# Multimodal Biometric Authentication System

A thesis submitted to the

***UPES***

For the award of

***Doctor of Philosophy***

In

*Computer Science & Engineering*

By

Sandeep Pratap Singh

March 2025

Supervisor

Dr. Shamik Tiwari

School of Computer Science (SOCS)

UPES

Dehradun, 248007: Uttarakhand, India

# Multimodal Biometric Authentication System

A thesis submitted to

***UPES***

For the award of

***Doctor of Philosophy***

In

*Computer Science & Engineering*

By

Sandeep Pratap Singh

(SAP ID: 500064224)

March 2025

Supervisor

Dr. Shamik Tiwari

Professor, School of Computer Science, UPES Dehradun

School of Computer Science (SOCS)

UPES

Dehradun, 248007, Uttarakhand, India

## DECLARATION

I declare that the thesis entitled **"Multimodal Biometric Authentication System"** has been prepared by me under the guidance of Dr. Shamik Tiwari, Former Professor, School of computer science, UPES, Dehradun, Currently, Dean & Professor School of Computer Science & Engineering IILM University, Gurugram. No part of this thesis has formed the basis for the award of any degree or fellowship previously.

**Sandeep Pratap Singh**

**School of Computer Science**

**UPES, Dehradun-248007, Uttarakhand**

UPES
UNIVERSITY OF TOMORROW

Great Place To Work Certified MAR 2021–FEB 2022 INDIA

## CERTIFICATE

I certify that Sandeep Pratap Singh has prepared his thesis entitled "**Multimodal Biometric Authentication System**", for the award of PhD degree of the UPES Dehradun, under my guidance. He has carried out the work at the School of Computer Science, UPES Dehradun.

**Supervisor**

13/3/25

**Dr. Shamik Tiwari**
**Professor ,School of Computer Science, UPES Dehradun**
**Currently, School of Computer Science & Engineering IILM University, Gurugram**
**Date:**

Energy Acres: Bidholi Via Prem Nagar, Dehradun - 248 007 (Uttarakhand), India T: +91 1352770137, 2776053/54/91, 2776201,9997799474 F: +91 1352776090/95
Knowledge Acres: Kandoli Via Prem Nagar, Dehradun - 248 007 (Uttarakhand), India T: +91 8171979021/2/3, 7060111775

## ABSTRACT

Biometric qualities have attracted a lot of study interest over the last few decades. Some traits, such as face and fingerprint, as well as iris, are in recent years the most widely investigated biometric traits in a variety of applications. However, as newer strategies for imitating such features emerge, modalities that are invulnerable to stealth or spoofing attacks are required. This allowed a new biometric trait, the electrocardiogram (ECG), to gain momentum, which is linked with medical diagnosis and is highly resistant to attacks due to its hidden nature and inherent liveness information. But Unimodal biometric systems attached with some demerits such as Noise in Data ,variation in same class, similarity in different class and more vulnerable to attacks . To counteract these flaws of unimodal systems (single biometric traits), multimodal biometric system by combining different biometrics features is required. Multimodal with ECG as one of the traits is the area we are exploring.As liveness detection of subject is not available for most of the modalities so it also need modality to support liveness of subject. It evaluate and discuss existing works in Multimodal biometrics, as well as its proposed methodologies, datasets. The information gathered is utilised to present advancement of ECG biometrics in a multimodal environment.

In the first study, shortcomings of the unimodal system were addressed by the introduction of multimodal biometric systems. The use of multimodal systems increased the biometric system's overall recognition rate. A new degree of fusion known as an intelligent Dual Multimodal Biometric Authentication Scheme has been established.In the suggested study two multimodal biometric systems are developed by combining three uni-model biometric systems namely ECG, Sclera and fingerprint. The sequential model biometric system is developed based on WOA-ANN. The parallel model biometric system is developed by based on SSA-DBN. The suggested plan makes use of the highest TPR, FPR, and accuracy rates.

In the second study, to enhance the accuracy and security of Biometric authentication systems, the work proposes a 90% confidence interval hybrid model

that integrates Hyper parameter Optimization-Adaptive Neuro-Fuzzy Inference System (HPO-ANFIS) Parallel and Hyper parameter Optimization-Convolutional Neural Network (HPO-CNN) Sequential techniques. This hybrid model aims to address the challenges of feature selection, hyper parameter optimization, and classification in dual multimodal biometric authentication. The optimisation process improves the overall performance of the authentication system, including accuracy, precision, recall, F1 score, and specificity. A key aspect of the proposed hybrid model is the incorporation of a 90% confidence interval, which ensures a reliable and statistically significant evaluation of its performance.
Keywords: Multimodal Biometric Authentication System, Electro cardio graph (ECG), Sclera, Fingerprint, Hyper parameter Optimization-Adaptive Neuro-Fuzzy Inference System (HPO-ANFIS), Hyper parameter Optimization-Convolutional Neural Network (HPO-CNN), Whale-optimization-algorithm-based artificial neural network (WOA-ANN), Salp-swarm-algorithm-based deep belief network (SSA-DBN)

## ACKNOWLEDGEMENT

I wish to extend my heartfelt appreciation to the individuals and institutions who have been pivotal in supporting and guiding me through my PhD journey.

Foremost, I am deeply grateful to Dr. Shamik Tiwari, my advisor, for his unwavering guidance, encouragement, and expert mentorship. His belief in my research and dedication of time have been instrumental in shaping this thesis.

I also express my gratitude to my committee members for their valuable feedback and suggestions, which have significantly enhanced the quality of my work.

Furthermore, I am thankful to the School of Computer Science and UPES for providing me with the necessary resources and opportunities to pursue my research.

I am especially indebted to my parents and spouse for their enduring love, support, and encouragement throughout my PhD studies.

Lastly, I extend my thanks to my friends for their companionship, understanding, and for providing much-needed breaks when required.

Sandeep Pratap Singh

UPES Dehradun

## TABLE OF CONTENTS

# LIST OF TABLES

# LIST OF FIGURES

## LIST OF ABBREVIATIONS

| | |
|---|---|
| ASD | Absolute Standard Deviation |
| AWF | Adaptive Wiener Filter |
| CCA | Canonical Correlation Analysis |
| CHT | Circular Hough Transform |
| CLAHE | Contrast Limited Adaptive Histogram Equalization |
| CNN | Convolutional Neural Network |
| DCT | Discrete Cosine Transform |
| DWT | Discrete Wavelet Transform |
| ECG | Electrocardiogram |
| EEG | Electroencephalogram |
| FSLDA | Full-Space Linear Discriminant Analysis |
| GLCM | Gray level Co-Occurrence Matrix |
| HAN | Hierarchical Attention Network |
| HE | Histogram equalization |
| HMM | Hidden Markov Model |
| HPO-ANFIS | Hyper parameter Optimization-Adaptive Neuro-Fuzzy Inference System (HPO-ANFIS) |
| HPO-CNN | Hyper parameter Optimization-Convolutional Neural Network (HPO-CNN) |
| ICP | Iterative Closest Point |
| KNN | K-nearest neighbour |
| LBP | Local Binary pattern |
| LPQ | Local Phase Quantization |
| MCCA | Multi-Canonical Correlation Analysis |
| MLP | Multilayer Perceptron |
| MSRC | Multimodal Spatial Regression with semantic Context |

| | |
|---|---|
| PCA | Principal component analysis |
| PCG | Phonocardiogram |
| QSVM | Quadratic support vector machine |
| RBM | Restricted Boltzmann Machine |
| ResNet | Residual Neural Network |
| SBVPI | Sclera Blood Vessels, Periocular and Iris |
| SMBR | Sparse Multimodal Biometrics Recognition |
| SSA-DBN | Salp-swarm-algorithm-based deep belief network |
| SVM | Support vector machine |
| WOA-ANN | Whale-optimization-algorithm-based artificial neural network |

# CHAPTER 1
# INTRODUCTION

Biometrics is the computational and analytical examination of biological data for user authentication or identification.

User recognition techniques in authentication or identification frameworks are classified based on their operating principles:

a) knowledge (e.g. passwords),

b) possession (e.g. identity card),

c) appearance (e.g. face), and

d) behaviour , actions (e.g. voice).

The latter two methods fall under biometric recognition, which encompasses physiological and behavioural characteristics that are unique to an individual.

Biometrics is the science of measuring and analysing distinctive physical or behavioural qualities that are used to identify a person. The term "biometric" is derived from the Greek words 'bios' meaning life and'metric' or'metrikos', meaning measure. Thus, it literally translates to "life measurement".

Physical features include face, fingerprint, DNA, ear, iris, retina, and hand geometry, which are all concerned with the form or measurements of the human body.

Features such as signature, voice, and gait are related to the behavior of a person or dynamic measurements.

Every biometric attribute has its merits and demerits. The correct biometric attribute should be deployed for any authentication application based on the needs of the application. Emerging technology applications use physical traits to identify persons. Nowadays, lot of applications depend on on authentication or identification to prove an individual's identity. Traditional login credentials, personal identification number, and ID cards have been used for personal identification to safeguard systems by limiting access, but they are readily hacked.

- Passwords are difficult to remember, and IDs can be stolen. Biometrics cannot be stolen, forgotten, borrowed, or fabricated.
- Biometric features can also be employed to provide additional security. Biometric systems have various benefits when compared to traditional authentication systems.
- To protect information, only authenticated users can access it, and they must be present during authentication [1].The traditional authentication technique is based on what you have and know, whereas biometric authentication is based on who you are. Thus, biometric-based authentication is the most secure solution.
- Biometrics are now widely used in domains such as forensic science, security, identity, and authorization systems.

For the past three decades, a good amount of valuable research has been carried out to improve fingerprint, voice, iris, and face-based biometric systems, to mention a few; however, new biometrics have lately emerged.

Another very popular topic in the field of biometrics over the past decade has been the use of bio signals such as EEG or ECG as biometric traits[2][3][4][5].

- ECG signals, such as Inter Pulse Interval (IPI) and Heart Rate Variability (HRV), can be utilised to identify individuals and serve as biometrics.
- ECG-based biometric devices are more accessible to various categories of persons, including persons with amputations. IPI can be obtained at various body parts—for example, fingers, toes, chest, and wrists.

- ECG-based biometrics offer multiple benefits, including smaller template sizes and reduced computational requirements. Basically, the ECG represents the electrical impulses that are produced by the heart. ECG signals represent the electrical activity of the heart.

Table 1.1: Advantages and disadvantages of biometrics

| **Advantages** | **Disadvantages** |
|---|---|
| Enhanced Security | Atmosphere and usage can influence measurements |
| Better Customer Experience | Systems may not be 100 percent accurate. |
| Cannot be lost or forgotten | Integration and/or additional hardware is necessary |
| Lower operational costs. | Once impaired, the system cannot be reset |

Table 1.2: Application of Biometrics

| | |
|---|---|
| Commercial Applications | Access Control |
| | Attendance Management |
| | Financial and Banking Services |
| Government Applications | Airports security , Immigration checks |
| | Communication Systems |
| | Social and healthcare applications |
| Forensic | Law Enforcement department and Surveillance |

Table 1.3: Benefits of biometrics

| | |
|---|---|
| Cooperation Not Required | Recognition requires no user cooperation. |
| Guarantees Physical Location | Guarantees the subject's presence at the time of identification. |
| Higher Throughput | High throughput even with fake identity and some fraud. |
| Unlosable | No chance of loss or steal |
| Unsharable | Cannot be shared with others |
| Cost Reduction | Effective implementation can result in cost savings |
| Compliance | Improved access control using authentication based on the user's physical and behavioural features |
| No Identity Theft | Using biometric authentication decreases theft of identity. |

Table 1.4: Characteristics of Biometrics

| | |
|---|---|
| Universality | Each one should have the biometric traits |
| Uniqueness | Each individual should have different features from others |
| Permanence | It should be should non changegble with time |
| Collectability | Data acquisition should be easy |
| Performance | Speed ,accuracy should be there |
| Acceptability | Large chunk of population should accept it |

**1.1 ECG as biometrics**

There has been a lot of popularity associated with a new set of biometric traits recently, and it is termed as medical biometrics. ECG compared to all the other biometric traits has been found to be very promising and performs better than most characteristics defining the quality of biometric trait. The inherent liveness detection in the biometric system inhibits spoofing efforts with the impossibility of capture and inject. Electrocardiogram acquisition settings are now acceptable and comfortable enough to be used with commercial biometric systems, however researchers have introduced new concerns such as increasing signal noise and variability. There are efforts by researchers to investigate several advanced deep learning algorithms that help in improving robustness, even though studies introduce new challenges related to the availability of data. Counterfeiting assaults in ECG biometrics are finally being handled..This study will present the ECG

Biometric rationale and obstacles, ECG anatomy and physiology, acquisition, and public datasets [5, 6].

### 1.1.1 ECG Biometrics Motivation and Challenges

From a biometrics standpoint, the ECG has been shown to include sufficient data for identification. Its benefits include universality, longevity, exclusivity, resistance to attacks, liveness detection, continuous authentication, and data minimization. Details are below [7].

a. *Universality:* It refers to the ability to collect biometric samples from the entire population. Because the ECG is such an important signal, this trait develops spontaneously.

b. *Longevity:* It is the capability of matching biometrics against previous designs. In other words, it means it is time-continuous. As will be explained further down the line, physical and psychic activity alter the ECG; however, while the exact local features of the signal varies, still the general diacritical waves and morphologies appear.

c. *Exclusivity:* The origin of the ECG signal is physiological, which ensures the distinctness of the signal. Although the pattern followed by the ECG signals of individuals is basically the same, there is a lot of interindividual variability for the number of electrophysiological variables controlling the genesis of this waveform.

d. *Robustness to attacks:* The unique look of the ECG wave pattern results from various factors of the human body's sympathetic and parasympathetic systems. Replicating or mimicking another person's ECG waveform is highly challenging. Currently, there are no known methods to falsify an ECG waveform for presentation to a biometric recognition system.

e. *Liveness detection:* ECG provides inherent liveness detection due to its inherent presence in a live person. Thus, recognition is simply a matter of checking the sensor status.

f. *Continuous authentication*: In contrast to other modalities scans, ECG is a dynamic trait that varies over time. In security monitoring settings, ECG can provide frequent updates to re-authenticate identity, typically every few seconds. This unique property of medical biometrics is crucial for preventing threats like impersonation of field officers.

g. *Data minimization:* Privacy concerns are growing in high-security environments. One approach to mitigate this issue is to minimize the use of identifying credentials. ECG biometrics offer potential for data minimization because signals can be collected independent of identification tasks. This is beneficial in environments such as tele-medicine, hospital patient monitoring, and monitoring of field agents (firefighters, police, soldiers), where ECG signals are routinely gathered).

Despite its advantages, this technology presents significant hurdles when considering large-scale application:

a. *Time dependency*. Time-varying biosignals, such as ECG, pose a risk to biometric security due to potential instant changes. Noise from body movements can affect surface ECG recordings significantly. Even without noise, the ECG signal may drift over time compared to a previously constructed biometric template due to physiological and psychological influences on cardiac function. Thus, research in ECG biometrics focuses heavily on understanding intra-subject variability to enhance reliability.

b. *Collection periods:* Unlike biometrics like face, iris, or fingerprint, where information can be captured at any moment, ECG signals are generated with each heartbeat, taking about a second. This can lead to longer wait times, especially when extracting features from longer ECG segments. The challenge lies in minimizing the number of heartbeats used for recognition to reduce processing time while maintaining accuracy.

c. *Privacy implications:* The process of gathering an ECG signal captures huge amounts of sensitive information. Such signals are reported to be capable of revealing present and past illnesses and might even give information about the current emotional state of a tested subject. In the past, access to ECG data was only given to medical professionals. Therefore, since the implications may be very grave, linking ECG samples to identities is of high privacy concern.

d. *Cardiac Conditions:* Cardiac disorders, while less common than injuries in traditional biometrics like fingerprint or face recognition, pose significant limitations for ECG biometric methods. These disorders can range from minor irregularities (such as premature contractions in the atria and ventricles) to severe conditions requiring immediate medical attention. Heart-related medical conditions can disrupt the electrical pulse conduction dynamics, leading to variability in ECG signals. Arrhythmia, a widely studied condition, causes substantial fluctuations in heart rate over time and has been shown by researchers to consistently impair the performance of ECG-based biometric systems [7].

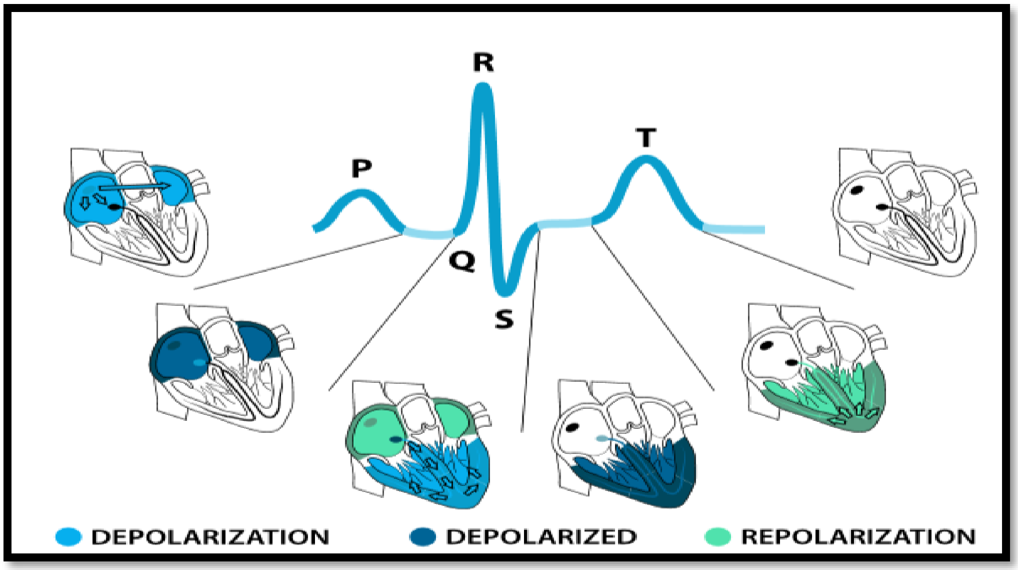



Figure 1.1: Relationship between electrical events in the heart and ECG waveforms during each heartbeat

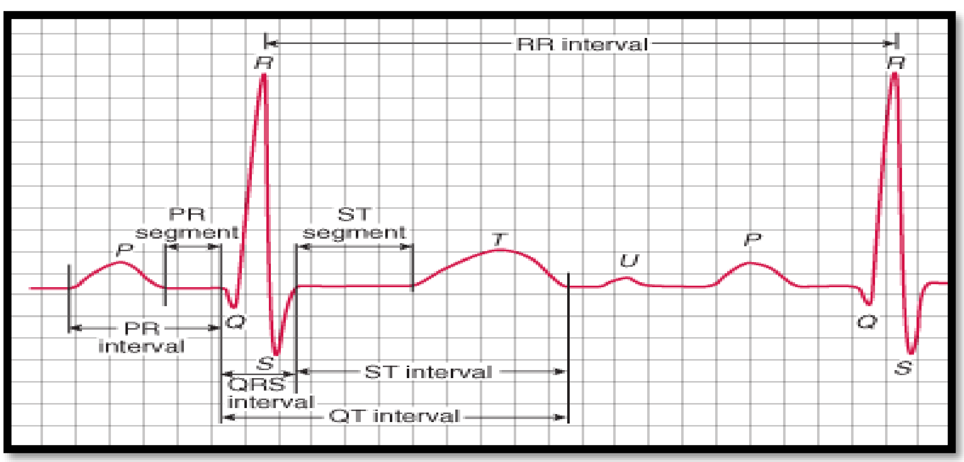



Figure 1.2: ECG Waveform

### 1.1.2 Anatomy and Physiology of the ECG

. The heart functions primarily as a pump, serving three main purposes: generating blood pressure by contracting the myocardium to keep blood circulating, redirecting venous blood to the lungs and distributing arterial blood throughout the body , and adjusting its contraction rate and force to meet the body's metabolic demands. This contraction is crucial as myocardial muscle cells respond to electrical currents, causing depolarization and triggering action potentials. These electrical currents flow through the heart and can be detected via electrodes positioned on the body, a practice known as electrocardiography (ECG). The resultant signal, an electrocardiogram (ECG), typically exhibits five distinct waves (P, Q, R, S, & T) in a repeating cycle shown in Figure 1.1, each corresponding to specific phases of the heartbeat.

Intra- and inter-subject diversity - Under normal conditions, the ECG signals of any person have similar deflections at all times. However, the timing sequence of cardiac depolarization and repolarization and their relation to different heartbeat waveforms can vary to a great extent within an ECG signal. Such variability of ECGs could be classified into intra-subject variability, cycle-to-cycle differences in a single individual's electrocardiogram, and inter-subject variability, differences between the ECG of different subjects. While the intra-subject variability is mainly studied for health monitoring and medical diagnosis, inter-subject variability plays a very important role in biometric recognition to distinguish different persons. Both of these types of variability can be caused by a variety of circumstances, most importantly:

Heart Geometry: It is also established that athletes have larger hearts with thicker myocardium secondary to intense physical training. This condition usually gives a higher voltage reading in the QRS complex of the ECG and a lower resting heart rate. The size, thickness of cardiac muscle, and general shape of the heart alter electrical current pathways, degree of muscle cell depolarization, and duration of depolarization throughout the heart.

Individual Attributes: Individual factors such as age, weight, and pregnancy alter the position and orientation of the heart. Changes in position and orientation turn electrical current conduction vectors within the heart so that electrodes face signals from other angles. Hence, these variations in turn can change the ECG waveforms' morphology.

### 1.1.3 ECG Acquisition

Acquisition methods for ECG-based biometrics have advanced significantly since early research projects. One of the intrinsic limits of ECG as a biometric trait, related to its acceptability for acquisition, has been overcome by researchers moving from the first uses in a clinical environment with multiple wet electrodes to the more recent trend of off-the-person approaches.

MEDICAL ACQUISITIONS Medical professionals use conventional electrode configurations to detect ECG signals and diagnose heart problems.Medical configurations have restrictions, such a high number of electrodes and unpleasant placement, as well as limited movement and recording time.

MOVING FREEDOM AND HOLTER SYSTEMS - To counteract these medical acquisition challenges, some studies used techniques that would allow unrestricted movement and longer time and fewer electrodes. One such example is through Holter systems that record ECG signals for a long period of time with subjects moving and carrying out daily activities.

WEARABLES AND SEAMLESSL ACQUISITION- Lately, there have been efforts to enhance off-body configurations and address unrestricted environments in ECG biometrics. These are initiatives that take another step closer to real applications in the commercial world: development of wearable technologies to acquire ECG or through sensors embedded into everyday objects, such as devices like Nymi BAND, miBEAT, and Cardiowheel [5].

