection using a boosted cascade of simple features*. *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*. CVPR 2001, 1:I–I, 2001.
 95. Cha Zhang and Zhengyou Zhang. *A survey of recent advances in face detection*. Technical Report MSR-TR-2010-66, June 2010.
 96. Cha Zhang and Zhengyou Zhang. *A survey of recent advances in face detection*. Technical Report MSR-TR-2010-66, June 2010.
 97. Zhanpeng Zhang, Ping Luo, Chen Change Loy, and Xiaoou Tang. *Facial landmark detection by deep multi-task learning*. 09 2014. ISBN 978-3-319-10598-7. doi: 10.1007/978-3-319-10599-4_7.
 98. Alem Fitwi, Meng Yuan, Seyed Yahya Nikouei, and Yu Chen. *Minor privacy protection by real-time children identification and face scrambling at the edge*. *EAI Endorsed Trans. Security Safety*, 7:e3, 2020.
 99. Tanoy Debnath, Md. Mahfuz Reza, Anichur Rahman, Amin Beheshti, Shahab S. Band, and Hamid Alinejad-Rokny. *Four-layer convnet to facial emotion recognition with minimal epochs and the significance of data diversity*. *Scientific Reports*, 12: 1–18, 2022. ISSN 2045-2322. doi: 10.1038/s41598-022-11173-0
 100. Jesus Olivares-Mercado, Karina Toscano-Medina, Gabriel Sanchez-Perez, Mariko Nakano Miyatake, Hector Perez-Meana, and Luis Carlos Castro-Madrid. *Face recognition based on texture descriptors*. In Ricardo Lopez-Ruiz, editor, *From Natural to Artificial Intelligence*, chapter 6.

- IntechOpen, Rijeka, 2018. doi: 10.5772/intechopen.76722. URL: <https://doi.org/10.5772/intechopen.76722>*
101. Tibor Trnovszký, Patrik Kamencay, Richard Orjeseck, Miroslav Benco, and Peter Sykora. *Animal recognition system based on convolutional neural network. Advances in Electrical and Electronic Engineering, 15:517–525, 2017.*
 102. Bilel Ameer, Sabeur Masmoudi, Amira Guidara Derbel, and Ahmed Ben Hamida. *Fusing gabor and lbp feature sets for knn and src-based face recognition. 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), pages 453–458, 2016.*
 103. Özgür Kaplan and Ediz Saykol. *Comparison of support vector machines and deep learning for vehicle detection. 11 2018.*
 104. Abhishek Bansal, Kapil Mehta, and Sahil Arora. *Face recognition using pca and lda algorithm. In Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies, ACCT '12, page 251–254, USA, 2012. IEEE Computer Society. ISBN 9780769546407. doi: 10.1109/ACCT.2012.52. URL <https://doi.org/10.1109/ACCT.2012.52>.*
 105. Musab Coşkun, Ayşegül Uçar, Özal Yildirim, and Yakup Demir. *Face recognition based on convolutional neural network. In 2017 International Conference on Modern Electrical and Energy Systems (MEES), pages 376–379, 2017. doi: 10.1109/MEES.2017.8248937.*
 106. Patrik Kamencay, Miroslav Benco, Tomas Mizdos, and Roman Radil. *A new method for face recognition using convolutional neural network. Advances in Electrical and Electronic Engineering, 15:663–672, 2017.*
 107. Dabiah Alboaneen, Hua Tianfield, and Yan Zhang. *Glowworm swarm optimization for training multi-layer perceptrons. pages 131–138, 12 2017. doi: 10.1145/3148055.3148075.*
 108. Imed Bouchrika, "A Survey of Using Biometrics for Smart Visual Surveillance: Gait Recognition", December 2017, DOI: 10.1007/978-3-319-68533-5_1 In book: *Surveillance in Action*.
 109. Mróz-Gorgo 'n, B.; Wodo, W., Andrych, A.; Caban-Piaskowska, K., Kozyra, C. *Biometrics Innovation and Payment Sector Perception. Sustainability 2022, 14, 9424. <https://doi.org/10.3390/su14159424>*
 110. Wikipedia. *Biometrics. <http://en.wikipedia.org/wiki/Biometrics>*
 111. A. K. Jain, R. Bolle, and S. Pankanti (eds.). *Biometrics: Personal Identification in Networked Society. Kluwer, New York, 1998.*
 112. Li YangLi YangKathy WintersKathy WintersJoseph KizzaJoseph Kizza, "Biometrics education with hands-on labs", Conference: *Proceedings of the 46th Annual Southeast Regional Conference, 2008, Auburn, Alabama, March 28-29, 2008, DOI: 10.1145/1593105.1593111*
 113. Norman, Jeremy. "Woodrow Bledsoe Originates of Automated Facial Recognition." *Jeremy Norman's History of Information. Updated December 30 (2020).*
 114. Bledsoe, Woody. "Automated Reasoning: Essays in Honor of." (1991).