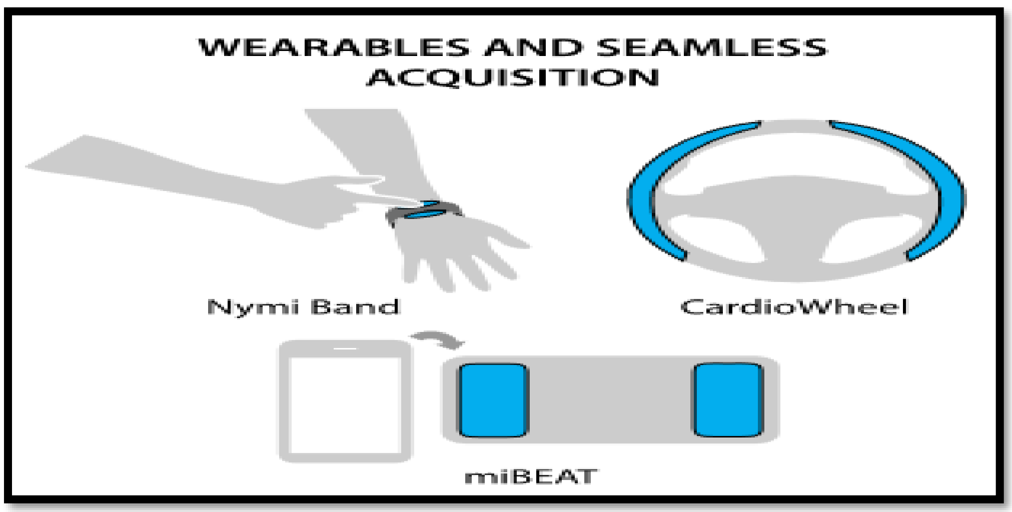



Figure 1.3: Wearables and seamless acquisition

### 1.1.4 ECG Datasets

Nowadays, several publicly available ECG databases are trying to address these problems by developing a challenging scenario for biometric system developers. Most of these datasets are archived by Physionet, while others are distributed directly by their owners. We present an overview and characterization of the most important ECG datasets available nowadays.

AHA ECG: The AHA ECG database, created by the American Heart Association, is designed to train healthcare professionals in diagnosing arrhythmias. This set has

154 ECG recordings of real patients, contributed by a number of institutions. Each record has 2 lead signals that last 3 hours, with the last 30 minutes annotated for seven different types of arrhythmias.

CYBHi: This dataset is part of the CYBHi initiative, taking into consideration that off-the-person ECG signals are acquired at two electrodes on the palms and two on the middle and index fingers. It includes a short-term dataset consisting of single-session recordings from 65 volunteers and a long-term dataset including recordings from 63 subjects taken during two sessions three months apart. Long-term recordings will also include video content designed for provoking the emotional responses of participants.

ECG-ID: The ECG-ID database focuses exclusively on biometric data and includes 20-second ECG recordings from 90 subjects, all accessible on Physionet. Each subject provided between 2 and 20 recordings over a six-month period. The data was collected using Lead I with limb-clamp electrodes placed on the wrists.

MIT-BIH Arrhythmia: The MIT-BIH Arrhythmia database, located on the Physionet repository, contains 48 signals. Each signal represents a 30-minute excerpt from ambulatory two-lead recordings that, in total, represent a large variety of arrhythmias by 47 subjects.

MIT-BIH Normal Sinus Rhythm: This database contains all excerpts from 18 subjects in the MIT-BIH Arrhythmia database identified as being free of arrhythmias or other abnormalities.

PTB: The PTB Diagnostic ECG database contains 549 recordings from 290 subjects both healthy and with various cardiac diseases: myocardial infarction, dysrhythmia, hypertrophy, or heart failure. The length of the records is from 38.4

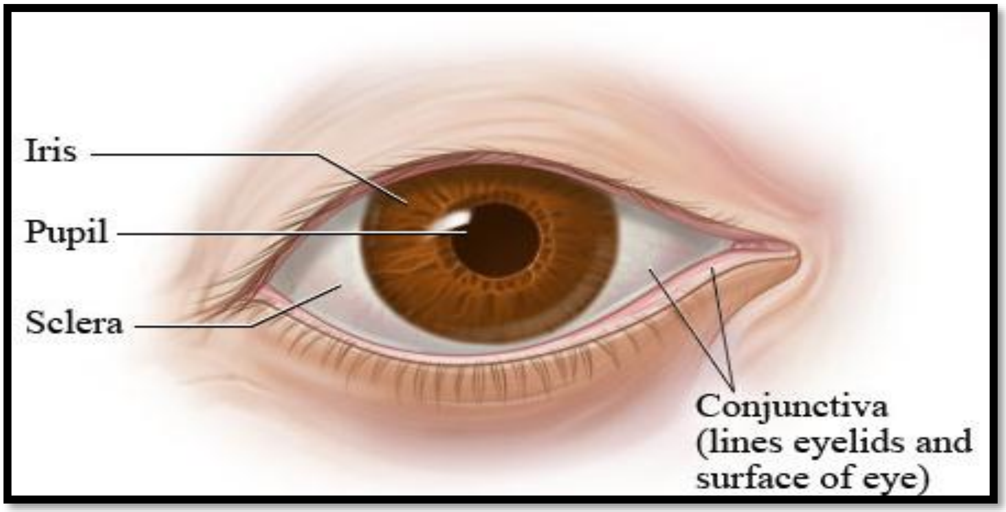
up to 104.2 seconds. All standard 12 leads and 3 Frank leads were used for recording.

UofTDB: The UofTDB, developed at the University of Toronto, is a biometric database containing off-the-person ECG signals obtained from 1019 subjects using dry electrodes on their thumbs. Each subject contributed up to six recordings over a six month period during measurements which were taken in a collection of postures including supine, tripod, exercise, sitting, and standing.

## 1.2 SCLERA as biometric

### 1.2.1 Sclera Background

Components of the Human Eye: The human eye consists of several components: the pupil, iris, cornea, upper eyelid, lower eyelid, aqueous humor, sclera, and scleral veins, as illustrated in Figure 1.4. Among these, the sclera is the white outer layer that safeguards the eye's structure. It is covered by a mucous membrane essential for smooth eye movement and is encircled by the optic nerve. The sclera is the thickest part of the eye, and its interior comprises the episclera, situated beneath the conjunctiva; the sclera proper, a dense white tissue that gives the sclera its distinctive color; and the lamina fusca, which consists of elastic fibers.




.

Figure 1.4: Human Eye

Unique blood vessel patterns, as shown in Figure 1.5, exist in the sclera and differ in every individual, including in identical twins. Because these vascular patterns are visible and do not change in a lifetime, it is possible to use this feature for real-time human recognition.

### 1.2.2 Sclera Biometrics

Among conventional biometric features applied in automated recognition systems, ocular properties have the advantage of being contactless data capture, showing a highly accurate rate of recognition, and being widely accepted by users. While iris recognition remains the leading technology in this field, recent research is increasingly exploring other ocular characteristics that could enhance iris-based features, aiming to create more secure and less easily spoofed authentication systems. The sclera vasculature in this regard turns out to be quite a promising alternative. The vascular pattern of an individual's sclera is unique and relatively stable over time; therefore, it may possibly be used for authentication purposes, as current research has indicated. These vascular patterns possess qualities that make them advantageous for recognition systems; for instance, they remain discernible even in cases of eye redness or when contact lenses are worn, which can impair iris recognition systems. Despite its promise, research on sclera vasculature as a biometric trait is still in its early stages. Several challenges need addressing before this technology can be integrated into commercial systems. Specifically, finer blood vessels within the sclera require accurate segmentation from ocular images to achieve competitive recognition performance. These vessels exhibit diverse border types and a complex texture, posing significant challenges for segmentation and modeling. To address the challenge, most conventional techniques normally adopt a two-step solution wherein the sclera region is first located from ocular images, followed by the extraction of its vascular structure using established algorithms, often unsupervised, utilizing techniques such as Gabor filters, wavelets, and gradient operators. While these methods have demonstrated potential, recent studies indicate that supervised techniques offer significantly improved segmentation accuracy, particularly for challenging off-angle ocular images. Beyond the intrinsic challenging nature of the task, one of the main difficulties in developing competitive supervised techniques for sclera recognition systems has been the deficiency of appropriately annotated datasets dedicated to the task of sclera segmentation.

Since ocular images are often captured without precise alignment and may display various gaze directions, it is unlikely that all parts of the scleral vasculature will be visible in every image. For effective comparison of sclera images in person identification, it is crucial to extract distinctive features from the segmented vasculature that are robust to variations in position, scaling, and rotation. These features should enable accurate comparisons even with only partial segments of the vascular structure.While these techniques have gained much popularity, recent trends in biometrics indicate that learned image descriptors based on convolutional neural networks normally outperform traditional local descriptor-based techniques [8, 9].

### 1.2.3 Sclera Recognition System

This process is the first step of most sclera recognition systems: segmentation of sclera from an image of the eye. Iris localization is used at the beginning for feature extraction. After finding the iris boundary, the left and the right portions of the remaining parts are utilized.

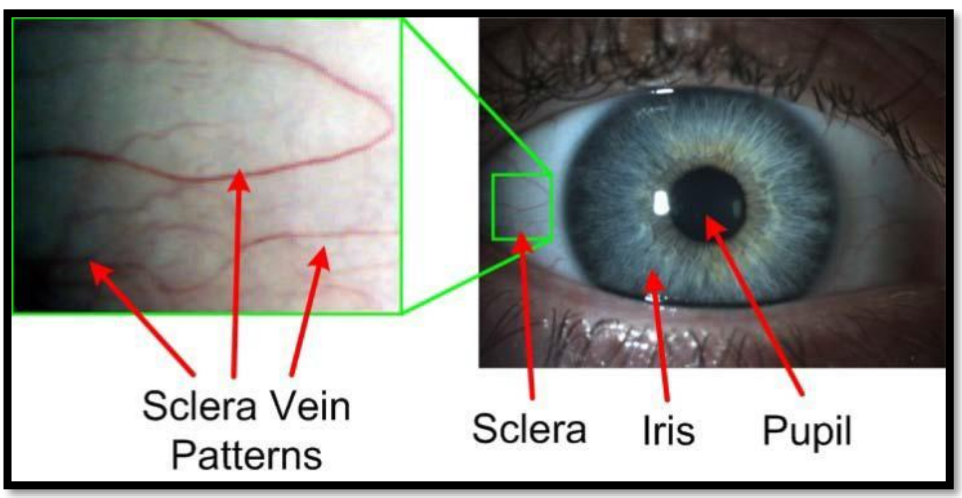



Figure 1.5: Sclera Vein Pattern

In the case of a single modal biometric system, only the sclera that is extracted can be used for recognition. On the other hand, multimodal biometric systems fuse different biometrics with sclera features to identify a person. One of the methods is fusion with iris and sclera . The algorithm uses an integro-differential operator to locate the iris boundaries and the Contrast Limitd Adaptive Histogram Equalization algorithm for enhancing the sclera region. The result will be an image containing information about iris and sclera. In [10], iris detection is based on an  k-means clustering algorithm, while the sclera is identified by red-green and red-blue values calculated from the saturation component. The sclera region could have noise due to distance or movement during capture. It proposes an efficient method of detecting the corners of the eye, which is essential in avoiding misclassification and determining the gaze direction. In the second stage, the system extracts the sclera image from the processesd eye image. The resulting sclera is improved to highlight the vein patterns and eliminate extraction-related noise. Finally, the extracted image is matched with those in the database for identification. In case of a successful match, it confirms the identity of the person; otherwise, in case of a mismatch, it is an authentication failure.

SCLERA DATASETS

Several datasets are currently accessible for research in ocular biometrics, including CASIA Iris v1, CASIA Iris v2, CASIA Iris v3, UTIRIS, UBIRIS v1, UBIRIS v2, MICHE-I, and SBVPI, all of which are publicly available.

### 1.3 Unimodal and Multimodal biometrics

Unimodal biometric systems use only one feature to authenticate the identity. In such systems, any physical or behavioral modality is utilised.

Most of the unimodal systems have four modules. The modules include sensor, feature extraction, matcher, and storage.

The sensor module captures user input, which can include various biometric features. This input is initially an image that is then preprocessed to enhance clarity. The feature extraction module isolates relevant details from this data, as not all parts of the image are used in the authentication process. Only specific features are selected. During enrollment, all extracted features are saved in a database via the storage module. In the verification phase, the matcher module compares the query against the stored template to confirm identity.

The unimodal biometric system has the following disadvantages: noisy data, intra-class variations, inter-class similarities, non-universality, and spoof attacks.

Noisy data includes irrelevant or undesirable information within the original dataset. Intra-class variances describe the differences in images captured during authentication and enrollment, which may result from sensor misalignments. Inter-class similarities refer to the resemblance between images of different individuals. Nonuniversality occurs when certain individuals cannot exhibit consistent features due to factors such as age, disabilities, or other variables. Additionally, attackers might replicate original traits through spoofing, creating a counterfeit copy in a spoof attack.

Multimodal biometric technology employs multiple biometric indicators to authenticate an individual's identity. Compared to unimodal systems, multimodal biometric systems are generally more reliable and efficient. If one attribute fails to verify the user, other characteristics can be used to ensure accuracy. Additionally, these systems offer enhanced security against spoofing through various template protection methods such as fuzzy vaults, watermarking, and cancellable biometric cryptosystems. The multimodal biometric system is comprised of five distinct modules:

The following modules are included: sensor, feature extraction, fusion, matcher, and storage.

The sensor module in a multimodal system operates similarly to a unimodal system, but it employs multiple sensors to capture various biometric parameters. All images captured by the sensors undergo preprocessing, with only the relevant features extracted by the feature extraction module. The fusion module then combines features from different biometrics to create a single, unified template. The matcher and storage modules function as they do in unimodal systems but work with this fused template containing multiple attributes. Therefore, image fusion is crucial in multimodal biometric systems, as all processes are based on the combined template.

Types of fusion include feature level , matching score level , and decision level fusion.

Feature level fusion combines features from multiple traits into a single template. In score level fusion, scores from different modalities against multiple classifiers get integrated and the highest level score is sought. Decision level fusion combines the result of the matching module

### 1.4 Organization of report

The thesis is organized as follows: Chapter 2 give the details of the work done in the field of biometric authentication, mainly concentrating on ECG multimodal. In chapter 3, the details of the first proposed multi-biometric system are presented including ECG and fingerprint ,Sclera that is A Dual Multimodal Biometric Authentication system based on WOA-ANN and SSA-DBN techniques. In chapter 4, the details of second proposed Hybrid modal has been presented.. The experimental results are analyzed and discussed in each of chapter 3 and 4. Finally, chapter 5 concludes the study.

# CHAPTER 2

## LITERATURE SURVEY

### 2.1 Review of various multimodal biomterics

In this chapter we will first discuss about various multimodal biometrics based on two modalities.

**Fingerprint iris**: One of the combination for multimodal is Fingerprint and Iris.Fingerprint is most widely used, reliable and traditional biometric trait in [11] paper these two modalities can be fused at score-level ,using z-score standardization ,scores are combined using approaches like min max score ,sum rule. In this feature level fusing techniques are used for multimodal biometrics. Ocular trait Iris is also gaining popularity which have proven accurate and contactless biometric technology.

**Face Iris**: Another combination for multimodal biometrics are Face and Iris. Iris is one the most accurate biometrics unaltered throughout life and can be segmented from eye images. Face is also the simplest way to recognise a person,low cost identification. Another reason for combination is high resolution face image can give you both Iris and face features. P.Moutafis et al [12] used eigenface for facial features and Daugman's algorithm for iris features.Researchers in [13] used 1D Log-Gabor filter for Iris .PCA,LBP are applied to extract facial featuresFor selection PSO ,Score and feature level fusion,tanh normalization and weighted sum rule are used.In [14] PCA,DCT forface and 1D log gabor ,genetic algorithm for IRIS are used. Hybrid fusion and multi resolution 2 –dimensional log gabor filter is applied by B Ammour et al [15].

**Face Ear**: Face and Ear can also be combined for multimodal biometrics as both are contact free , can be captured by same type of sensor ,ear are independent of facial expression, these are some reasons to combine. Both can be combined using score level fusion,feature level fusion ,decision level fusion, rank level fusion and sensor level fusion.[16] used sensor level fusion using principal component analysis based algorithm for feature extraction.[17] used FSLDA,[18] used CNN based method.

Xu and Mu [19, 20] merges face and ear features at feature level.They achieved enhanced accuracy with the help of Kernel CCA(canonical correlation analysis ) feature fusion technique. Theoharis et al [21] suggested an integrated technique that merges 3D face and ear features..They created annotated face model (AFM) and an annotated ear model (AEM) with the help of statistical data.It attained good recognition rate.Huang et al. [22] proposed a multimodal technique named MSRC, it joins PCA features of ear and face in serial one after other and applied SR classification .MSRC performs better than CCA based techniques.Score level fusion with its schemes like sum ,product ,median rule is used by,Xu and Mu [23],Yan [24],Mahoor et al [25], Islam et al [26],Huang et al [27],with some methods like FSLDA algorithm,ICP method,CNN models, sparsity-based matching metric.

**Iris Voice**: In [28] Iris and Voice are fused at score level for multimodal system using min max scheme.For feature extraction Gabor Wavelet and Hamming distance is applied.

## 2.2 Review of ECG based multimodal biometrics

At first we will discuss about Multimodal Biometrics with ECG(Two Modalities).

One Numerous multimodal biometric systems based on conventional modalities such iris, fingerprint have been created during recent years; but only a few studies have been done on a multimodal biometric system that integrates ECG.

Komeili et al. [29] used an ECG with a fingerprint to identify and confirm liveness. They did not, however, emphasis on fingerprint authentication accuracy and instead concentrated on liveness verification.

Zhao et al. [30] proposed a multimodal biometric architecture based on finger ECG and fingerprint readings, although they did not test it .

Manjunathswamy et al. [31] devised a biometric recognition method based on ECG and fingerprints. To combine the ECG with the fingerprint, they employed decision level fusion.. They did, however, work on a low authentication barrier (75 percent) and did not offer details on the study's user count.

Singh et al. [32] also described a multimodal biometric system, however the ECG data have been acquired from chest readings, ignoring one of the key benefits of a smaller finger based device.

However,all above focused on traditional machine learning algorithms, which frequently suffer from overfitting and perform poorly when verified on a various other dataset..

Zokaee et al. [33] proposed a multimodal biometric system using ECG biometrics and palmprint, which they developed using principal component analysis for palmprint feature mining, mel-frequency cepstrum coefficients method for ECG features followed by the application of the k-nearest neighbours (KNN) classifier .

Fatemian [34] proposed a multi-biometric identification method based on the combination of 2 heart related features, ECG and PCG, and the decision level.

In 2007, Sim et al. [35] developed a fusion method based on face and fingerprint recognition using modalities and time. The authors presented a Bayesian framework in which a mathematical model was presented based on the HMM model, while constructing a model of biometrics where users who log in continuously confirm their presence.

Boumbarv et al. [36] combined ECG ,face biometrics using rules like minimum rule, maximum rule ,summation rule, product rule, depending on each classifier's output probabilities., For facial biometrics, the support vector machine was used and for ECG biometrics, the Radial Basis function network based classifier was employed.

Jaina et al. [37] conducted a number of studies on various normalization methodologies and the efficiency of various rule based on hand shape size, fingerprint, and face biometric system. To the multimodal biometric system, the researchers used the normalisation techniques z-score, min–max, followed by a summation of scores fusion method.

Pouryeyevali [38] proposed combining fingerprint and ECG modalities to create a multimodal biometric recognition method. Support vector machine , likelihood ratio ,weighted sum rules and were used in the fusion system, which was based on cutting-edge techniques. For real-world applications, the fusion technique performs admirably and is resistant to spoof attacks.

They examined the performance of the biometric dataset for ECG, face, and fingerprint traits in Raju and Udayashankara [39] , who offered a different method for individual idenfication on the basis of dataset privacy using multimodal biometrics. Multimodal biometrics improve biometric individual authentication accuracy and security, according to the findings.

Shekhar et al. [40] based on a multimodal sparse method proposed a sparse multimodal biometrics recognition (SMBR) approach, in which the test data is denoted by a sparse linear combination of training data.

Barra et al. [41] demonstrated a biometric architecture that integrated the six different EEG bands with first ECG lead I . The EEG spectrum features and fiducial point features from the ECG were retrieved, and the fusion was done based on these features. Product, sum, and weighted sum are the multimodal system operators implemented on ECG s and EEG .Sabri et al. [42] proposed a biometric identification model based on sequential feature and workflow management using a range of classifiers in 2019. For dynamic individuals' authentication, the matching on card method and matching on host processes are utilised.They used their architecture on a multimodal chimera database, which improves the acccuracy of a conventional match on card .Ching [43] tested a novel mix of accelerometer-based gait modalities,speaker and face in a fused biometrics system. They built the MMU GASPFA (GAit–SPeaker–FAce) multimodal database, in which accelerometer-based gaits were gathered from people wearing various footwear, encumbrance, and clothes to see how each aspect affected the identification process.

Meryem Regouid et al. [44] proposed Multimodal system of biometrics based on local descriptors for ECG, ear and iris recognition.It one of few that uses 3 modalities.Mohamed Hammad et al used CNN on feature and decision level Fusion of Fingerprint and ECG, achieved good results .Mohamed Hammad et al [45] proposed model with ECG and fingerprint Parallel score fusion for human identity verification using CNN .Sahar A. El_Rahman [46] used different classifiers like NN,FL LDA for Multimodal biometric systems based on various fusion techniques (score,decision) of ECG ,fingerprint .Monwar and Marina et al [47] proposed a model , that merge face, ear,iris data. This uses Hough transform method and Hamming distance for iris recognition and the Fisher image method to the ear and face image datasets for recognition.Analysis in tabular form is shown in Figure 2.1.

| Authors and Year | Modalities | Fusion Techniques /Fusion Level | Sample size,Dataset used | Performance measurment | Remarks |
|---|---|---|---|---|---|
| Komeili et. al.(2018) | ECG,Fingerprint | Score based fusion | LivDet2015 database | average EER 2.9% | Only liveness detection concentrated not targeted on fingerprint authentication performance |
| Zhao et al.(2012) | ECG,Fingerprint | AC/LDA(autocorrelation/linear discriminant analysis) method | - | Did not evaluated | No evaluation |
| Manjunathswamy et al.(2014) | ECG,Fingerprint | Score based fusion | Biopac MP35 for different subjects used for ecg aquisition | Multimodal biometric: match rate up to 92.8% ,FAR = 2.5, FRR = 0 | Low authentication threshold (75%), |
| Zokaee and Faez (2012) | ECG and palmprint | score level Matching | data of 50 subjects | Multimodal: Acc. 94.7%<br>Palmprint: Acc. 82.1%<br>ECG: Acc. 89% | |
| Fatemian (2009) | ECG and PCG | fusion Decision level | data of 21 subjects | ECG: for 95% similarity accuracy of 93% threshold<br>%<br>Multimodal: accuracy of 96.4%<br>PCG: accuracy of 88.7% with a certainty 70 | Intrasubject variability issue |
| Boumbarov et al . (2011) | ECG and face | Max rule, Min rule , Sum rule ,Product rule ,Decision level, | data of 19 subjects | Multimodal Minimum rule: Acc 99.0%,Maximum rule: Acc. 93.15% rule of sum: 99.1% rule of product: 99.5% | Intrasubject variabilty issue |
| Pouryayevali (2015) | ECG and fingerprint | Likelihood ratio, Weighted sum rule, SVM | data of 45 subjects | Multimodal: EER of 1% | |
| Barra et al . (2017) | ECG and EEG | Score level,Sum ,Product ,Weighted sum | 52 subjects data(EEG Motor Movement/Imagery Dataset (EEGMI)and PTB database | Good results over basic fusion methods with different bands of EEG | Not much features explored |
| Sabri et al. (2019) | Fingerprint and face | Score level, | 200 subjects | | No liveness |
| Mohamed Hammad et al.(2018) | ECG ,Fingerprint | Classifier based decision fusion ,Feature fusion with addition | MDB1 and MDB2 | Feature fusion with addition MDB1 EER=0.40%,MDB2=0.32%,Classifier based decision fusion MDB1 EER= 0.14%,MDB2 EER=0.10% | simultaneous Intrasubject variabilty issue+ Fingerprint issues |
| Sahar A El Rahman(2020) | ECG ,Fingerprint | NN,LDA,FL (For score based fusion),score level fusion,decision level fusion,Max rule ,Sum rule ,Product rule., | FVC 2004 Fingerprint database ,47 subjects data (MIT-BIH database) and | SEM(Standard error of mean) is up to 0.00824 for decision level,, and up to 0.01045 for score level, | simultaneous Intrasubject variabilty issue+ Fingerprint issues |

Figure 2.1: Analysis of ECG with two modalities

In this section we analyzed few articles that has explored the **three modality** field with one  being ECG in it.It is presented in tabular form in Figure 2.2.

| Authors and Year | Modalities | Fusion Techniques /Fusion Level | Sample size,Dataset used | Performance measurement | Remarks |
|---|---|---|---|---|---|
| Singh et al(2012) | ECG with face and Fingerprint | Transformation based score fusion, Weights on match scores distributions (FTMSD)Weights on equal error rate (FTEER) , | MIT-BIH arrhythmia .+ST -T +MIT NSR+QT | EER=1.52% | a compact finger-based system is not used for ECG collection which may be the disadvantage |
| Jaina et al. (2005) | Fingerprint, face, and hand geometry | Max-score rule ,Min-score , Sum of scores | data of 100 subjects | Multi-biometric : Maximum-score: GAR up to 93.6% Minimum-score: 85.6<br>Sum of scores: 98.6% | No liveness |
| Raju and Udayashankara (2017) | ECG, face, and fingerprint | SVM-based , Likelihood ratio based ,,Weighted sum rule, | data of 50 subjects | -- | simultaneous Intrasubject variability issue+ Fingerprint issues |
| Shekhar et al. (2014) | Iris ,fingerprint,face | Support vector machine (SVM) , Multiple kernel learning (MKL),Sparse multimodal biometrics recognition (SMBR) , | 219 subjects data (WVU multimodal dataset) | Multimodal<br>SMBR-WE: 98.7 ± 0.5<br>SMBR-E: 98.6 ± 0.5<br>SVM-Major: 81.3 ± 1.7<br>SVM-Sum: 94.9 ± 1.5<br>MKL Fusion: 89.8 ± 0.9 | No liveness |
| Meryem Regouid et al.(2019) | ECG, Ear and Iris | feature level | CASIAv1 iris databases ,ID-ECG and USTB1, USTB2 and AMI ear | 0.54%, 0%, 1.1%,100%, for ERR, FAR and FRR, , CRR resp. | Iris may not work in certain deformity, Ear more prone to give error |
| Monwar et al.(2011) | Face, Iris and Ear | Rank level | CASIA database ,USTB database,(FERET) database | -- | No liveness |

Figure 2.2: Analysis of ECG with three modalities

El-Rahiem, et al. [48] introduced a multimodal biometric confirmation technique in light of can be profound merging of ECG and finger vein. This framework had three primary parts that are biometric pre-handling, profound component extrication, and verification. On the time of pre-handling, standardization and separating strategies were adjusted for every biometric. In the element extraction process, the highlights were extricated utilizing a proposed profound CNN model. Then, at that point, the confirmation cycle was performed on the removed elements utilizing five notable AI classifiers: SVM, KNNs, RF, NB, and ANN. Likewise, to address the profound elements in a low-layered highlight space and accelerate the verification task, the creators embraced MCCA. Exploratory outcomes stated improvement as far as validation execution with EERs of 0.12% and 1.40% utilizing highlight combination and score combination, individually.

Valsaraj, et al. [49] dissected the EEG signals for trademark highlights evoked by development and creative mind of 4 unique upper appendage developments. Similar development symbolism undertakings were looked at for execution and its legitimacy in fostering a powerful multi-modular biometric framework for people with engine handicaps. The review included 10 subjects implementing envisioned raising of right and left hands and gripping right and left -hand clench hands. Alongside envisioned development (Engine Symbolism), information for genuine appendage development was gathered, and the presentation was analyzed for both nonexistent and real development. This framework pipeline accomplished under 2% misleading acknowledgment rate for every one of the fanciful and real activities. A innovative multimodal technique consolidating diverse MI activities was effectively executed with 98.28% precision. In addition, both fanciful and real developments showed similarly great capacity for biometrics purposes recommending the convenience of the introduced biometrics framework for individuals who lost engine capacities or individuals with unfortunate engine symbolism abilities.

Cherifi et al. [50] developed a totally unobtrusive and robust multimodal verification system that passively authenticates a user by the way he/she picks up his/her phone, following the removal of arm and ear signal modalities from this single action. In order to overcome the challenges which real applications create for ear and arm signal confirmation frameworks, the authors proposed a different approach based on image discontinuity, making the ear recognition more robust against obstruction. The ear feature extraction was done locally by Neighborhood

Phase Quantization in a way to gain robustness regarding pose and illumination variation. They also developed a set of four factual features that would help distinguish elements from arm movement signals. Their multimodal biometric system achieved an EER of 5.15%.

Gavisiddappa, et al. [51] introduced a successful element determination calculation to decide the ideal component values for additional working on the exhibition of multimodal biometric confirmation. At first, the info pictures were gathered from CASIA dataset. Then, at that point, highlight extraction was done by utilizing LBP, seemingly trivial details include extraction, GLCM highlights like bunch noticeable quality, IDMN and autocorrelation. After highlight extraction, adjusted help include determination calculation was utilized for dismissing the insignificant elements or for picking the ideal highlights.

Sudhamani et al. [52] developed a biometric system that combines finger vein and facial features, utilizing Convolutional Neural Networks (CNNs) to streamline the feature extraction process. The model, trained on a GPU-enabled cloud platform, was optimized by adjusting hyperparameters like dropout rates and mini-batch sizes. Minimal preprocessing with min-max normalization helped reduce computational time. The CNN model, which uses a softmax classifier for feature extraction, achieved a baseline Equal Error Rate (EER) of 0.46%, outperforming existing authentication systems.

Bansong et al. [53] introduced the Diverse Hierarchical Attention Network (HAN), a multimodal approach incorporating palm images, facial images, voice prints, and digital signatures. HAN improves verification accuracy through layer-by-layer isolation and advanced attention mechanisms, offering more precise and secure user authentication. The model was developed on a cloud-based platform and integrated with an Android application. Evaluations showed that HAN outperforms previous models in terms of effectiveness.

Wang et al. [54] suggested a biometric system with finger vein and face bimodal component layer fusion using a Convolution Neural Network (CNN), which conducted fusion in the part layer. It is designed with a self-supervised framework to obtain representations of the two biometrics, combined with the RESNET residual network and combined with the self-supervised weight characteristics concatenated with the bimodal fusion integrate channel thought. In the experimentation part, Alex Net and VGG-19 connection models have been chosen for isolating finger vein and face picture features as contributions to component blend module to demonstrate the high effectiveness of bimodal component layer blend. Massive experiments have been conducted, showing that the affirmation accuracy of the two models has gone over 98.4%, demonstrating their high efficiency for bimodal component mix.

Ayu et al. [55] developed an iris recognition system for eyes wearing noncosmetic contact lenses, wherein discrete wavelet transform was used for feature extraction and circular Hough transform for iris localization in the preprocessing step. It was observed that experiments yielded quite promising results with an accuracy of 0.95 for the noncontact lens category and 0.8 for the category with noncosmetic lenses. The results also showed just how critical the iris localization step is to a recognition system.

According to Nawawi et al. [56], despite its potential advantages, ECG remains a rarely used biometric mechanism in practical wearable applications. This is despite the fact that biomedical signals like the electrocardiogram continue to increasingly be used for biometric purposes in tandem with growing interest in wearable technology. This work focused on analyzing the ECG signals captured from the wearable Hexoskin Proshirt in various physiological conditions for biometric authentication. The ECG signal of each subject under investigation was captured in this work while standing, sitting, walking, and during uncontrolled activity. First, the raw ECG signal is pre-processed in the time domain with Butterworth filters for noise removal, and then an efficient QRS segment feature extraction method is applied. In the end, about 854 datasets were created for training and validation, and on the remaining 300 datasets, a quadratic support vector machine was employed to test the suggested recognition method. The results demonstrated that this method could firmly provide accuracy above 98% on the internal datasets. The results clearly show that intelligent textile shirts and ECG biometrics are feasible and can successfully perform authentication in most real-life scenarios with changing physiological parameters.

### 2.3 Gap analysis and Problem statement

Multi - biometric frameworks are considered to be more reliable and productive than unimodal biometrics frameworks because multimodal will fulfil the drawbacks of single biometric model.As seen in figure 2 and figure 3 remarks each combination of modalities has certain parameter lagging either it be liveness,intravariability issues,low authentication threshold,less feature explored.On the basis which certain gaps has been concluded and some novelty is suggested.There are number of multimodal system based on two modalities like EEG+ECG, ECG+Face,ECG+Speech,ECG +Fingerprint in all this cases if Intra-variabilty issues(cardiac condition) and failure of other modality occur simultaneously then system can be failedThere are also some multimodal that uses three modalities like Ear+Iris+Face, fails to check liveness of subject, ECG+Iris+Ear this system will fail if Intra-variabilty issues(cardiac condition) and other modality fails like Iris( incase of contact lenses, potential eye redness ,blindness) occurs.There is no Multimodal with a combination of ECG+ Sclera +Fingerprint.It removes problem of two modality ,also Sclera works better over Iris in existing three modal system

So a novel biometric system can be proposed. In this system we combine ECG, Fingerprint and Sclera. ECG will add liveness detection over fingerprint and Sclera. Sclera will remove age constraint, wear and tear, easy duplication over fingerprint and cataract, visually impaired issues over IRIS. Fingerprint and Sclera will give advantage over ECG in case of intra-subject variability like cardiac conditions. So fusion of this three will be a robust system.ECG and Fingerprint are natural choice as both can be captured from fingers and Sclera will add robustness against physical damage to fingers and cardiac condition.

**Problem Statement** : In real-world applications, unimodal biometric systems that use a single biometric modality have various issues, including noise in sensed data, intra-class variances, inter-class similarities, non-universality, and spoof assaults. To address the shortcomings of unimodal systems, we require a system that overcomes the constraints of any single paradigm.As a result, a multimodal biometric system with liveness requires the combination of several biometric traits. Furthermore, because most modalities do not allow subject liveness detection, we require modality support for liveness.

## 2.4 Objectives of the research

To design a multimodal biometric system based on fusion of ECG, Fingerprint and Sclera.

Sub-objectives

a. To design a sequential multimodal biometric system

b. To design a parallel multimodal biometric system

c. To design a hybrid multimodal biometric system

# CHAPTER 3

## A DUAL MULTIMODAL BIOMETRIC AUTHENTICATION SYSTEM BASED ON WOA-ANN AND SSA-DBN TECHNIQUES

### 3.1 Introduction

Confirmation is the most common way of recognizing a person or thing, to give access control to frameworks through a coordinating course of clients' information with the information put away in an approved data set. Customary confirmation frameworks in view of logins and passwords are definitely more helpless to assaults than biometric validation frameworks. Biometric recognizable proof is the craft of utilizing physical or actual attributes (i.e., iris, veins, face, palm , fingerprint, tooth shape, ECG, ear shape, and so on) and conduct qualities (i.e., voice, walk, mark, and keystroke elements, and so on) to distinguish clients [57]. Biometric systems are characterized by several key properties: exceptionality (each biometric should be unique to an individual, even among twins), comprehensiveness (the biometric should be consistently linked to the individual), permanency (the biometric should remain stable over time), quantifiability (the biometric should be measurable with standard technology), and ease of use (the system should be user-friendly). While biometrics offer extensive applications, they face challenges such as environmental impacts on measurements, integration with additional hardware, and the inability to reset compromised biometrics. These systems rely on unique biological traits to function effectively [58]. Many works ordinarily endeavor to utilize three biometric characteristics to be specific ECG sign, sclera and unique mark.

An electrical sign that transmitted by the heart is termed as the ECG signal. It tends to be estimated non-rudely by sensors appended to the chest of human [59,60]. As of late, it can be utilized for validation, as it encounters the vast majority of biometric determinations. One of the upsides of ECG-based validation is Aliveness, and dissimilar to other verification strategies, for example, finger impression and secret key confirmation, it tends to be put in exclusively for alive people. Additionally, ECG perhaps given by a more extensive scope of individuals, for example, tragically handicapped people and incapacitated, who can't give regular biometrics, for example, unique mark, iris or palm print. Moreover, ECG information perhaps removed from different pieces of the body, for example, fingertip that makes it pertinent for a many people [61,62].

The sclera, which is the white part of the eye, forms a sturdy protective barrier. It is coated with a fluid layer necessary for the eye's smooth movement [63,64]. Moreover, it is the thickest part of the eye, surrounded by the optic nerve. It comprises the episclera, which is underneath the conjunctiva; the sclera proper, consisting of a thick white fibrous tissue that gives the eye its white color; and lastly, the lamina fusca, which is partly elastic and partly fibrous. Vein patterns within the sclera are unique to each individual, even differing between identical twins [65, 66]. These vein patterns can be used for identifying individuals in various scenarios, as they are visible and remain unchanged throughout a person's life. In a unimodal biometric system, only the isolated scleral patterns can be used for recognition purposes.

Unique finger impression-based confirmation is one of the main advances of the biometric verification and is acquiring its prominence in everyday life [67, 68]. The development of a confirming unique mark acknowledgment framework is critical these days and has drawn the consideration of parcel of specialists. The fingerprints acknowledgment frameworks are currently comprehensively utilized for 1:1 coordinating (confirmation) or 1: N looking (ID) all over the planet. They are able to do dependably perceiving people for the delicate certifiable applications like financial exchanges, PC/cell security, criminology and global boundary crossing. Principally, unique finger impression acknowledgment framework has a course of coordinating of finger impression to be validated with the current information base of fingerprints [69, 70]. Then, at that point, it might likewise be utilized as an as a gadget for security. Taking into account finger impression based verification frameworks, found finger impression is an association of number of edges and valleys on the picture surface [71, 72].

There are two sorts of biometric frameworks, for example, the unimodal biometric framework and the multimodal biometric framework. In this, unimodal biometric frameworks utilized only one biometric quality for acknowledgment frequently influence problems, for example, biometric information variety, absence of peculiarity, low acknowledgment precision, and parody assaults. To find the issue, multimodal biometric frameworks are utilized. Multimodal biometric frameworks, combining various attributes, address limits of unimodel biometric frameworks in matching precision, caricaturing trouble, comprehensiveness, and attainability, and so forth [73]. When contrasted with single-modular biometric frameworks, a multimodal biometric framework increments acknowledgment precision, security, and framework dependability.

However, the information degeneration of any of the biometric model in the multimodal biometric framework corrupts the exhibition. This is because of the way that most existing multimodal approaches also employs combination rules that are fixed or their combination rules can't successfully alter to the diversities of biometric attributes and the ecological changes. Regardless, the degree of combination turns into an issue of concern, then, at that point, the Element portrayal and matching procedures are too muddled to even consider performing. From that point, the Interest gets compromised between verification execution, calculations and cost.

### 3.2 Contribution

This work is aligned to sub-objective 1 and 2 i.e. "To design a sequential multimodal biometric system" and "To design a parallel multimodal biometric system" based on ECG, fingerprint and Sclera. The work has fostered the work has fostered an original Multimodal Biometric validation framework whose goal is

- To make an equal combination multimodal biometric framework utilizing three biometric qualities to be specific ECG, Finger impression and Sclera.
- To make a successive combination multimodal biometric framework utilizing three biometric qualities in particular ECG, Unique mark and Sclera.

### 3.3 Methodology

In this research work, two multimodal biometric systems are developed as shown in figure 3.1 & 3.2. These are developed by combining three uni-model biometric systems. ECG, Sclera and fingerprint are the unimodel systems selected for this work. The sequential model biometric system is developed by decision level fusion. The parallel model biometric system is developed by score level fusion.

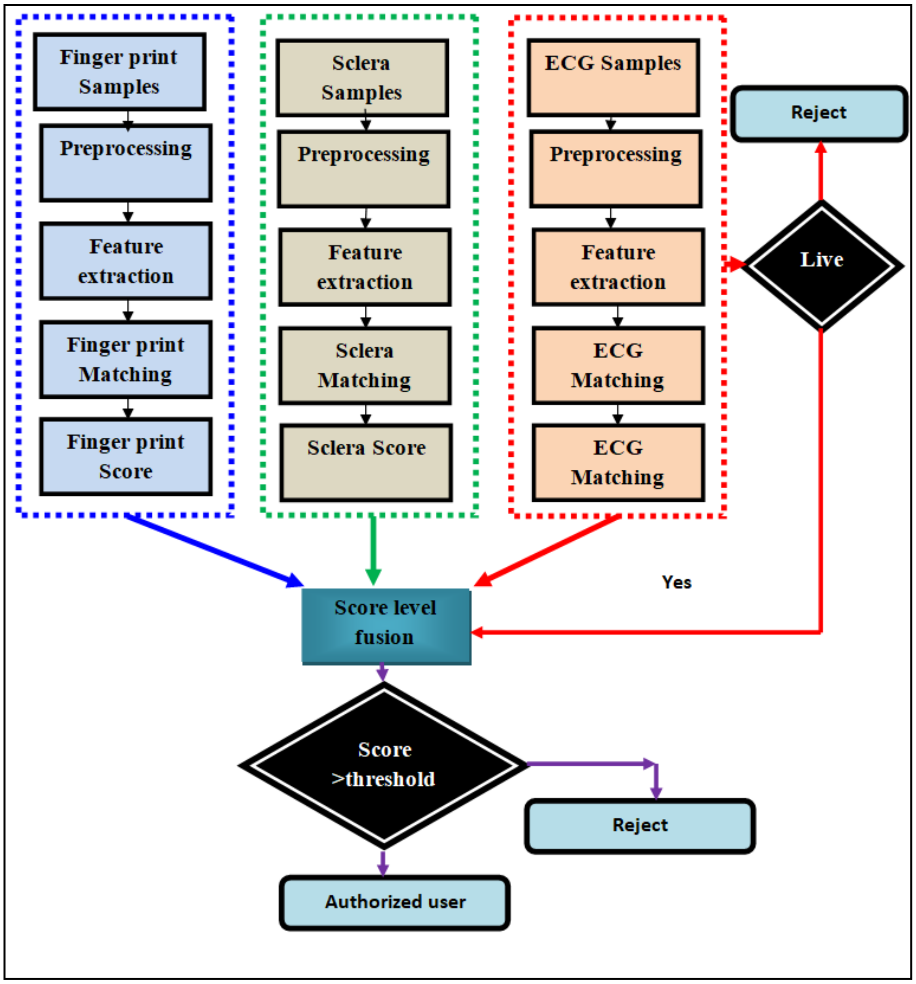



Figure 3.1: Parallel modal architecture

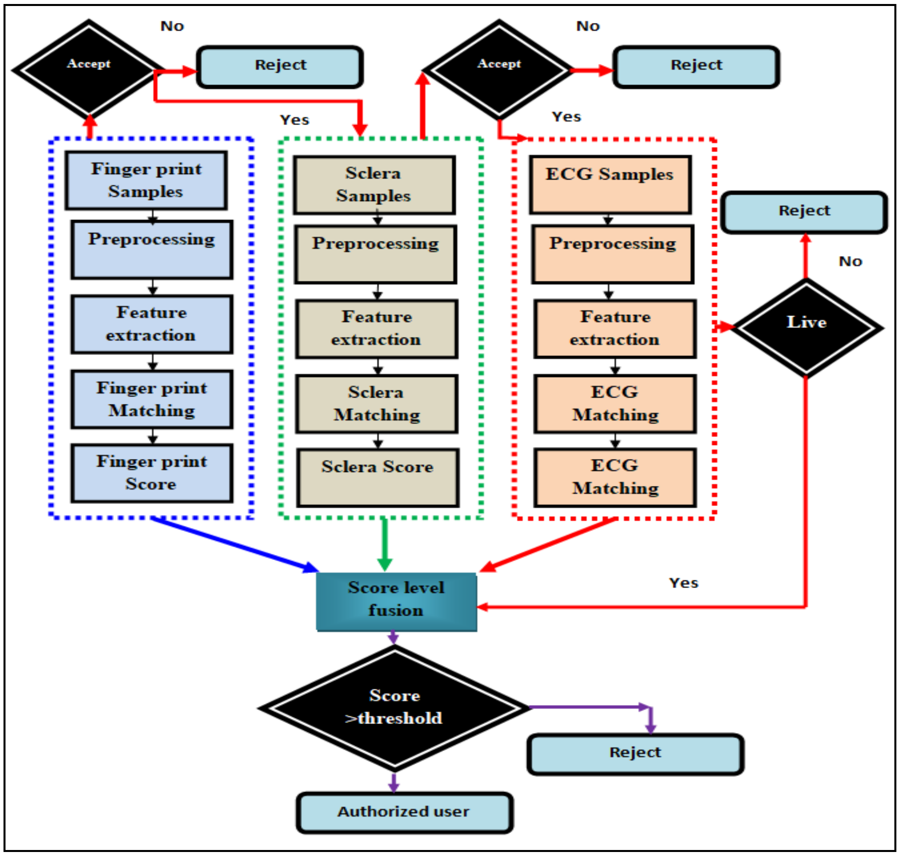



Figure 3.2: Sequential modal architecture

### 3.3.1 Parallel and sequential Model

Parallel model architecture comprises of decision making box for ECG stating that whether a person is live then proceed for fusion otherwise reject.