115. Muhammad, Hashiru Isiaka, Kabir Ibrahim Musa, Mustapha Lawal Abdulrahman, Abdullahi Abubakar, Kabiru Umar, and Abdulhakeem Ishola. "Enhancing detection performance of face recognition algorithm using PCA-faster R-CNN." *European Journal of Electrical Engineering and Computer Science* 5, no. 3 (2021): 9-16.
116. Suganthi, S. T., Mohamed Uvaze Ahamed Ayoobkhan, Nebojsa Bacanin, K. Venkatachalam, Hubálovský Štěpán, and Trojovský Pavel. "Deep learning model for deep fake face recognition and detection." *PeerJ Computer Science* 8 (2022): e881.
117. Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., ... & Farhan, L. (2021). Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. *Journal of big Data*, 8, 1-74.
118. Onur Can Kurban, Tülay Yildirim, " A comparative analysis of multi-biometrics performance in human and action recognition using silhouette thermal-face and skeletal data" , *Neural Networks*, Volume 170, 2024, Pages 1-17, ISSN 0893-6080, <https://doi.org/10.1016/j.neunet.2023.10.016>.
119. Anshul Mahajan, Sunil K. Singla, "DeepBio: A Deep CNN and Bi-LSTM Learning for Person Identification Using Ear Biometrics", *CMES - Computer Modeling in Engineering and Sciences*, Volume 141, Issue 2, 2024, Pages 1623-1649, ISSN 1526-1492, <https://doi.org/10.32604/cmes.2024.054468>.
120. Shuyi Li, Lunke Fei, Bob Zhang, Xin Ning, Lifang Wu, "Hand-based multimodal biometric fusion: A review", *Information Fusion*, Volume 109, 2024, ISSN 1566-2535, <https://doi.org/10.1016/j.inffus.2024.102418>.
121. Hosam El-Sofany, Belgacem Bouallegue, Yasser M. Abd El-Latif, " A proposed biometric authentication hybrid approach using iris recognition for improving cloud security", *Heliyon*, Volume 10, Issue 16, 2024, ISSN 2405-8440, <https://doi.org/10.1016/j.heliyon.2024.e36390>.
122. Wanchao Li, Zhuangzhuang Du, Xianbao Xu, Zhuangzhuang Bai, Jie Han, Meng Cui, Daoliang Li, "A review of aquaculture: From single modality analysis to multimodality fusion", *Computers and Electronics in Agriculture*, Volume 226, 2024, ISSN 0168-1699, <https://doi.org/10.1016/j.compag.2024.109367>
123. J. Bhuvana, Amit Barve, Shah Pradeep Kumar, Sukanya Dikshit, "Image sensor fusion for multimodal biometric recognition in mobile devices", *Measurement: Sensors*, Volume 36, 2024, ISSN 2665-9174, <https://doi.org/10.1016/j.measen.2024.101309>.
124. Shreyansh Sharma, Anil Saini, Santanu Chaudhury, "Multimodal biometric user authentication using improved decentralized fuzzy vault scheme based on Blockchain network", *Journal of Information Security and Applications*, Volume 82, 2024, ISSN 2214-2126, <https://doi.org/10.1016/j.jisa.2024.103740>.
125. Dilip Kumar Vallabhadas, Mulagala Sandhya, Sudireddy Dinesh Reddy, Davala Satwika, Gatram Lakshmi Prashanth, "Biometric template protection based on a cancelable convolutional neural

- network over iris and fingerprint ", Biomedical Signal Processing and Control, Volume 91, 2024, ISSN 1746-8094, <https://doi.org/10.1016/j.bspc.2024.106006>.*
126. *Reem Alrawili, Ali Abdullah S. AlQahtani, Muhammad Khurram Khan, "Comprehensive survey: Biometric user authentication application, evaluation, and discussion" ,Computers and Electrical Engineering, Volume 119, Part A, 2024, ISSN 0045-7906, <https://doi.org/10.1016/j.compeleceng.2024.109485>.*
 127. *Vipul Vekariya, Manish Joshi, Sukanya Dikshit, S.K. Manju bargavi, "Multi-biometric fusion for enhanced human authentication in information security", Measurement: Sensors, Volume 31, 2024, ISSN 2665-9174, <https://doi.org/10.1016/j.measen.2023.100973>.*
 128. *Li Wan, Kechen Liu, Hanan Abdullah Mengash, Nuha Alruwais, Mesfer Al Duhayyim, K. Venkatachalam, "Deep learning-based photoplethysmography biometric authentication for continuous user verification ", Applied Soft Computing, Volume 156, 2024, ISSN 1568-4946, <https://doi.org/10.1016/j.asoc.2024.111461>.*
 129. *Manocha, A., Singh, R. An intelligent monitoring system for indoor safety of individuals suffering from Autism Spectrum Disorder (ASD). J Ambient Intell Human Comput 14, 15793–15808 (2023). <https://doi.org/10.1007/s12652-019-01277-3>.*