Sequential model architecture comprises of decision making process for each component i.e. fingerprint, sclera and ECG. It evaluates whether the finger print, sclera is matching then move further or reject the user and for ECG same as for parallel model.

### 3.3.1.1. Fingerprint

The preprocessing step for fingerprint involves noise removal by binarization, fingerprint enhancement by Gabor filter, histogram equalization, and extraction of the regions of interest. Finally normalization will be applied. Minutia Marking, Thinning, Removal of Breaks and Spikes are carried on the fingerprint to extract the features. Convolutional Neural Network (CNN) will be used for matching and generating Fingerprint score.

**A) Binarization**

The first grayscale picture is changed over into a double picture which presents the picture as a 2D dark level force capability with values going from 0 to $L-1$, where $L$ indicates all singular dim levels. Allow $\eta$ to signify the all out number of pixels in a picture and be the quantity of pixels with dim level $i$, and the likelihood that dim level $i$ might happen is characterized as

$$\Re_i = \frac{\eta_i}{\eta} \tag{3.1}$$

The unique finger impression picture dark level is found the middle value of with

$$\forall_T = \sum_{i=0}^{L=1} i\Re_i \tag{3.2}$$

In the wake of averaging, the unique mark picture pixels are characterized into two unmistakable gatherings: and with $t$ as the limit esteem. The objects of interest in the forefront and foundation of a given picture relate to the $w_1$ and $w_2$, separately. Conditions (3.3) and (3.4) are the individual probabilities:

$$w_1(t) = \sum_{i=0}^{L=1} \Re_i \tag{3.3}$$

$$and\ \ w_2(t) = \sum_{i=i+1}^{L=1} \Re_i \tag{3.4}$$

The typical dark level qualities for $w_1$ and $w_2$ are determined, separately, with the accompanying conditions:

$$\aleph_1(t) = \sum_{i=i+1}^{L=1} \frac{i\Re_i}{w_1(t)} \tag{3.5}$$

$$and\ \ \aleph_2(t) = \sum_{i=i+1}^{L=1} \frac{i\Re_i}{w_2(t)} \tag{3.6}$$

Afterward, an enhancement process is used to raise the quality of the impression.

**B) Enhancement**

Enhancement is the most common way of changing advanced pictures so the outcomes are more appropriate for show or further impression investigation.

- **Gabor filter**

Finger impression shares a few normal qualities like wrinkles and edges. Other palm print qualities are standard lines and kinks. A bank of 2D Changed Gabor channels is utilized to channel palm print and unique mark pictures every which way to feature these qualities and eliminate clamors. In Altered Gabor channels, rather than cosine capability $\cos(a;S)$ another occasional capability $f\left(a, S_1, S_2\right)$is utilized. It is formed with two cosinusoidal useful bends with various periods $S_1$ *and* $S_2$. The parts over the x-pivot comprise of a cosinusoidal useful bend with a period $S_1$ and the ones beneath the x-hub comprise of another cosinusoidal utilitarian bend with various period $S_2$. A 2D Changed Gabor channel has the accompanying structure in the picture space $(a,b)$ as displayed in (3.7) and (3.8), where $a$ and $b$ are pixel organizes, and $\phi$ is the nearby direction of current pixel:

$$\Im(a,b,S_1,S_2,\phi)\Im(a,b,S_1,S_2,\phi)=\hbar_a''(a,b,S_1,S_2,\phi)\hbar_a''(b,\phi) \tag{3.7}$$

$$\Im(a,b,S_1,S_2,\phi)=\left[\exp\left(\frac{-a\phi^2}{\alpha_a^2}\right)f(a,\phi,S_1,S_2)\right]\left\{\exp\frac{-b\phi^2}{\alpha_b^2}\right\} \tag{3.8}$$

Where,

$$a\phi = a\cos\phi + y\sin\phi,\;\; b\phi = -a\sin\phi + y\cos\phi \tag{3.9}$$

- **HE**

For tunning the force appropriation that comprises those pixel values, the phase that need to accomplish is histogram leveling. Consolidating the force of fluffy histogram balance with combined histogram evening out, thus favor twofold histogram adjustment. Histogram leveling is utilized to uniformly spread pixel power histogram to increase the scope of pixels that is dynamic thus maximizes the differentiation. Combined histogram adjustment was finished before Fluffy histogram balance. a) Combined histogram evening out Succeeding are the moves toward execution for Total histogram leveling of a picture. Picture histogram is acquired first. 2. Histogram of combined conveyance capability is acquired. For each dim worth of unique picture, another relating esteem is found by histogram adjustment recipe.

Absolute number of pixels = $\ell$

Complete number of conceivable power levels= $\xi$ then

$$\wp_k = \frac{\xi}{\ell} * c_R(k) - 1 \tag{3.10}$$

Now the enhanced image of fingerprint $\wp_k = [\wp_{1x1}, \ldots\ldots \wp_{1xn}]$ is followed with feature extraction $\rho(\wp_k) = \rho_k[\wp_{1x1}, \ldots\ldots \wp_{1xn}]$.

**C) Feature extraction**

Feature extraction helps to extract knowledgeable feature in order to avoid high error rate which leads to inaccurate authorization of user.

- **Minutiae Extraction**

The build of Crossing number (CN) is wide utilized for separating the random data. Crossing number procedure limits the misleading acknowledgment rate (FAR). As edges have almost hundred and fifty choices and peculiarity, it's more straightforward to look throughout the different random data assortments of the unique mark . As a general rule, for each 3x3 window, on the off chance that the focal picture component is one and has explicitly three one-esteem neighbors, then, at that point, the focal picture component might be an edge branch. In the event that the focal picture component is one and has just a single one-esteem neighbor, then the focal picture component might be an edge finishing (i.e., for an image component $\rho$, in the event that $\lambda n(\rho) = 1$ it's an edge finish and assuming that $\lambda n(\rho) = 3$ it's an edge bifurcation point).

$$\lambda n = 0.5 \sum_{i=1}^{8} |\rho_i - \rho_{i+1}| \tag{3.11}$$

Matching is material just during distinguishing proof or confirmation after they gave unique mark has been handled. This step finishes up the finger impression acknowledgment process.

- **Normalization**

Match scores from unique finger impression module while utilizing Suprema range from 0 to 1. Thus prior to continuing with combination, the match scores from finger vein module should be standardized, since these scores range from 0 to ∼500 (note that these address distances). We utilize twofold sigmoid capability for score standardization which maps they got scores to stretch [0, 1]. The standardized score utilizing twofold sigmoid is then given as follows.

$$\forall_k^{/}(\lambda n) = \begin{cases} \dfrac{1}{1+\exp\left(-2\left(\forall_k - t\right)/R_1\right)} & if \forall_k < t \\ \dfrac{1}{1+\exp\left(-2\left(\forall_k - t\right)/R_2\right)}, & otherwise \end{cases} \tag{3.12}$$

Where, $t$ is the reference working point and $R_1$ and $R_2$ signify the left and right edges of the area where the capability is direct, i.e., the twofold sigmoid capability shows straight attributes in the stretch ( $\left(t-R_1, t-R_2\right)$. Esteem $t$ is for the most part decided to be some worth from the district of cross-over between the veritable and fraud score conveyance, while $R_1$ and $R_2$ are made equivalent to the degree of cross-over between the two disseminations toward the left and right of $t$, individually.

### 3.3.1.2 Sclera

Sclera is second component used by the multimodal in this work. Sclera image is also preprocessed to avoid high error rate. Preprocessing comprises of:

**A) Normalization**

Standardization accomplishes the straight change of the picture to squeeze into a specific reach. Here, Min-max standardization strategy is used for the normalization of picture which straightly changes the data. Min-Max standardization is finished through the going with condition (1):

$$Q = \frac{\tilde{X} - \tilde{X}_{\min}}{\tilde{X}_{\max} - \tilde{X}_{\min}} \tag{3.13}$$

Where, $\tilde{X}_{\min}$ and $\tilde{X}_{\max}$ are the base and greatest qualities in picture $\tilde{X}$ , where $Q$ is the standardized picture.

**B) Bilateral filter**

The two-sided channel takes a weighted amount of the pixels in a close by neighborhood; the loads relied upon the spatial distance and the power distance. Unequivocally, at a pixel area x, the result of a two-sided channel is figured as follows:

$$F(X) = \frac{1}{C} \sum_{Y' \in N(X')} e^{\frac{-\|Y'-X\|^2}{2\sigma_R^2}} e^{\frac{-\|F(Y')-F(X)\|^2}{2\sigma_K^2}} \tag{3.14}$$

where, $\sigma_R^2$ and $\sigma_K^2$ are boundaries controlling the tumble off of loads in spatial and power spaces, separately, $N(X')$is a spatial neighborhood of pixel $F(X)$, and $C$ is the standardization steady. This Reciprocal channel is generally used for smoothing the picture in the space of low variety varieties that would further develop division.

#### 3.3.1.3 ECG

ECG is third component used by the multimodal in this work. ECG image is also preprocessed to avoid high error rate. Preprocessing comprises of:

**A) Median Filter**

The focal thought of the middle channel is on having the info signal by input and supplant every section with the middle of the adjoining passages. The neighbors style termed the "window" that slide, section by passage, alongside the whole sign. For one-Layered (1D) signals, the central window obvious is the essential few going before and succeeding sections, in the interim two-Layered (2D) or higher-layered plans are feasible. It's vital to inform that assuming the windows have passages with odd qualities, the middle is assessed effortlessly and basically attempted the sections by explored window mathematically. To get unpretentious scope of sections, there are more than 1 potential middle. The result of non-recursive channel at some degree is that the middle worth of the info information inside the window centered at the point.

If " $X(k) \leq k \geq L$ and $Y(k) \leq k \geq L$ ", respectively, the info and result of the one-Layered (1-D) SM channel of window size $2N+1$, then:

$$Y(k) = mid\{X(k-N),.......X(k-1), X(k), X(k+1),.....X(k+N)\} \qquad (3.15)$$

For account start and last impact, $X(N)$ and $X(1)$, individually are rehashed N times toward the beginning and toward the completion of the info..

**B) QRS Extraction**

Profound learning procedures demonstrated their effectiveness in excess of a space. The stacked auto encoder brain network can be used in our identifier; it is a connection of heterogeneous and homogeneous brain organizations. The encoder layers is consisted within homogeneous organizations. The softmax classifier that put later the last encoder layer is termed as the heterogeneous part. A basic (shallow) auto encoder is made up of three layers, namely, the primary layer is the input, the second layer is the hidden layer, and the last one is the reconstruction layer (output). In general, it is trained greedily, if the auto encoder has more than one hidden layer. Fig. 1 illustrates the average stacked auto encoder structures. Provided information $X$ , the relating yield $Y$ of a brain network is

$$Y = wX + b \tag{3.16}$$

In which, $X$ the columns of the framework, $w$ indicates the loads connecting the info hubs to the comparing hub from the secret layer, $f$ is the enactment capability, and $b$ is the predisposition vector. The point of enhancement comprises in tracking down the weight grid $w_e$ that maps the contribution to the secret layer (encoder) and the weight framework $w_d$ that recreates the contribution from the secret layer (decoder), that is

$$\arg\min_{w_e w_d}\left(f_d\left(w_d f_e\left(w_e X + b_e\right) + b_d\right) - X\right)^2 \tag{3.17}$$

Eq. (3.17) reflects that the outcome from every layer is the consequence of network increase of the information vector with the encoder weight framework, and afterward an inclination vector is added. Essentially, the result of every decoder layer is a grid increase of the result of the point of reference layer and the decoder weight lattice, and afterward an inclination vector is added. The consequence of every hub in the design is gone over an enactment capability. The goal capability utilized for driving the streamlining of the auto encoder is the squared contrast among the information vector, $X$, and the result of encoder-decoder phases. Basically, the auto encoder brain network is a solo learning framework which attempts to imitate a duplicate of its contribution at the result with no requirement for marked examples. The principal objective of building auto encoder engineering is for looking for an inborn portrayal of the information that can't be found by hand-created highlights. The bottleneck stowed away layer is taken advantage of as a productive arrangement of programmed highlights. As referenced over, every secret layer is pre-prepared alone, and afterward every layers are stacked organized to construct the acknowledgment framework. Practically speaking, just the encoder layers are utilized for the stacked auto encoder. In the wake of linking both the encoder layers and the softmax classifier layer, the entire framework is tweaked in a supervised

$$err = \frac{1}{2}\sum_{i=1}^{N}\left(Y_i - t_i\right)^2 \tag{3.18}$$

Where $Y_i$ address the anticipated results, $t_i$ the objectives (wanted yields) and $N$ is the quantity of results. The scaled form slope improvement calculation was utilized for ravenous preparation stages. It was picked for its straightforwardness of execution and low algorithmic intricacy. Furthermore, the scaled form inclination is more powerful, against introductory supposition decisions, than a straightforward slope plunge technique. The slope update of the loads is evaluated by the accompanying conditions:

$$w_{k+1}^{i} = w_{k}^{i} + \beta\nabla g^{i} \tag{3.19}$$

In Eq. (19), the loads of layer $i$ at the time of $k$th emphasis are refreshed by the inclination plunge $\nabla g$, succeeding a stage size $\beta$. The slope drop is figured beginning from the result layer in the regressive course till arriving at the info layer. This calculation is rehashed a few times until combination is reached. It has been demonstrated in many examinations that the back spread is exceptionally effective in preparing multi-facet structures. The worth of the inclination that limits the mistake is executed by:

$$\nabla g^i = \min_{w^i} e^i = -\frac{de^i}{dw^i} \tag{3.20}$$

Without a doubt, the encoder layers pre-preparing exactness isn't significant. Continuously, a tweaking stage is performed including all beforehand pretrained brain network layers. Notwithstanding, for the last tweaking stage, the Levenberg-Marquardt is utilized rather for its greater exactness, intermingling strength, and semi-independency from starting speculation. Practically speaking, the back spread way to deal with limiting the mean squared blunder accomplishes great execution to the detriment of slow union. To speed up the assembly, cross-entropy capability was utilized to appraise the blunder at the result of the softmax layer, which is the last coming about highlight from the encoder layers.

### 3.3.2 Parallel fusion

Parallel fusion uses optimized Deep Belief Network (DBN) will be utilized for the parallel fusion. The Relu activation function of the DBN will be optimized using Salp Swarm Algorithm (SSA). The optimized DBN classifier will be utilized for obtaining the scores of every biometric model. This is followed by the fusion rule among ECG scores, Sclera scores, and fingerprint scores to have the end score.

The DBN classifier is created by utilizing one multi-facet Perceptron (MLP) layer and two Restricted Boltzmann machines (RBMs) layers as portrayed in Fig 3.3. The associations are put among the covered up and the apparent neurons in the DBN classifier and there are no associations are done among the secret neurons and among the apparent neurons. The score level combination yield is provided as the contribution for the primary RBM. The result got from the secret layer of the primary RBM is exposed to the contribution of the apparent layer in the subsequent RBM and the result from the subsequent RBM is taken care of to the info layer within the MLP layer. The noticeable layer that has the element vector as its feedback, and the secret layer of the principal RBM can be evaluated as,

$$z^{I} = \left\{ z_j^{e}, z_j^{f}, z_j^{i} \right\} \tag{3.21}$$

$$F^{I} = \left\{ F_1^{I}, F_2^{I}, \ldots\ldots F_n^{I} \ldots\ldots F_r^{I} \right\}; 1 \le n \le R \tag{3.22}$$

Where, $M_1^{Q}$ addresses the $Q^{th}$ apparent RBM 1 neuron, $F_n^{I}$ signifies the nth secret layer, and $R$ be the aggregate sum of stowed away neurons. Every neuron in the secret layer and noticeable layer has a predisposition. Look at band as an allude to predispositions in covered up and the noticeable layer. The two predispositions connected with neurons in the two layers for RBM 1 is given by,

$$X^{I} = \left\{X_{1}^{I}, X_{2}^{I}, \ldots\ldots X_{Q}^{I} \ldots\ldots X_{Z}^{I}\right\} \tag{3.23}$$

$$Y^{I} = \left\{Y_{1}^{I}, Y_{2}^{I}, \ldots\ldots Y_{Q}^{I} \ldots\ldots Y_{Z}^{I}\right\} \tag{3.24}$$

Where, $M_1^Q$ be the inclination with $Q^{th}$ noticeable layer, and $Y^I$ intensifies the predisposition connected with $n^{th}$ secret layer. For the primary RBM, the weight vector is given as,

$$w^{I} = \left\{w_{QN}^{I}\right\}; 1 \leq Q \leq Z; 1 \leq 1 \leq R \tag{3.25}$$

Where, $w_{QN}^I$ signifies the nth hidden neuron's weight and $Q^{th}$ noticeable neuron, and the weight vector component is indicated as z × r. Subsequently, the result of the secret layer is processed in view of its loads and predisposition relating to each apparent neuron as,

$$F_{N}^{I} = \wp\left[b_{n}^{1} + \sum z^{I} w_{QN}^{I}\right] \tag{3.26}$$

Where, the actuation capability is addressed as σ. Subsequently, the result acquired in the main RBM is evaluated as,

$$F^{I} = \left\{F_{n}^{I}\right\}; 1 \leq n \leq R \tag{3.27}$$

From that point onward, the educational experience of RBM 2 starts utilizing the result of the secret layer of the underlying one. The apparent neuron's aggregate sum is equivalent to the aggregate sum of stowed away RBM 1 neurons and is addressed as,

$$z^{2} = \left\{z_{1}^{2}, z_{2}^{2}, \ldots z_{N}^{2}\right\} = \left\{F_{n}^{I}\right\}; 1 \leq n \leq R \tag{3.28}$$

The second RBM stowed away layer portrayal is communicated as,

$$F^2 = \{F_1^2, F_2^2, ......F_n^2.\}; 1 \le n \le R \tag{3.29}$$

The secret layer and apparent layer predisposition have similar portrayals given in Eqs. (3.28) and (3.29), . The load in second RBM layer is communicated as,

$$w^2 = \{w_{NN}^2\}; 1 \le Q \le Z; 1 \le 1 \le R \tag{3.30}$$

Where, $w_{NN}^2$ be the load among nth secret neuron and $N^{th}$ noticeable neuron in the RBM 2 layer. The element of the weight vector is signified. The result of the secret neuron is resolved in light of the principal case as,

$$F_N^2 = \wp\left[b_n^2 + \sum z^2 w_{QN}^2\right] \forall M_Q^2 = F_N^1 \tag{3.31}$$

Consequently, the result got from the secret layer is communicated as,

$$F^2 = \{.F_n^2\}; 1 \le n \le P \tag{3.32}$$

Eq. 3.33 is evaluated as the contribution to MLP, in which, addresses the aggregate sum of neurons existed in the info layer. The input of the MLP layer is evaluated by,

$$\hbar = \{\hbar_1, \hbar_2, ..\hbar_N\} = \{.F_n^I\}; 1 \le n \le P \tag{3.33}$$

Where, addresses the aggregate sum of neurons that is offered to the secret layer result of the subsequent RBM. The secret layer of MLP is communicated as,

$$t = \{t_1, t_2, ..t_P...t_U.\}; 1 \le P \le U \tag{3.34}$$

In which, $U$ indicates the quantity of secret neurons. Allow us to review YP signifies the predisposition of $P^{th}$ stowed away neurons, in which $P = 1,2,...U$ = 1, 2… Q. The MLP result is communicated as,

$$o = \{o_1, o_2, ..o_z ...o_U.\}; 1 \le z \le U \tag{3.35}$$

In which, $U$ means the complete neurons in the result

The MLP comprises of two weight vectors, one among the covered up and include layer, and the other among yield and secret layer. Contemplate $w^j$ is the weight vector among the information and secret layers, as addressed as,

$$w^j = \{w^J_{N^P}\}; 1 \le K \le m; 1 \le r \le x \tag{3.36}$$

Where, $w^J_{N^P}$ be the load among $j^{th}$ input neuron and $P^{th}$ stowed away neuron so the size of $w^j$ is $r \times x$. In view of loads and predisposition, the result of the secret layer is figured as,

$$h_r = X_r \left[ \sum_{n=1}^{r} h_n w^J_{jr} \right] \forall h = F^2_N \tag{3.37}$$

Where, $\varphi_r$ indicates the inclination of stowed away neurons which is optimized by SSA and $h_n = F^2_N$, so the contribution to the MLP is the aftereffect of RBM 2. The loads among the result layer and secret layer are communicated by,

$$w^L = \{w^L_{r^z}\}; 1 \le K \le m; 1 \le r \le x \tag{3.38}$$

The result vector is determined in view of the result of the secret layer, and the weight $w^L$ , as provided underneath,

$$O_z = X\left[\sum_{r=1}^{Q} h_r w_{rz}^L\right] \tag{3.39}$$

Where, $w_{rz}^L$ be the load between $P^{th}$ covered up and $z^{th}$ output neuron, and the secret layer yield is indicated as $h_r$ .

Now the Relu activation function is replaced by Salp swarm algorithm. The Salp has a place with the Salpidae family. Similar to how fish swim in schools [18] Salps structure chains to advantage their outcome in taking care of, security, motion, and multiplication. The SSA conduct is determined by working out it with the Salp chain look for ideal food sources. In SSA, in light of the person (that is slaps) position in the chain, they are isolated into supporters or pioneers. The chain is started by the pioneer while devotees submit to bearings for their development.

The proposed strategy outlines the SSA, where the closeness to one more multitude smart calculation and the effortlessness of SSA are shown. At the point when it began with the Salp populace instatement, the multitude of Salp is epitomized as 2D network. Then, the Salp wellness can be assessed for deciding the Salp utilizing the ideal wellness (that is., pioneer). The pioneer area can be overhauled by

$$O_t = \left[O_1^1 O_2^1 \ldots O_d^1 O_1^2 O_2^2 \ldots\ldots O_d^2 : O_1^n : O_2^n \ldots\ldots O_d^n\right] \tag{3.40}$$

$$O_1^1 = \left[Y_i + E_1((U_i - L_i))E_2 + L_i)E_3 \geq 0 Y_i + E_2((U_i - L_i))E_2 + L_i)E_2 \geq 0Y\right] \tag{3.41}$$

Here, address the area of starting Salp in ith boundary and means the food area in ith boundary. What’s more, addresses the lower and upper limits of ith boundary, correspondingly, likewise the coefficient is assessed by the accompanying condition. $E_1$ and $E_2$ also, signifies irregular qualities inside [0, 1].

$$E_1 = 2e^{-(\Delta l / L)^2} \tag{3.42}$$

Here, $L$ addresses the maximal emphasis and $l$ shows the current cycle. It is eminent that the coefficient is critical in SSA since it adjusts investigation and abuse in the entire looking through technique.

$$X_i^j = \frac{1}{2}vt^2 + \Phi_0 t \tag{3.43}$$

Here, $j \geq 2, \Phi_0$ signifies an underlying pace, address the area of $j^{th}$ Salp in ith aspect, addresses the time and while. During improvement, $E_1$ the time shows the cycle. Consequently, the inconsistency among cycles is identical to 1. Consider the supposition that $\Phi_0$ =0, the resulting equation is used.

$$X_i^j = \frac{1}{2}(X_i^j - X_i^{j-1}) \tag{3.44}$$

While $j \geq 2$ assuming some Salp moves beyond the looking through space condition (6) exhibits how to return them to the looking through space

$$X_i^j = \{l^j \ if \ (X_i^j \leq l^j s^j \ \ if \ \ X_i^j \geq l^j s^j \ otherwise) \tag{3.45}$$

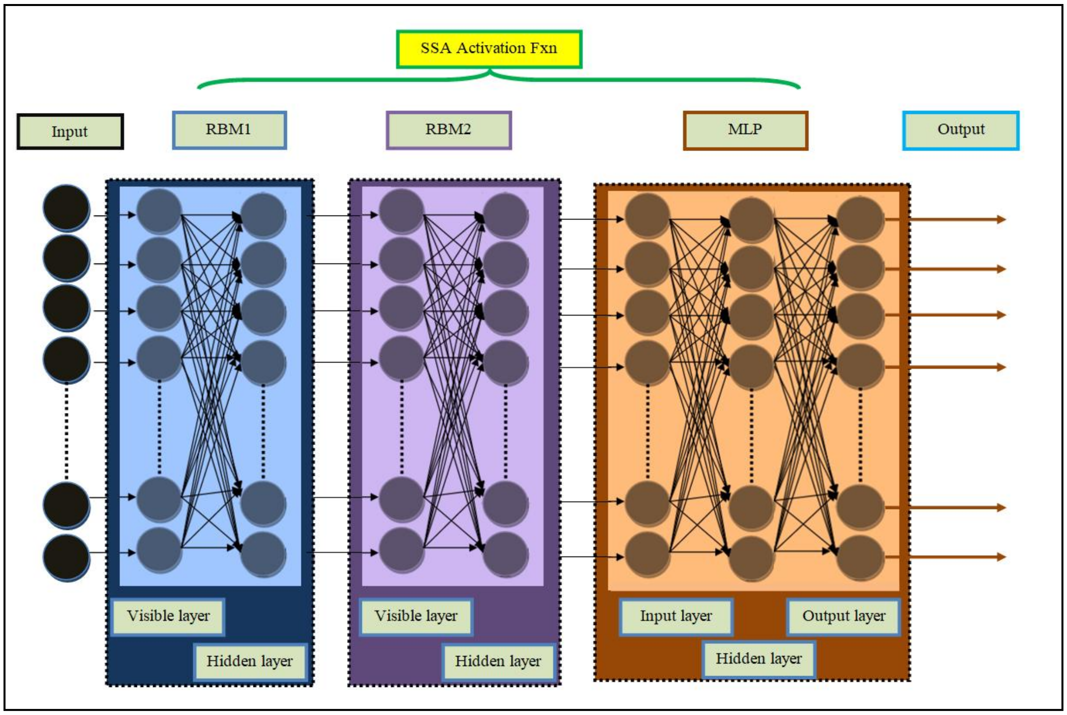



Figure 3.3: Proposed SSA_DBN Architecture

### 3.3.3 Sequential Fusion

An optimized Artificial Neural Network (ANN) is utilized for the sequential fusion. The Sigmoid activation function of the ANN will be optimized using Whale Optimization Algorithm (WOA). By the effective employing of OR Rule, the decision outputs combination is attained for achieving the superlative performance.

Building forecasting models is equivalent to determining the output variable that provides the best estimate of the target value given the known inputs. Typically, environmental monitoring involves a vast number of characteristics influencing the target, and the relationship between inputs and outputs is not linear. Different forecasting methodologies are available, with ANN being picked based on comparative analysis offered in past study work for various forecasts. Developing a prediction model is part of machine learning techniques that necessitate a large training dataset.

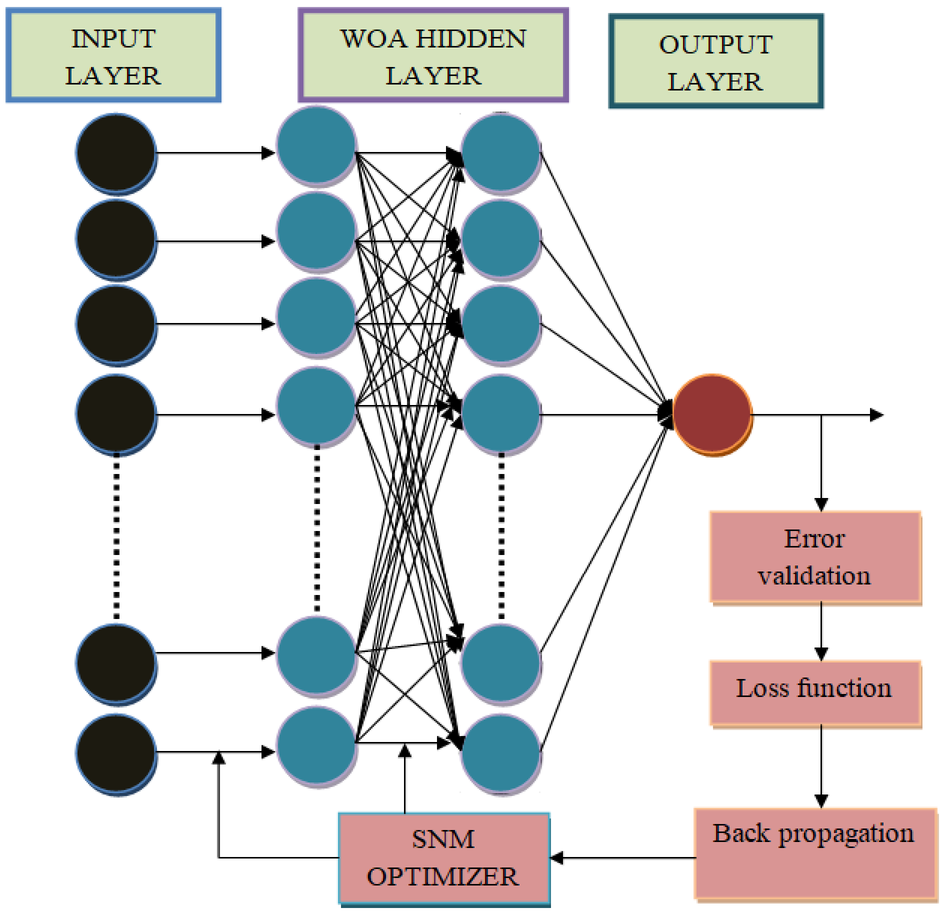



Figure 3.4: Proposed WOA-ANN Architecture

For pattern p ($\zeta net$), the net input to hidden layer neuron is calculated as the average of every emission of the input neurons ($\Gamma_{p,i}$; input value) multiplied by weight ($O_{p,ji}$). An activation function calculates the output of the neuron $j$, of the hidden layer ($act_{\Gamma,j}$) and the output of the neuron $k$, of the output layer ($o_{p,k}$) for pattern p as follows :

$$T_{WOA} = Lw_{t+1} \tag{3.46}$$

In which, activation function coefficient of WOA is $T_{WOA}$, and NET is described as $act_{\Gamma,j}$ or $o_{p,k}$ as per the following:

$$act_{\Gamma,j} = T\left(\sum_i \Gamma_{p,i} \mathrm{O}_{p,ji}\right) \tag{3.47}$$

$$o_{p,k} = T\left(\sum_j act_{p,j} w_{p,kj}\right) \tag{3.48}$$

Where, $\mathrm{O}_{p,ji}$ and $w_{p,kj}$ are the weights of the connections among input layer neuron $i$ and hidden layer neuron $j$, and among hidden layer neuron and output layer neuron $k$, correspondingly. Weights are set to modest random numbers at the start. Because of its sigmoid, nonlinearity functions are commonly employed. To minimize error, the learning algorithm updates the weights ($\mathrm{O}_{p,ji}$ and $w_{p,kj}$)).

The error's sum ($e_p$) in every neuron in pattern p is estimated as per the following:

$$e_p = \frac{1}{2}\sum_k \left(g_{p.k} - o_{p,k}\right)^2 \tag{3.49}$$

$$te = \sum_p e_p \tag{3.50}$$

Where $g_{p.k}$ represents the target value for sequence at synapse $k$ and $te$ is the overall error. With a forward process the activation level computations pass over the hidden to the output layer (s). Every neuron in every subsequent layer combines its data and afterwards performs a frequency response to generate its outcome. The channel's activation function subsequently generates the conclusive result, which is the projected goal value.

Each neuron's error value contains the amount of error associated with that neuron. As a consequence, the neurons are instructed to update for the appropriate weight adjustment. Hidden neuron weights are implemented according to the following:

$$\delta_{p,k(o)} = o_{p,k}\left(1 - o_{p,k}\right)\left(g_{p.k} - o_{p,k}\right) \tag{3.51}$$

An example of such is the period control device, which has been used in the determination of the kind of movement taken throughout time. It controls, not just the behaviour of type A and type B swarms, but that of jellyfish movements towards an approaching tide. The obligation cycle component is described in detail in the following sections. To attain the best results, the researchers employed sutskever Nesterov momentum to update the weights and learning rate.

$$w_{t+1} = w_t + \varphi_t v_t - \vartheta_t \nabla T\left(w_t + \varphi_t v_t\right) \tag{3.52}$$

Finally, the work promotes a clever activation determination model under various component properties.

Presently the Whale calculation is utilized as enactment capability as expressed in equation 3.46. The motivation is taken from the natural way of behaving of the whales that compares to the average way trailed by Whale Calculation to accomplish an upgraded arrangement. There are two periods of the calculation, abuse and investigation stage. In the abuse stage whale trails the twisting way to encompass the prey. In the subsequent stage, prey is arbitrarily looked.

## 3.4 Results and discussion

The proposed work will be implemented in PYTHON**.**The proposed model's performance will be matched to other existing models in terms of ROC, Sensitivity, Specificity, Efficiency, Likelihood ratio**.**

***Dataset:***Fingerprint: FVR 2004 **,**ECG: MIT Arthmyia **,**Sclera: http://sclera.fri.uni-lj.si/

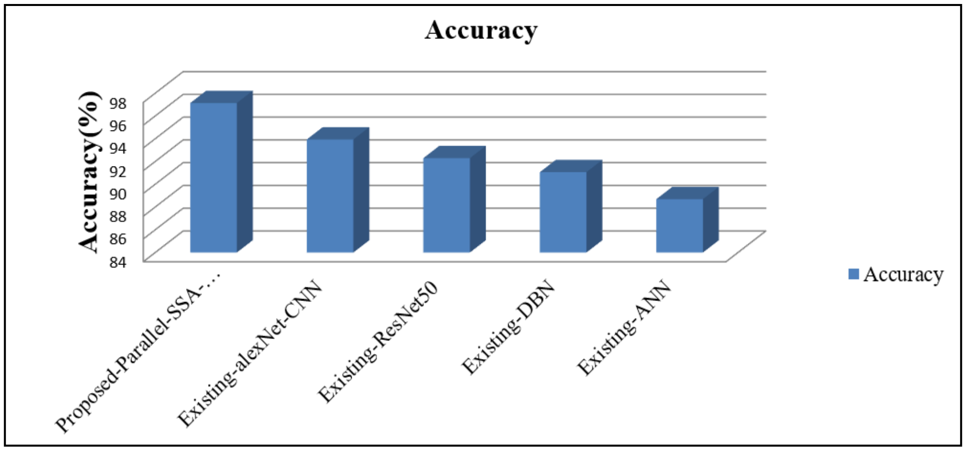
### 3.4.1 Performance Analysis of proposed Parallel model architecture

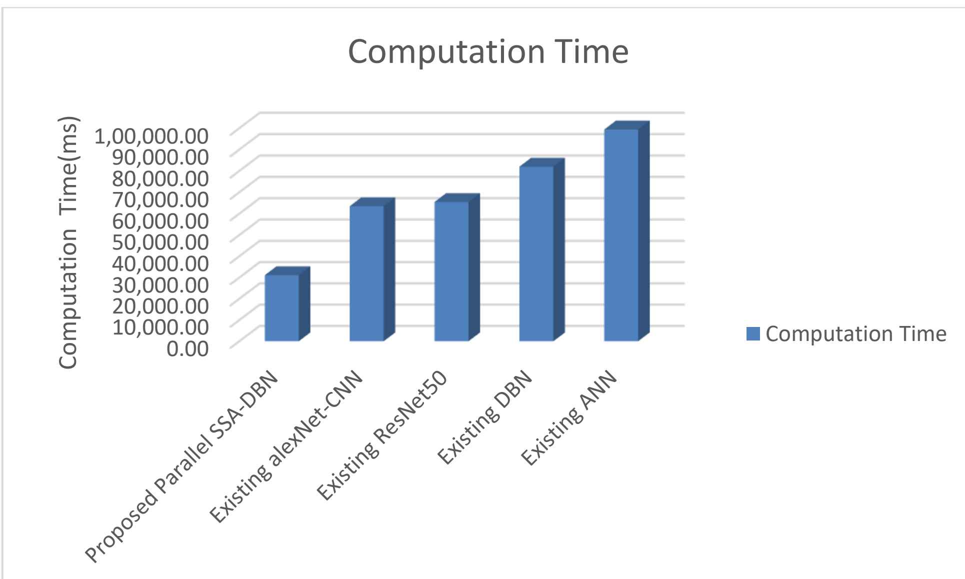
The Parallel SSA-DBN proposed is inspected fixated on the measurements like Accuracy, Sensitivity, Specificity, F-Measure, Precision, FPR, MCC, FNR, FRR, NPV, computation time and furthermore analogized with the existent techniques like alexNet-CNN, Resnet50, DBN, and ANN. Table 3.1 summarises the proposed strategy's evaluation alongside the prevalent strategies centred on authorised user recognition.

Table 3.1: Evaluation of classification metrics for Proposed-Parallel-SSA-DBN

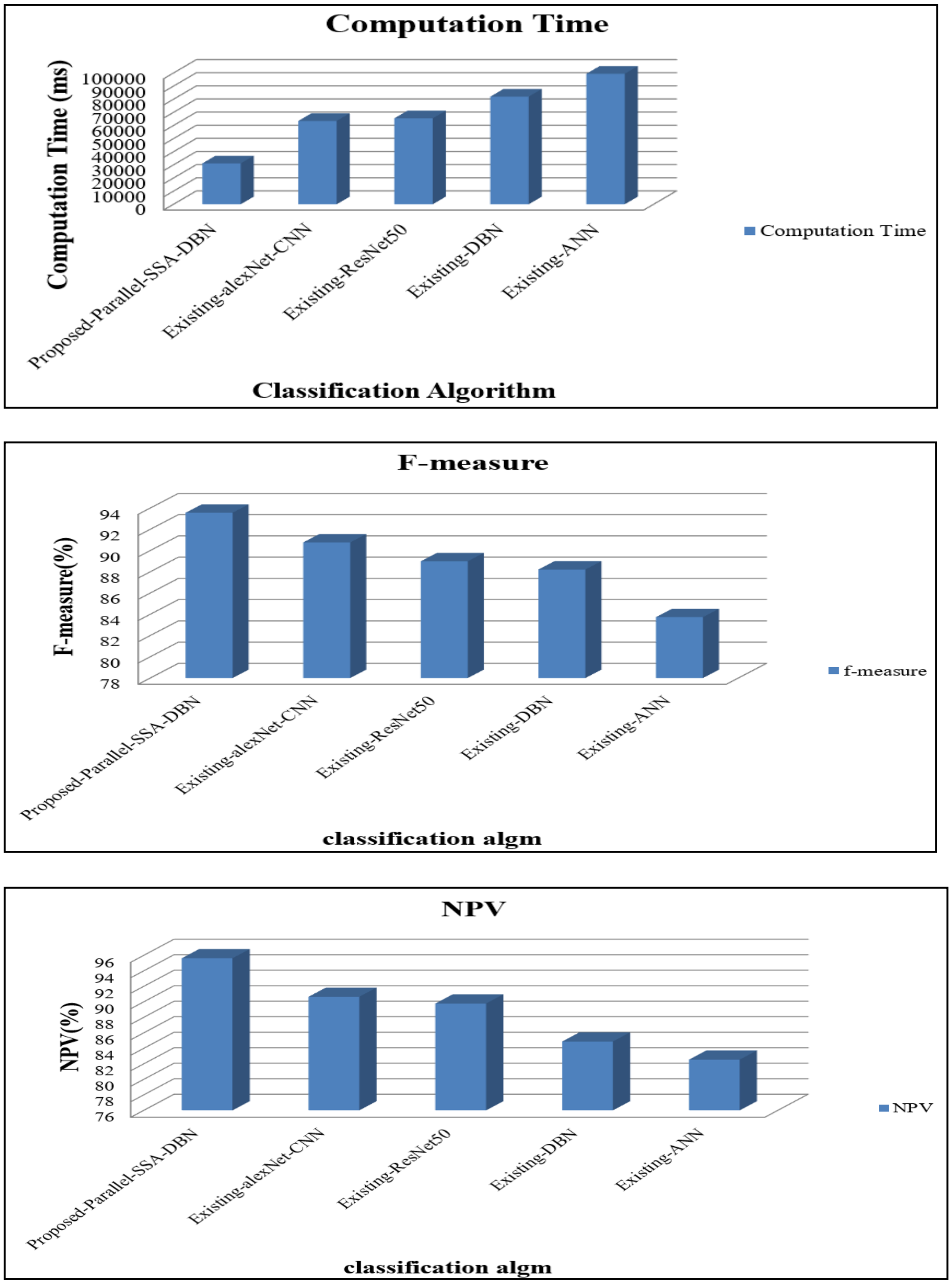
| Techniques | Recall | f-measure | NPV | Specificity | Accuracy | Precision |
|---|---|---|---|---|---|---|
| **Proposed-Parallel-SSA-DBN** | 98.12 | 93.55 | 95.62 | 96.11 | 97.13 | 96.65 |
| **Existing-alexNet-CNN** | 94.44 | 90.76 | 90.65 | 90.00 | 93.93 | 91.38 |
| **Existing-ResNet50** | 91.22 | 88.99 | 89.78 | 86.74 | 92.29 | 88.57 |
| **Existing-DBN** | 90.52 | 88.21 | 84.88 | 87.45 | 91.06 | 87.55 |
| **Existing-ANN** | 86.12 | 83.73 | 82.54 | 81.86 | 88.69 | 83.38 |

Table 3.1 displays the proposed Parallel SSA-DBN investigation fixated on different execution measurements like Accuracy, Sensitivity, Specificity, F-Measure, Precision, FNR, FPR, and furthermore NPV, FRR etc. The measurements esteem is accomplished focused on '4' fundamental boundaries, similar to genuine TP, TN, FP, and furthermore FN. As TP characterizes that the real worth isn't an assault and the worth anticipated additionally yields something similar; TN characterizes that the genuine worth is an assault and the worth anticipated likewise yields something similar; FP establishes that the genuine is an assault, but the projected value is not an assault., and FN characterizes that the genuine worth isn't an assault anyway the worth anticipated is expressing an assault. Thus, an assault's (unauthorized) assessment is totally dependent on the '4' boundaries.

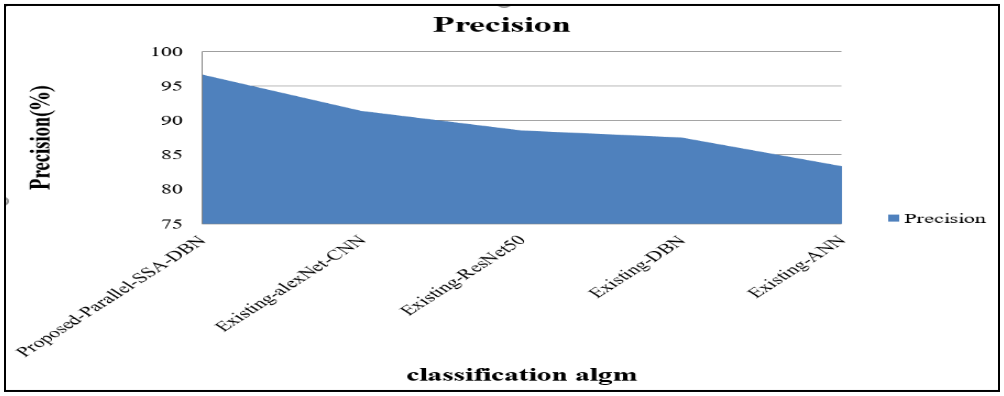

Accuracy
Accuracy(%)
98
96
94
92
90
88
86
84
Proposed-Parallel-SSA-...
Existing-alexNet-CNN
Existing-ResNet50
Existing-DBN
Existing-ANN
Accuracy

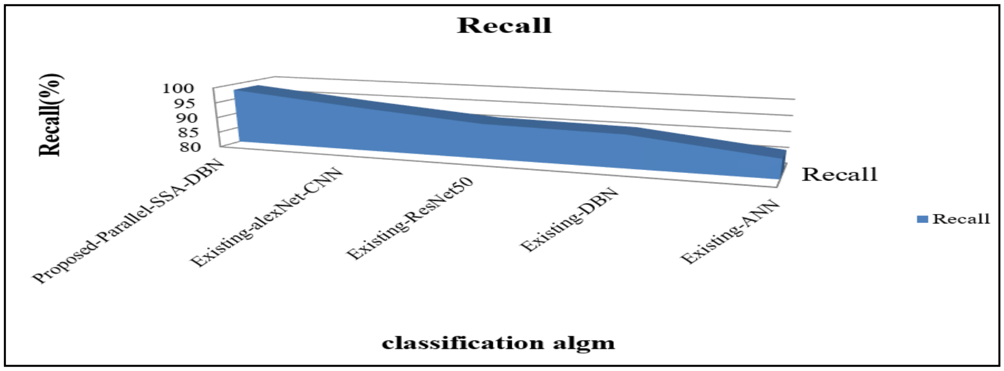

Computation Time
Computation Time(ms)
1,00,000.00
90,000.00
80,000.00
70,000.00
60,000.00
50,000.00
40,000.00
30,000.00
20,000.00
10,000.00
0.00
Proposed Parallel SSA-DBN
Existing alexNet-CNN
Existing ResNet50
Existing DBN
Existing ANN
Computation Time

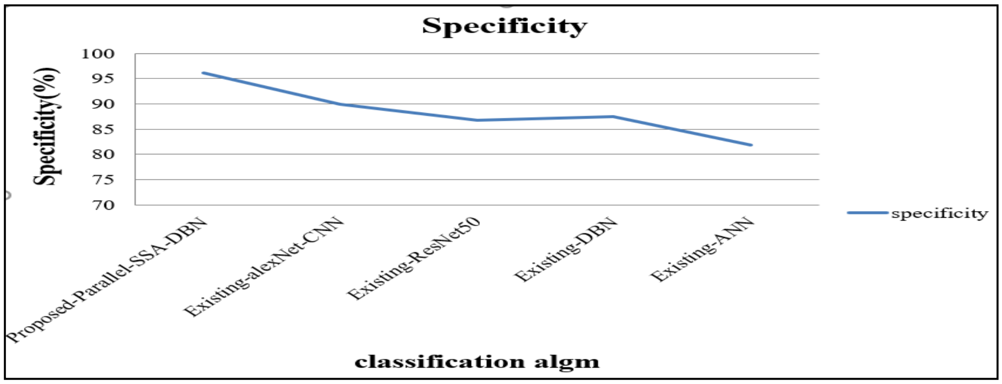
(a)


Computation Time
Computation Time (ms)
100000
90000
80000
70000
60000
50000
40000
30000
20000
10000
0
Proposed-Parallel-SSA-DBN
Existing-alexNet-CNN
Existing-ResNet50
Existing-DBN
Existing-ANN
Computation Time
Classification Algorithm
F-measure
F-measure(%)
94
92
90
88
86
84
82
80
78
f-measure
classification algm
NPV
NPV(%)
96
94
92
90
88
86
84
82
80
78
76
NPV
classification algm

(b)




(c)

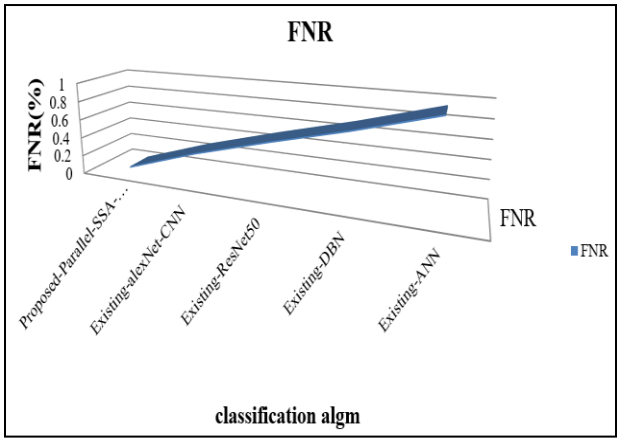
Figure 3.5:(a)(b)(c) Graphical demonstration of classification metrics for proposed method along with existing methods

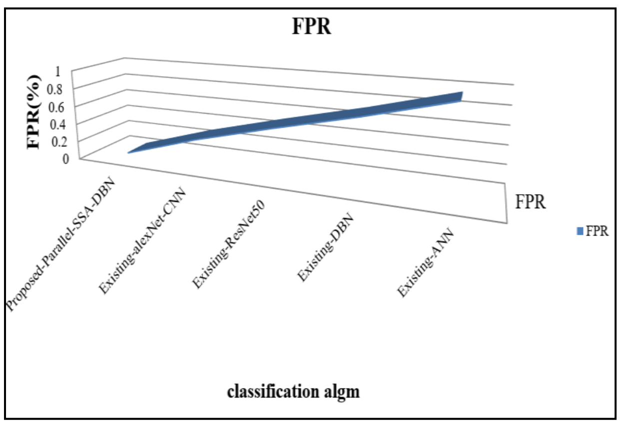
Figure 3.5 (a)(b)(c)shows the proposed Parallel SSA-DBN graphical examination along with the assorted existing methods, as alexNet-CNN, Resnet50, DBN, and ANN focused on metric i.e. specificity, accuracy, Recall, NPV, Precision and F-measure. The measurements accuracy, review embody that the work's adequacy on the assorted dataset (i.e.) the implemented order strategies' unshakable quality. With respect to, the plan proposed achieves a more noteworthy specificity, accuracy, Recall, NPV, Precision and F-measure of 98.12%,97.13%,98.12%,95.62%,96.65% and 93.55% respectively, correspondingly; in any case, the existent method achieves the metrics value running in between 81.86% - 94.44% that represents lesser plan viability as analogized to the Parallel SSA-DBN procedure proposed. In addition, the Parallel SSA-DBN proposed is broke down fixated on F-Measure measurements that depict the exactness for lopsided dispersion probability. With respect to quantify measurements, the strategy proposed yields a higher worth of for recognizing authorized user and avoids false detection rate as shown in table which leads to low mistake rate. Thusly, the Parallel SSA-DBN strategy proposed produces proficient unwavering quality and furthermore avoids assaults' misclassification as analogized to the existent procedures.

Table 3.2: Evaluation of more classification metrics for Proposed-Parallel-SSA-DBN

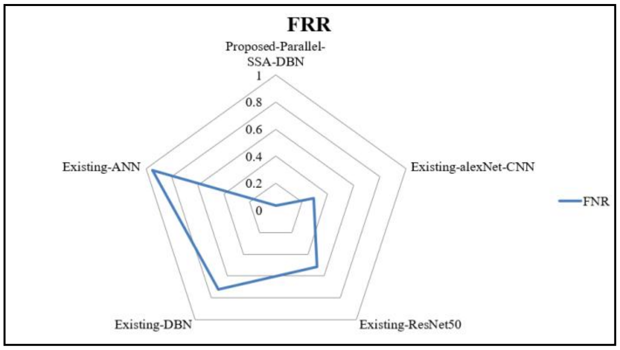
| Techniques | FPR | MCC | FRR | Computation time | FNR |
|---|---|---|---|---|---|
| **Proposed-Parallel-SSA-DBN** | 0.02 | 94.49 | 0.03 | 31117.00 | 0.03 |
| **Existing-alexNet-CNN** | 0.37 | 92.00 | 0.29 | 63474.00 | 0.29 |
| **Existing-ResNet50** | 0.53 | 91.00 | 0.51 | 65454.00 | 0.51 |
| **Existing-DBN** | 0.61 | 88.37 | 0.72 | 81986.00 | 0.72 |
| **Existing-ANN** | 0.96 | 84.89 | 0.95 | 99384.00 | 0.95 |

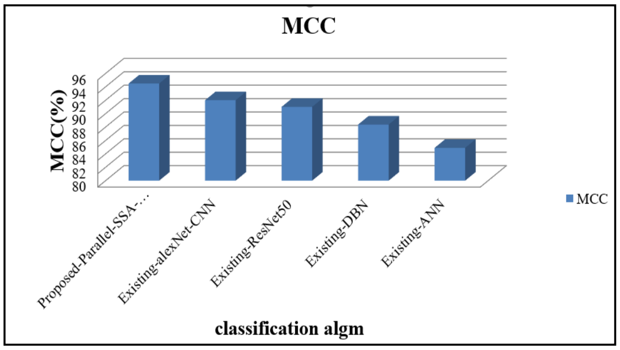
Table 3.2 discuss about the metrices such as FRR,FPR,Computation ,MCC and FNR for the Biometric authentication model. The proposed model has achieved an FRR, FPR, Computation ,MCC and FNR value of 0.03%,0.02%,31117s,94.49% and 0.03% respectively, which is better metrics value as compared to the existing methods. The outcome mainly tells about the analysis between the predicted and actual class values. A low FNR, FRR, FPR value illustrates a good model. The MCC is the proportion of subjects truly classified as negative against all the cases which returned a negative test result, including data that falsely analyzed as non-attack. This trademark can anticipate how likely it is for an information to really be gone after, in the event of a negative experimental outcome.


FNR
FNR(%)
1
0.8
0.6
0.4
0.2
0
Proposed-Parallel-SSA-...
Existing-alexNet-CNN
Existing-ResNet50
Existing-DBN
Existing-ANN
FNR
FNR
classification algm


FPR
FPR(%)
1
0.8
0.6
0.4
0.2
0
Proposed-Parallel-SSA-DBN
Existing-alexNet-CNN
Existing-ResNet50
Existing-DBN
Existing-ANN
FPR
FPR
classification algm

(a)



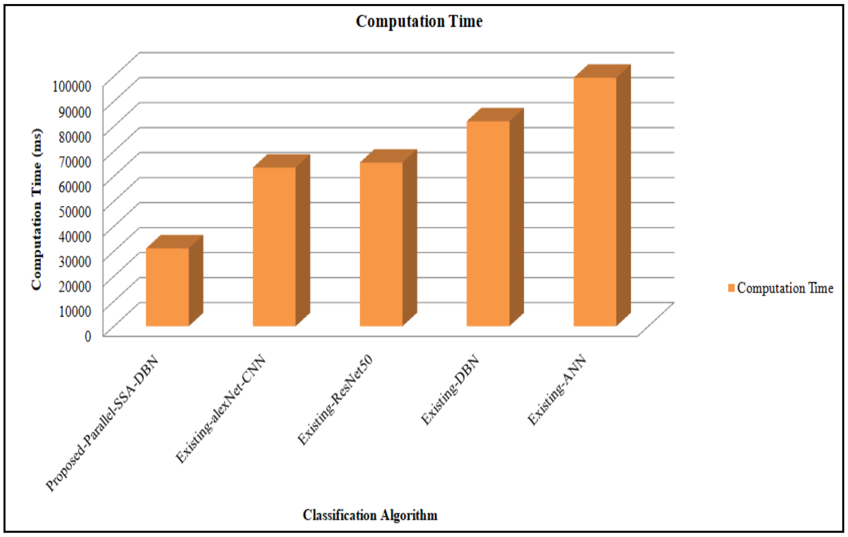




Figure 3.6(a)(b): Classification metrics Graphical Demonstration

Figure 3.6 displays the graphical assessment focused on the measurements like FRR,FPR,Computation ,MCC and FNR focused on the Parallel SSA-DBN proposed. Then, the measurements accomplished are analogized with different existent philosophies, as alexNet-CNN, Resnet50, DBN, and ANN. Focused on a plan to work successfully it should involve the possibility to yield a low FRR,FPR, and FNR esteem. Concerning, the convention proposed yields an efficient exactness, explicitness and responsiveness. The proposed strategies accomplished worth surpassed the existent techniques' accomplished the measurements values running in between 0.29 to 92% that is somewhat inefficient as analogized to the convention proposed. The Parallel SSA-DBN procedure proposed yields productive measurements worth to find the assault and shown to be efficacious analogized to the existent strategy.

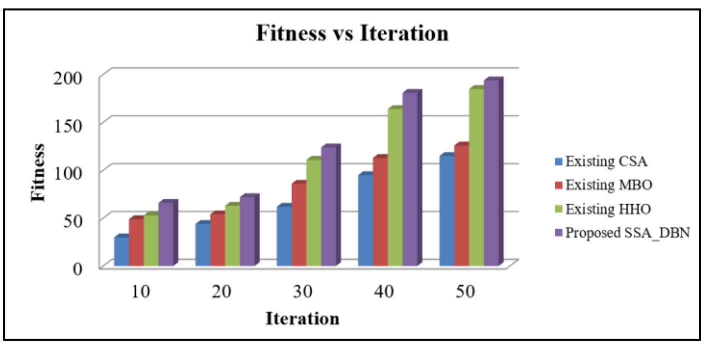



Figure 3.7: Fitness vs. Iteration for proposed Parallel SSA-DBN

Figure 3.7: Fitness vs. Iteration for the proposed method along with the existing methodology. The proposed method seems to go well with activating the neurons within high fitness value for a low number of iterations. As the proposed method tends to achieve an fitness value ranging between 66 to 194,whereas the existing

techniques achieves between 30 to 185 which is comparatively low then proposed method.

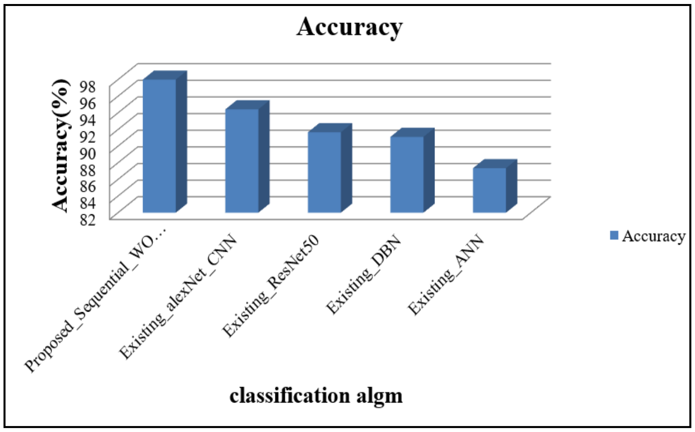
### 3.4.2 Performance analysis of proposed Sequential model architecture

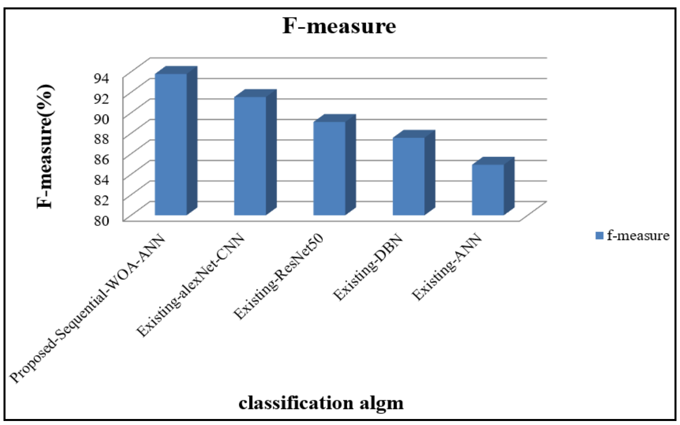
The developed Sequential-WOA-ANN is inspected based on measurements such as Accuracy, Sensitivity, Specificity, F-Measure, Precision, FPR, MCC, FNR, FRR, NPV, computation time and furthermore analogized with the existent techniques like alexNet-CNN, Resnet50, DBN, and ANN. Table 1 compares the suggested solution to common techniques for authorised user recognition.

Table 3.3: Evaluation of classification metrics for Proposed-Sequential-WOA-ANN

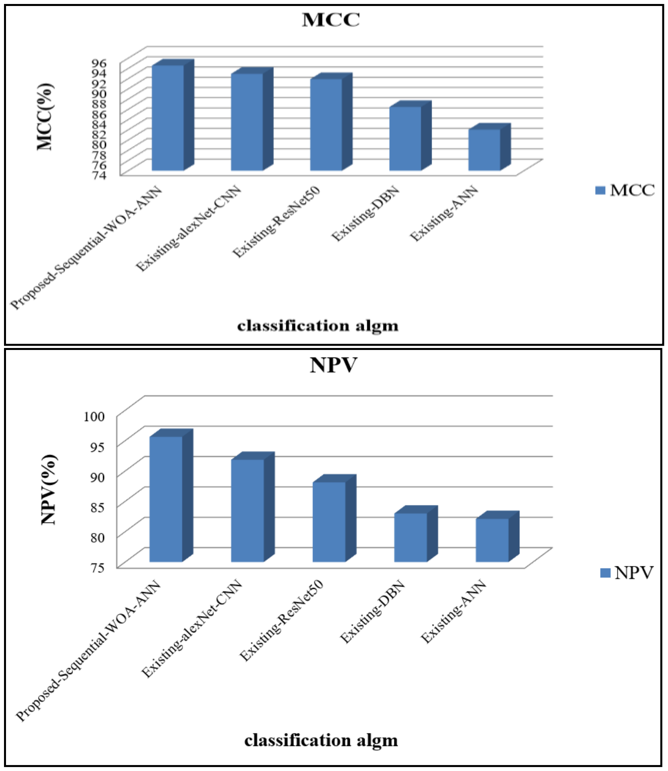
| | Specificity | Accuracy | Precision | F-Measure | NPV | MCC |
|---|---|---|---|---|---|---|
| **Proposed-Sequential-WOA-ANN** | 95.54 | 98.00 | 95.23 | 93.79 | 95.63 | 94.56 |
| **Existing-alexNet-CNN** | 91.46 | 94.42 | 90.85 | 91.54 | 91.85 | 92.95 |
| **Existing-ResNet50** | 87.00 | 91.67 | 88.86 | 89.10 | 88.13 | 91.89 |
| **Existing-DBN** | 87.69 | 91.12 | 86.11 | 87.56 | 83.00 | 86.46 |
| **Existing-ANN** | 80.18 | 87.35 | 82.94 | 84.93 | 82.11 | 82.05 |

Table 3.3 compares the suggested Sequential-WOA-ANN graphical examination to the various existing techniques, such as alexNet-CNN, Resnet50, DBN, and ANN focused on measurements, i.e. specificity, accuracy, Recall, NPV, Precision, MCC and F-measure. The measures accuracy, review include that the work's adequacy on the assorted dataset (i.e., the applied order methods consistent quality). With respect to, the plan proposed achieves a more noteworthy specificity, accuracy, NPV, Precision, MCC and F-measure of 95.54%,98.00%,95.63%,95.23%,94.56% and 93.79% respectively, correspondingly; In any event, the existing method achieves the metrics value ranging between 80.18% and 91.85%, which symbolises poorer plan viability as analogized to the Sequential-WOA-ANN procedure proposed. In addition, the Sequential-WOA-ANN is broke down fixated on F-Measure measurements that shows the exactness for lopsided dispersion probability. With respect to quantify measurements, the strategy proposed yields a higher worth of for recognizing authorized user and avoids false detection rate as shown in table which leads to low mistake rate. Thusly, the Sequential-WOA-ANN strategy proposed yields proficient unwavering quality and furthermore sidesteps assaults' misclassification as analogized to the existent procedures.

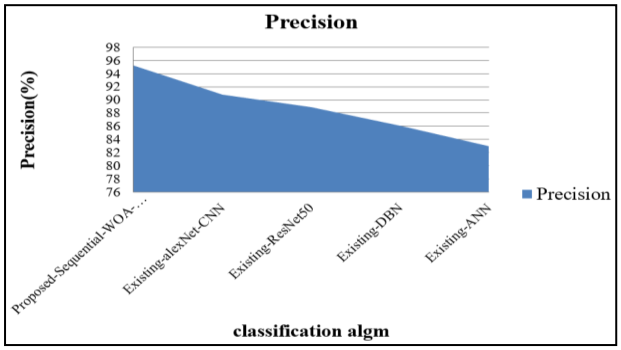

Accuracy
Accuracy(%)
98
96
94
92
90
88
86
84
82
Proposed_Sequential_WO…
Existing_alexNet_CNN
Existing_ResNet50
Existing_DBN
Existing_ANN
Accuracy
classification algm


F-measure
F-measure(%)
94
92
90
88
86
84
82
80
Proposed-Sequential-WOA-ANN
Existing-alexNet-CNN
Existing-ResNet50
Existing-DBN
Existing-ANN
f-measure
classification algm

(a)


MCC
MCC(%)
96
94
92
90
88
86
84
82
80
78
76
74
Proposed-Sequential-WOA-ANN
Existing-alexNet-CNN
Existing-ResNet50
Existing-DBN
Existing-ANN
MCC
classification algm
NPV
NPV(%)
100
95
90
85
80
75
Proposed-Sequential-WOA-ANN
Existing-alexNet-CNN
Existing-ResNet50
Existing-DBN
Existing-ANN
NPV
classification algm

(b)



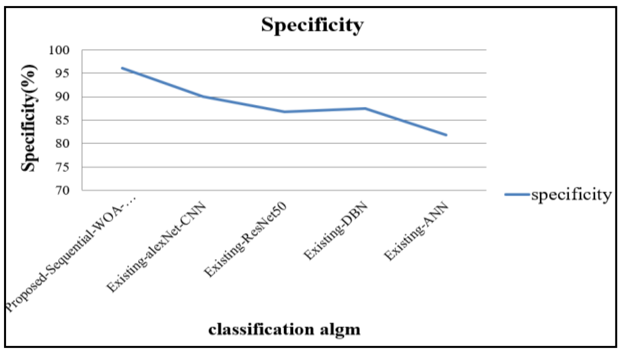




Figure 3.8(a)(b)(c): Classification metrics for Sequential model architecture

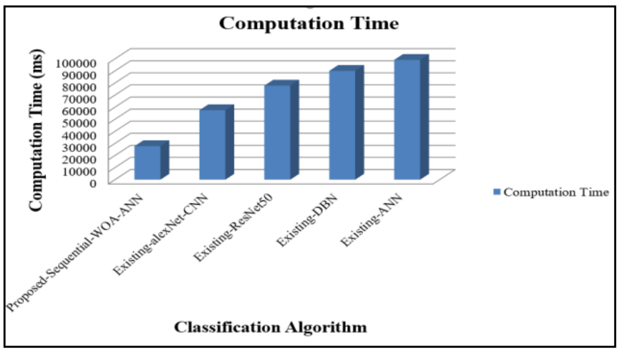
Figure 3.8 demonstrates the classification metrics for the proposed method along with the existing methodology. The proposed method tends to perform with low error rate, whereas the existing techniques achieve low metrics value which leads to low error rate.

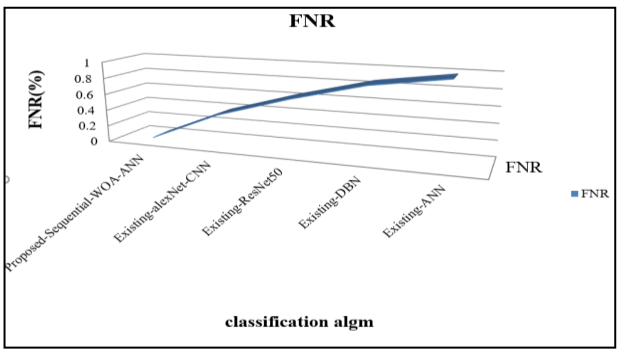
Table 3.4: Evaluation of more classification metrics for Proposed-Sequential-WOA-ANN

| | FPR | FRR | Computation Time(ms) | FNR | Recall |
|---|---|---|---|---|---|
| **Proposed-Sequential-WOA-ANN** | 0.0311 | 0.024 | 27717 | 0.02 | 98.46 |
| **Existing-alexNet-CNN** | 0.4295 | 0.388 | 57464 | 0.39 | 95.90 |
| **Existing-ResNet50** | 0.6112 | 0.644 | 77814 | 0.64 | 92.22 |
| **Existing-DBN** | 0.6966 | 0.861 | 89986 | 0.86 | 89.35 |
| **Existing-ANN** | 0.9572 | 0.986 | 99114 | 0.99 | 86.74 |

Table 3.4 shows the proposed Sequential-WOA-ANN graphical examination along with the assorted existent strategies, as alexNet-CNN, Resnet50, DBN, and ANN focused on measurements, specifically FRR, FPR, Recall, computation time and FNR. The measurements recall embody that the work's viability on the dataset (i.e.) the implemented grouping strategies' unshakable quality. As to, the plan proposed accomplishes a more prominent Recall worth of 98.46% correspondingly; nonetheless, the existent strategy accomplishes the recall esteem going in between 86.74% to 95.90% that epitomizes poorer plan viability as analogized to the

Sequential-WOA-ANN procedure proposed. Also, the Sequential-WOA-ANN proposed is examined fixated on FPR, FRR and FNR measurements that depict the misclassification's chance. Concerning and FNR measurements, the procedure implemented yields a minimum worth of 0.03 FPR 0.024 FRR and furthermore 0.02 FNR; in any case, the existent strategies yielded the FPR and FRR, and FNR values running in between 0.39 to 0.95% that caused misclassification. Thus, the Sequential-WOA-ANN strategy proposed yields effective unwavering quality and furthermore sidesteps assaults' misclassification as analogized to the existent procedures.



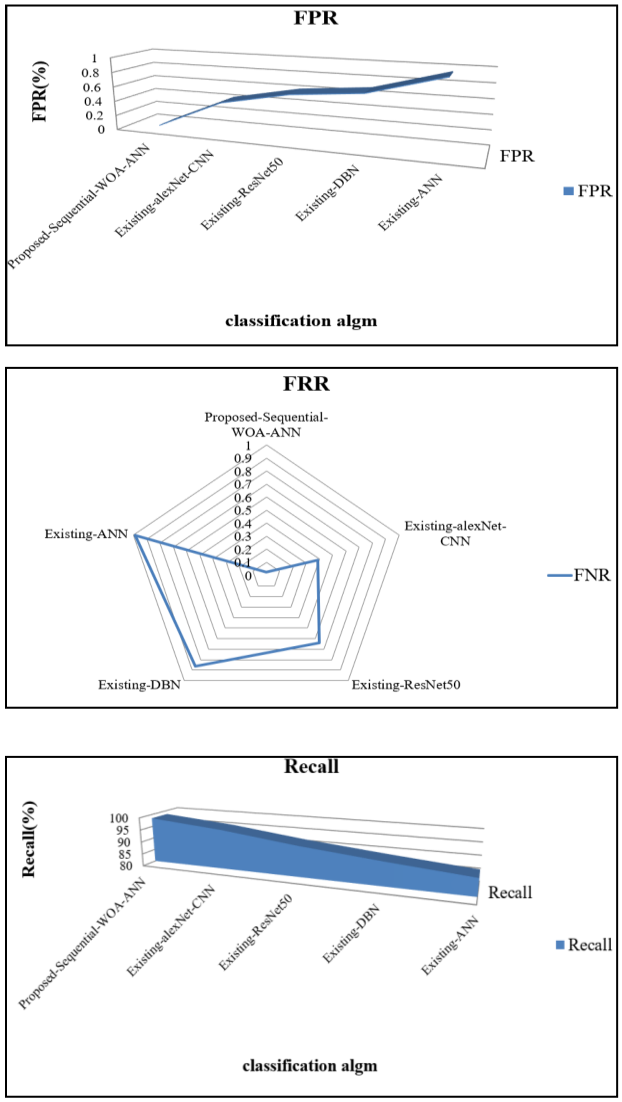



Figure 3.9: Graphical demonstration of Classification metrics for Sequential model architecture

Figure 3.9 discuss about the metrices such as FRR, FPR, Recall, computation time and FNR for the Biometric authentication model. The proportion of subjects genuinely analyzed as negative to every one of the individuals who had negative experimental outcomes (counting Data that erroneously analyzed as non-assault).

This trademark can anticipate how likely it is for an information to really be gone after, in the event of a negative experimental outcome.

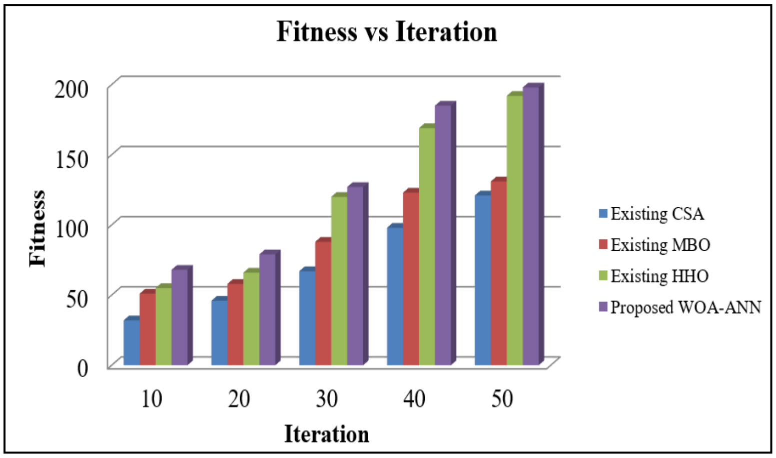



Figure 3.10: Fitness vs. Iteration for the proposed method

Figure 3.10 demonstrates the fitness vs. iteration for the proposed method along with the existing methodology. The proposed method tends to perform well for activating the neurons within high fitness value for low number of iteration. As the proposed method tends to achieve an fitness value ranging between 68 to 198,whereas the existing techniques achieves between 32 to 192 which is comparatively low then proposed method.

### 3.5 Summary

Authentication is a significant element on guaranteeing security for different applications. Multimodal biometric framework improves the vigor of the verification instrument as a result of its intrinsic one of a kind natural example. It precisely segregates the people in light of the caught design from their characteristics. Appropriately the work has created Double Multimodal Biometric validation conspires which works on the vigor of the framework, for example, getting human hereditary code and data for future reference. The proposed model avoids the data degeneration of any one of the biometric model in the multimodal biometric system which leads to degradation of the system performance. The proposed method gets adapted to variations of biometric traits and the environmental changes .Ensemble fusion method is adapted with highly efficient Feature representation and matching techniques. The model don't compromises between authentication performance, computations and cost. Experiential assessment approved that the Parallel model plan achieves 97.13% of Accuracy, 96.11% of specificity, 93.55% of f-measures and FNR of 0.03%. In addition to that the Sequential model plan achieves 98.00% of Accuracy, 95.54 % of specificity, 93.79 % of f-measures and FNR of 0.02%. Overall the sequential model tends to obtain better outcome as compared to parallel model and remains to highly secure as compared to existing techniques.

# CHAPTER 4

## A HYBRID MODEL THAT INTEGRATES HPO-ANFIS PARALLEL AND HPO-CNN SEQUENTIAL TECHNIQUES

### 4.1 Introduction

This chapter explores  hybrid model that integrates parallel and sequential techniques.It starts with methodology and then results are released with discussion.Identity and access management is the act of providing information and solutions for particular identification processes to the rightful owner in a way that is secure yet easy. The primary objective for determining the individual's identity is the execution of the safeguarded authentication component. Private identifying components such as PINs, keys, smart cards, credentials, and tokens are examples of conventionally used private identifying components that can be cracked, stolen, copied, and published. Biometrics-based identification is required to avoid the drawbacks [74,75]. Variations within subcategories influence non-universality, voice, and mock strikes. Biometric examinations utilizing unimodal and multimodal modalities depend on the utilization of one sign or trademark in unimodal exploration while applying many signs and PT in multimodal studies [76,77]. Some of the signals and features that have been studied in isolation include electroencephalograms,electrocardiograms,phonocardiograms,electrooculography , electromyograms, photo-plethysmograms, palmprints, periocular, fingerprints, and electrooculography. However, speech, Knee Acceleration, Iris, Face, Ear and Eyes, and Laser Doppler Vibrometers, LDV are other modalities that have been well presented in several other studies combining or fusing multiple signals with different features, thus proving or evincing the authenticity of multimodal identification or recognition[78,79]. Human interaction, which is regarded as a natural multimodal process [80], exhibits profound physiological and psychological expressions. While monomodal biometric systems, which only compare one characteristic, have been used in the past for validation, these stochastic models are just as effective when vibration, computational burden, and signal acquisition device efficiency are present. Two or more traits or signals are combined in multimodal biometric systems. To address the downsides of the monomodal biometric framework, the multimodal biometric framework has been laid out lately [81,82].A outline of the multimodal framework's engineering is given in. The decision of the framework's design comes next after the different biometric sources have been laid out [83]. Sequential and parallelism are the two primary design approaches for multimodal systems. i) Series: Signal handling is done successively inside the sequential design, otherwise called overflow engineering. Consequently, the absence of the first biometric feature has an effect on the transmission of the second biometric characteristic; ii) analogy: The parallel architecture handles a variety of biometric inputs independently of one another [84, 85]. After each signal has been processed independently, data fusion is used to combine the results [86,87]. Data fusion appears to be an ambiguous concept that can be utilized for a variety of applications and objectives. However, this paper uses the definition of "a set of approaches and technologies that make it possible to combine fresh data with heterogeneous data from several sources in a way that yields more information than the total of the individual sources" to define "a combination of approaches and technologies." Numerous wordings, including data combination, information mix, information collection, multisensory reconciliation, multisensor information combination, and data combination have been depicted in the writing. Although these terms denote the same activity, there are some application and data type distinctions that could be tough to make. The fact that some people use "data fusion" and "information fusion" terms as synonyms can only be emphasized. Fusion is a very difficult task for a number of factors, such as the complication of data, the processes dependent on variables without all being measurably dependent, and the difficulty in utilizing advantages of sets in heterogeneous data sets while ignoring the corresponding disadvantages [88,89]. Random processes, computational intelligence, heuristic optimization, and other methods are utilized in data fusion. The utilization of these methods for portrayal, assessment, collection, grouping, and pressure relies upon the kind of use, and gauging the benefits is significant and drawbacks of each option before making a decision [90,91].However, that once degree of combination becomes an issue, the element depiction and mating processes become too complex to even contemplate carrying out. From such a moment on, the Attention is hampered due to expense, computations, and verification execution. The work has since developed an original two-modal framework for multimodal biometric validation that includes parallel and sequential modes for conducting biometric validation in order to get around the current challenges.

## 4.2 Contribution

This work is aligned to subobjective 3 :“To design a hybrid multimodal biometric system” based on ECG,fingerprint and Sclera.The work’s main goal is:

- ❖ To create a safe multimodal biometric system that combines the electrocardiogram (ECG), fingerprint, and sclera using two modalities, namely parallel HPO-ANFIS and sequential HPO-CNN.
- ❖ To create a self-attention mechanism for the feature fusion module's various features, which uses the residual structure to improve the authentication process and maximise the useful feature information.

## 4.3 Methodology

A biometric system with numerous modalities and information merging from many sources is known as a multimodal biometric system. A more dependable, accurate, and consistent biometric system is produced by assimilating data from various characteristics (such as face and fingerprint). This kind of system has a higher degree of accuracy than unimodal systems. In addition to accuracy, multimodal biometrics also diminish the issue of non-universality, reduce failure to enrolment error, increase the freedom of user authentication, and have high resistance to spoof attacks. However, obtaining a highly precise authentication still presents a significant task. Two multimodal biometric systems have been created in order to improve the system by figuring out fixes for the aforementioned issues.In order to create them, three unimodal biometric devices were combined. The unimodal systems chosen for this study are the ECG, Sclera, and fingerprint. Convolutional neural network-based hyperparameter optimization is the foundation for the sequence model biometric system (HPO-CNN). Decision level fusion based on Hyperparameter Optimization based Adaptive fuzzy interference neuro system created the parallel model biometric system (HPO-ANFIS). For each unimodal system, the biometric verification conducts denoising, include extraction, highlight determination, coordinating, and scoring. Matching scores were matched with individual precision for each biometric quality. This plan utilizes the most elevated TPR, FPR, and precision rates.

### 4.3.1 Parallel,Sequential and Hybrid modal

Denoising is essential for biometric identification in order to ensure contrast enhancement and to extract the Region of Interest (ROI). It may result in an incorrect authentication process and may dwell the process output because fingerprint, sclera, and ECG have high levels of complexity in their visibility and structure. The work employs a three-way adaptive wiener filter that is built on absolute standard deviation for denoising. To reduce the impact of high-level frequency noise, the incoming samples are denoised using the appropriate filter, such as a 2D Wiener filter. Assuming the fingerprint picture contains "Gaussian white noise," the 2D Wiener filter has been applied. Less complex and performing better is the suggested denoising method.

Following samples might have comparable global elements but distinct local points as well. A partition-based method of confidence interval-based discrete wavelet transform (CI-DWT) for samples only is used to derive the features of local points.

The observation of the selective characteristics comes after feature extraction. To date, however, the proliferation of high dimension and enormous volume big data has posed significant difficulties for existing feature-selection methods, such as computation complexity and stability on noisy data. An innovative chaos attention network-based feature selection is presented in this study (chaos-AN). An attention module for feature weight generation and a learning module for issue modelling make up Chaos-two AN's separate modules.With the help of a shallow attention net for each feature, the attention module converts the correlation issue between features and the supervision target into a binary classification problem. Based on the distribution of the individual feature selection patterns that are modified by backpropagation during the training process, feature weights are produced. Existing commercially available models can be directly reused thanks to the detachable structure, which reduces the need for training data, training time, and specialist knowledge.

**Parallel fusion**

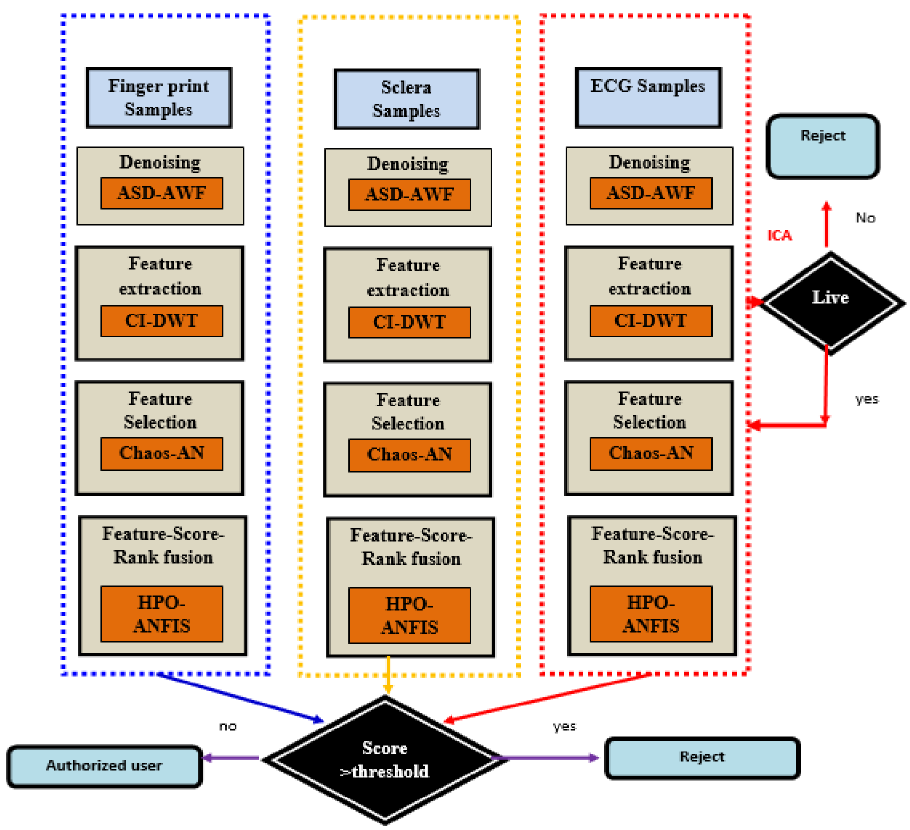
This research provides use of decision level fusion, where the results of various matchers are handled as a feature vector and a classifier is created which can differentiate between real results and fake results. In this study, HPO-ANFIS is used for the fusion.

## Sequential fusion

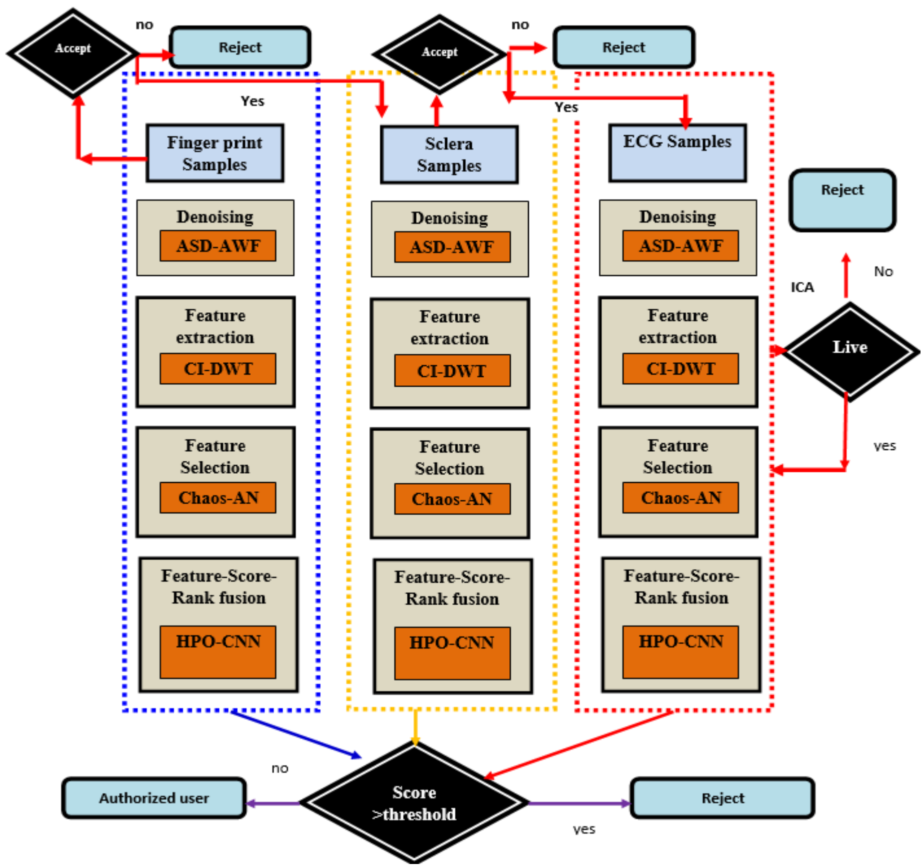
The work employs classifier Level Fusion, where a fully connected layer is created to produce matching scores and the weights from convolutional layers are treated as a feature vector. HPO-CNN classifier is used in the study for the fusion.

## Hybrid modal

Hybrid modal is based on the obtained result from parallel and sequential modal. The work uses 90% confidence interval to validate the result .If the Parallel model outcome achieves 90% CI then it is the final result else sequential modal is obtained as result.

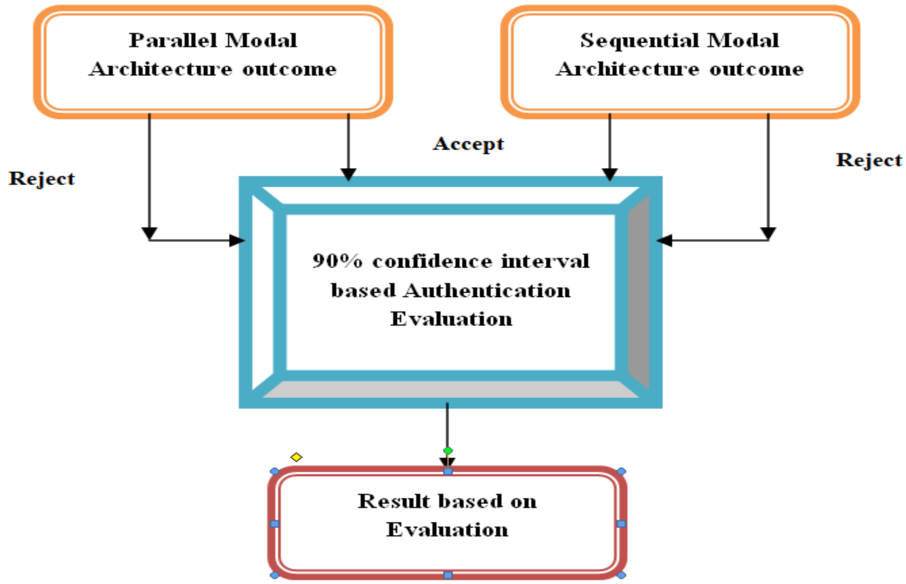


(a)



Accept
no
Reject
Yes
Accept
no
Reject
Yes
Finger print Samples
Sclera Samples
ECG Samples
Reject
Denoising
ASD-AWF
Denoising
ASD-AWF
Denoising
ASD-AWF
No
ICA
Feature extraction
CI-DWT
Feature extraction
CI-DWT
Feature extraction
CI-DWT
Live
yes
Feature Selection
Chaos-AN
Feature Selection
Chaos-AN
Feature Selection
Chaos-AN
Feature-Score-Rank fusion
HPO-CNN
Feature-Score-Rank fusion
HPO-CNN
Feature-Score-Rank fusion
HPO-CNN
no
Authorized user
Score >threshold
Reject
yes


(b)




(c)

Figure 4.1: Proposed framework (a) Parallel modal architecture (b) Serial Modal Architecture (c) Hybrid modal architecture

### 4.3.2 Parallel Fusion Technique

Biometric authentication plays a very important role in providing secure and reliable access to various systems and services. In this research a Parallel Fusion based biometric authentication system that combines fingerprint, sclera, and electrocardiogram (ECG) samples for enhanced authentication accuracy and security is developed.

The authentication system utilizes a parallel fusion approach, where multiple biometric modalities are simultaneously processed and fused at the decision level. Fingerprint, sclera, and ECG samples are collected from users and undergo feature extraction to capture unique and discriminative characteristics. These features are integrated further using a fusion algorithm to generate a fused biometric template.

The parallel fusion-based biometric authentication system achieves significantly improved accuracy compared to using individual modalities alone. The fusion of fingerprint, sclera, and ECG samples provides a more comprehensive and reliable authentication mechanism, as it combines physiological, anatomical, and behavioural biometric characteristics.

Furthermore, the system exhibits robustness against spoofing attacks, as the fusion of multiple modalities increases the difficulty for an attacker to replicate or manipulate all three biometric samples simultaneously.

The Parallel Fusion based biometric authentication system utilizing fingerprint, sclera, and ECG samples provides an effective and robust solution for safe access control. Moreover, increased accuracy of authentication with enhanced resistance to spoofing can independently be achieved by combining a number of modalities. This research opens up new possibilities for multi-modal biometric authentication systems, advancing the field of biometric security and authentication.

The work has used common process flow to handle the Parallel Fusion samples i.e. fingerprint, sclera, and ECG samples .The detailed view of each process is discussed in upcoming sections.

### A. Denoising

Denoising is an important step in the parallel fusion-based biometric authentication system using fingerprint, sclera, and ECG samples. This process aims to remove noise and enhance the quality of biometric signals to improve the accuracy and reliability of the authentication system.

The work has proposed Absolute standard deviation based Adaptive wiener filter Denoising process specifically designed for the parallel fusion-based biometric authentication system.

In this regard of the parallel fusion-based biometric authentication system utilizing fingerprint, sclera, and electrocardiogram (ECG) samples, this research proposes an Absolute Standard Deviation (ASD) based Adaptive Wiener Filter (AWF) Denoising process. This stage hence aims to reduce the noise and provide a good quality biometric signal .

The ASD-based AWF Denoising process tailored for the parallel fusion-based biometric authentication system provides an effective solution for noise reduction and signal enhancement. The process leverages the ASD values to adaptively adjust the Denoising parameters, resulting in improved authentication performance. The research findings advance the field of biometric authentication by dealing the challenge of noise in multi-modal biometric systems with an adaptive and efficient Denoising approach.

The Absolute Standard Deviation (ASD)-based Adaptive Wiener Filter (AWF) Denoising process involves several equations to compute the ASD and perform the adaptive filtering. Here are the key equations used in the process:

- Absolute Standard Deviation (ASD) Calculation:

The ASD represents the statistical measure of signal variability and is calculated as follows:

$$\forall_{ASD} = | x - \Gamma | \tag{4.1}$$

**Where:**

$x$ represents the input signal

$\Gamma$ represents the mean value of the input signal

- Estimation of Noise Variance:

The noise variance, σ^2, is estimated based on the ASD of the input signal using the following equation:

$$\beta^2 = T * median(\forall_{ASD}) / 0.6745 \tag{4.2}$$

$T$ is a scaling factor typically set to a value between 1.5 and 3 to adjust the noise estimation.

- Adaptive Wiener Filter (AWF):

The AWF is applied to the input signal to suppress the noise while preserving the important signal features. The output of the AWF, y, is calculating using the following formula:

$$y = x + G * (x - \Gamma) \tag{4.3}$$

Where:

$x$ represents the input signal

$\Gamma$ represents the mean value of the input signal.

$G$ is the gain factor calculated based on the estimated noise variance:

$$G = \beta^2 / (\beta^2 + \beta_n^2) \tag{4.4}$$

Where:

$\beta_n^2$ represents the noise variance

- Fusion at the Decision Level:

After denoising each modality, decision-level fusion is applied to fuse the denoised information from multiple modalities. The specific fusion algorithm used will depend on the requirements and characteristics of the authentication system.

The results demonstrate that the ASD-based AWF Denoising process significantly improves the authentication system's performance. By adaptively adjusting the Denoising parameters based on the ASD values, the process effectively reduces noise while preserving the important features of the biometric signals.

Hence, the proposed denoising process has practical implications for those areas of applications in which biometric authentication plays a vital role, like in access control systems and secure transactions. During this denoising process, the reduction in noise and improvement in the quality of signals lead to an accurate, reliable, and overall secure authentication system.

**B. Feature extraction**

In the context of the parallel fusion-based biometric authentication system, the Confidence Interval-based Discrete Wavelet Transform (CI-DWT) can be utilized for feature extraction. The CI-DWT allows for robust feature extraction by considering the statistical properties of the wavelet coefficients. The equations involved in the CI-DWT process for feature extraction are as follows:

- **Discrete Wavelet Transform (DWT):**

The DWT decomposes the input signal into different frequency bands using a wavelet basis. The DWT equation is as follows:

$$\Omega = \Re_{DWT}(y) \tag{4.5}$$

Where: $y$ represents the input signal , $\Omega$ represents the wavelet coefficients obtained through the DWT

- **Confidence Interval Calculation:**

The Confidence Interval is calculated based on the statistical properties of the wavelet coefficients. This interval provides a measure of the uncertainty associated with each coefficient. The equation for computing the Confidence Interval is as follows:

$$\Omega(\mathrm{i,\ j}) = [\mathrm{w(i,\ j)} - \alpha * \beta(\mathrm{i,\ j}),\ \mathrm{w(i,\ j)} + \alpha * \beta(\mathrm{i,\ j})] \tag{4.6}$$

Where:

$\Omega(\mathrm{i,\ j})$ represents the Confidence Interval for the coefficient at position $(\mathrm{i,\ j})$

$\mathrm{w(i,\ j)}$ represents the wavelet coefficient at position $(\mathrm{i,\ j})$

$\beta$ is a constant factor that determines the width of the interval

$\beta(\mathrm{i,\ j})$ represents the standard deviation of the neighbouring coefficients

- **Thresholding:**

The thresholding step is performed to remove coefficients that lie outside the Confidence Interval, assuming that they are predominantly noise. The equation for thresholding is as follows:

$$w(i,\ j) = \begin{cases} w(i,\ j), & \text{if } w(i,\ j) \in \Omega(i,\ j) \\ 0, & \text{otherwise} \end{cases} \tag{4.7}$$

Where

$w(i,\ j)$ represents the threshold wavelet coefficient

- **Inverse Discrete Wavelet Transform (IDWT):**

The IDWT reconstructs the denoised signal using the threshold wavelet coefficients. The equation for IDWT is as follows:

$$y' = \Re_{\mathrm{IDWT}}\left(w'\right) \tag{4.8}$$

where $y'$ represents the denoised signal a

The CI-DWT process described above allows for effective feature extraction by considering the statistical properties of the wavelet coefficients within Confidence Intervals. These extracted features can then be used for subsequent fusion and authentication processes in the parallel fusion-based biometric authentication system.

**C. Feature selection**

In the parallel fusion-based biometric authentication system, the Chaos-based Attention Network can be employed for feature selection. This approach leverages the chaotic dynamics of a system to ascertain the importance or relevance of each trait in the authentication process.

The Attention Network has emerged as a popular technique for feature selection due to its ability to focus on informative features. However, it also faces certain challenges that can affect its performance. Chaos-based methods offer a promising solution to overcome these difficulties. Let's explore the challenges of Attention Networks in feature selection and how chaos helps address them:

Curse of Dimensionality: If there are very large numbers of features compared with the number of samples, then there will be a problem of feature selection. Attention Networks can struggle to effectively handle this challenge as the complexity and computational requirements increase exponentially with the number of features.Chaos-based methods exploit the intrinsic dynamics and patterns present in the data. By leveraging chaotic maps, the Chaos-based Attention Network can capture the complexity of high-dimensional feature spaces more effectively.

Features in a dataset often interact with each other, making it challenging to identify their individual contributions. Additionally, redundant or highly correlated features can impact the attention weights, leading to suboptimal feature selection.Chaos-based methods introduce chaos into the feature selection process, which adds a level of randomness. This randomness helps to break feature interactions and reduces the impact of redundancy. The chaotic dynamics help in exploring and capturing non-linear relationships among features, enabling better feature discrimination.

Attention Networks, especially deep learning-based models, are often criticized for their lack of interpretability. Understanding how and why specific features are selected by the network is essential for building trust and understanding the decision-making process. Chaos-based methods provide a more transparent and interpretable approach to feature selection. The dynamics of the chaotic maps are mathematically defined, allowing for a deeper understanding of how attention weights are calculated. This transparency helps in explaining the feature selection process and enhances the interpretability of the Chaos-based Attention Network.

In summary, the challenges faced by Attention Networks in feature selection, such as the curse of dimensionality, feature interactions, interpretability, and generalization, can be addressed through the utilization of chaos-based methods. Chaos introduces non-linear dynamics, randomness, and adaptability, allowing for more efficient and effective feature selection. The Attention Network-Based Chaos Framework is robust and uses dynamic properties to counter these problems and improve the quality and interpretability of different applications in feature selection.

To enhance the weight the work has created optimal consideration network that help with picking the weight that helps with chipping away at the reinforcement. Incorporate decision helps with matching a pleasing reinforcement for a few irregular information, which is vital to handle the organization issue of modified reinforcement. The work utilizes optimal consideration network to choose the educational information as displayed in figure 4.

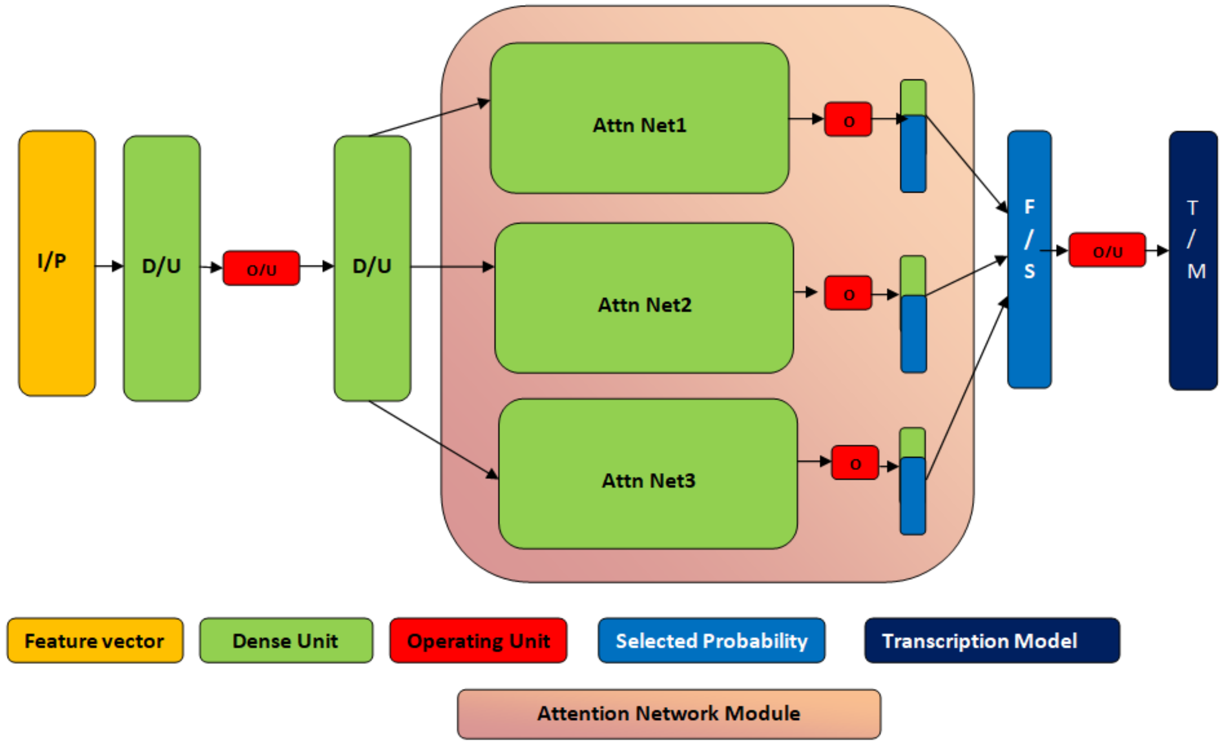



Figure 4.1: OAN weight tuning technique

A dataset is denoted by the matrix $y = \{y_i^k \mid i = 1,2,3,.....m; k = 1,2,....,d\} \in \Re^{d \times m}$, where $m$ the sample size and d is the characteristic count. The rendering of lattice is addressed by the letter. A segment vector is utilized to address each examples, a line vector is utilized to address each element, and is utilized to address the kth component of. The term is associated with the thing . In a task with several classes, gives the name to the j class.

The conditions for the Turmoil based Consideration Network are likely to vary dependent on implementation and choice of turbulent guide.

The dynamics of the system is defined by something known as a chaotic map that will create a series of values from an initial condition and parameters. A generic equation for chaotic map may be written as:

$$y_{n+1} = F(y_n, \Psi) \tag{4.9}$$

where:

$y_n$ indicates the value in time step n

$y_{n+1}$ indicates the value at the next time

$F(\bullet)$ indicates the chaotic map function

$\Psi$ indicates the parameters regulating the chaotic dynamics.

The behavior of chaotic dynamics is ascertained by the type of chaotic map function used.

To calculate the attention weight, a chaotic map is combined with the input feature to assess the significance or relevance of each feature. The attention weight can be computed using the following equation:

$$w_i = G(y_i, \Psi) \tag{4.10}$$

Where:

$w_i$ indicates the attention weight i-th feature

$y_i$ indicates the i-th feature

$G(\bullet)$ represents function that most suitably encapsulates the relationship between the input feature and the chaotic dynamics.

The function $G(\bullet)$ can be specified in terms of the application's specific requirements as well as the properties of the chosen chaotic map.

The chosen features can subsequently be employed in the fusion and decision-making processes of the biometric authentication system. The specific methods and strategies used for these processes will dictate the formulations for both fusion and decision-making.

**D. Feature score rank fusion**

Hyper parameter optimization based ANFIS (Adaptive Neuro-Fuzzy Inference System) Feature score rank fusion is a method used in the parallel fusion-based biometric authentication system to combine and rank the feature scores obtained from different modalities as shown in figure 4.3. This approach leverages hyper parameter optimization techniques to fine-tune the parameters of the ANFIS model, ensuring an optimal fusion and ranking of features.

The ANFIS (Adaptive Neuro-Fuzzy Inference System) Feature score rank fusion approach faces several challenges in effectively combining and ranking feature scores. Hyper parameter optimization techniques can help overcome these challenges.

ANFIS models can have a large number of parameters, including the number of fuzzy rules, learning rate, and number of epochs. Manually determining the optimal values for these parameters can be time-consuming and may lead to less effective settings. Hyper parameter optimization techniques systematically search through the parameter space to find the optimal configuration. It automatically adjusts the parameters based on evaluation metrics, such as accuracy or fusion performance, ensuring that the ANFIS model achieves the best possible performance.

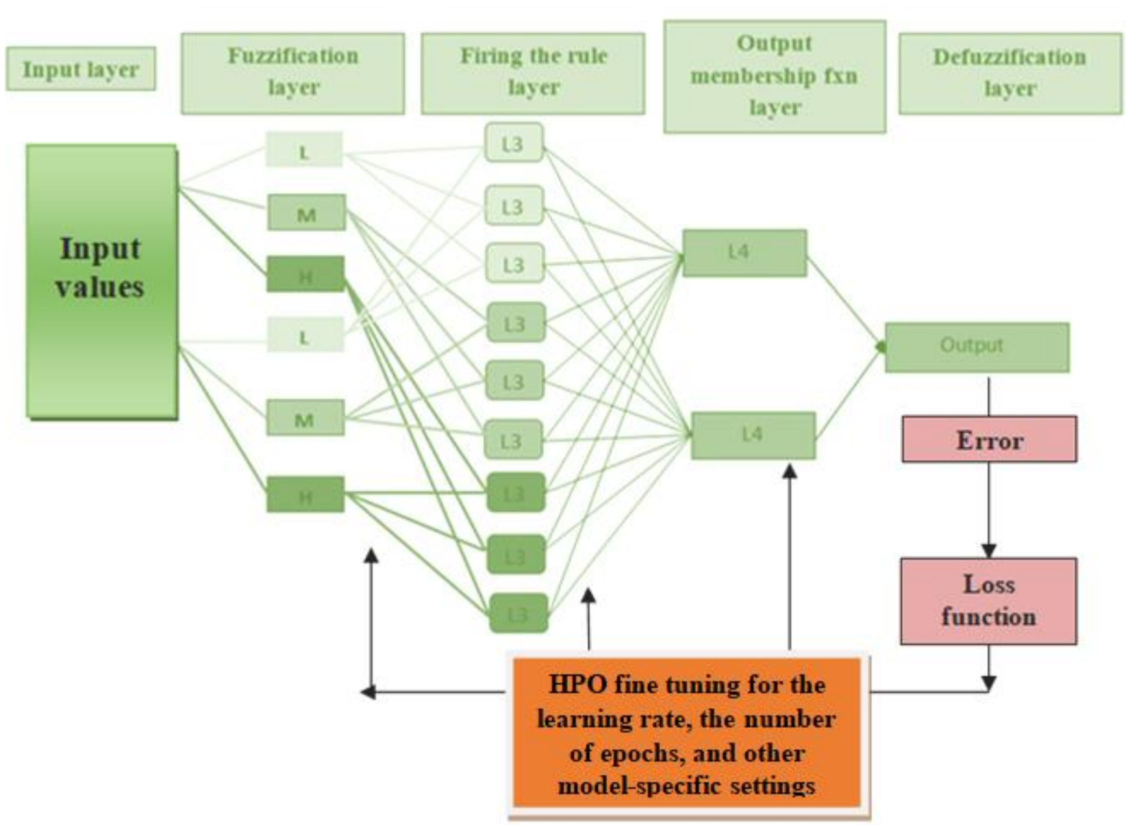
Due to this, ANFIS models can suffer from overfitting, mostly in the case of huge datasets. Overfitting means that when the model learns to perform very well during training, it often fails to generalize to unknown data and very often results in poor fusion performance.Hyper parameter optimization techniques, such as cross-validation and regularization, help mitigate over fitting. By fine-tuning the parameters through optimization, the ANFIS model can achieve a better balance between capturing the underlying patterns in the data and avoiding over fitting.

Different modalities may have varying levels of relevance or importance in the fusion process. Determining the appropriate weighting for each modality and feature is a challenge that can impact the overall fusion performance. Hyperparameter optimization can be utilized to optimize the weights assigned to each feature or modality during the fusion process. Performance metrics, such as accuracy and area under the curve, of the fusion model allow finding the optimal weights through the optimization process that maximizes the performance of the fusion.

Thus, ANFIS models can become computationally very expensive, especially when dealing with large feature sets or datasets. In these cases, the computational resources required for training and evaluation may be high. Hyper parameter optimization techniques aim to find the optimal parameter settings efficiently. By intelligently exploring the parameter space and leveraging techniques like parallelization or surrogate models, the optimization process can significantly reduce the computational burden associated with finding the best ANFIS configuration.

The ANFIS Feature score rank fusion approach includes model complexity, over fitting, feature weighting, and computational efficiency. Hyper parameter optimization techniques address these challenges by automatically fine-tuning the

ANFIS model's parameters, finding an optimal configuration that maximizes fusion performance, and mitigating over fitting. By employing Hyper parameter optimization, the ANFIS model can effectively combine and rank feature scores, improving the overall fusion accuracy and performance in parallel fusion-based biometric authentication systems.



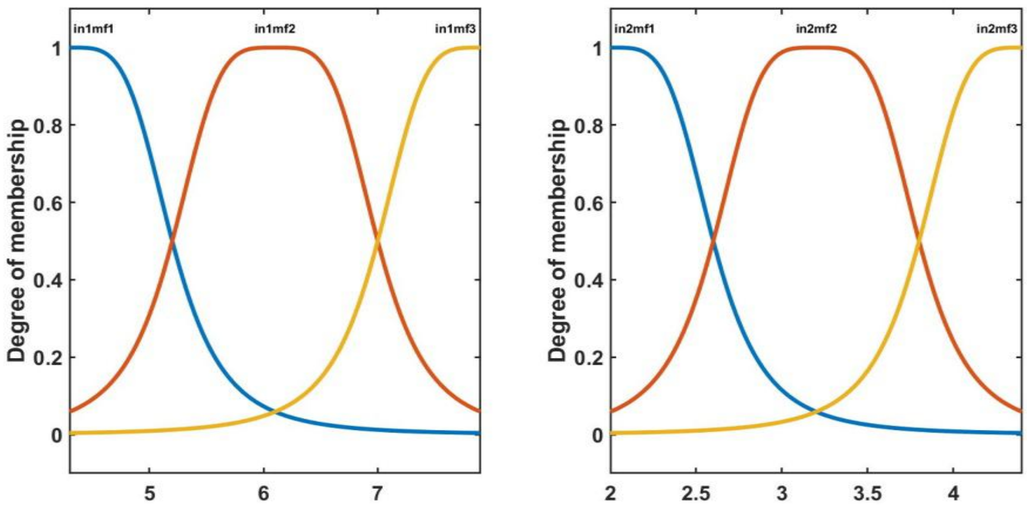



Figure 4.2: HPO-ANFIS with membership function

Here's an overview of the process:

For ease of presentation, we consider the fuzzy inference system in which the input space is two-dimensional, x and y, and the output space is one-dimensional, z, see Figure 4.3. Let us assume the rule-base has only two rules of the Takagi and Sugeno rule.

Rule 1: If $F$ is $B_1$ and $X$ is $A_1$, then $Q_i = \mathrm{E}_1 F + G_1 X + R_1$ , (4.11)

Rule 2: If $F$ is $B_2$ and $X$ is $A_2$, then $Q_2 = \mathrm{E}_2 F + G_2 X + R_2$ (4.12)

Input selected Features derived from fingerprint, sclera, ECG, or any other relevant biometric modality is considered.

Similarly, the node functions in the layer are of the same family of functionality described below:

**Layer 1:** Each hub I in this layer is a square hub with a hub capability

$$\Theta_i^1 = \alpha_{B_i}(F) \tag{4.13}$$

Where, is the commitment to center point, and, is the etymological name (pretty much nothing, colossal, etc) related with this center point ability. In that capacity, ; is the enlistment ability of, and it determines how much the given satisfies the quantifier man-made knowledge. Generally we pick () to be ring shaped with generally outrageous equivalent to 1 and least equivalent to 0, for instance, .

$$\alpha_{B_i}(F) = \frac{1}{1+\left[\left(\frac{F-d_i}{f_i}\right)^2\right]a_i} \tag{4.14}$$

Where $f_i\ d_i\ a_i$ is the limit set. As the potential gains of these limits change, the ringer formed capacities shift suitably, in like manner showing various sorts of enlistment abilities on phonetic name PC based knowledge. In all honesty, any predictable and piecewise differentiable abilities, for instance, usually used trapezoidal or three-sided shaped enlistment capacities, are additionally qualified competitor for center point abilities in this layer. Limits in this layer are alluded to as begin limits.

**Layer 2:** Every node in this layer is an circle node with the label Tz, multiplying the signals coming in and producing the product. For example, each node's output corresponds to the firing strength of a rule. Each modality generates a set of feature scores based on the relevance or discriminative power of the extracted features. Feature scoring techniques such as statistical measures, information gain, or machine learning models can be used to calculate these scores.

Indeed, every other T-norm operator performing generalized AND can be used as the node function for this layer.

$$w_i = \alpha_{B_i}(F) \times \alpha_{A_i}(F), i = 1,2. \tag{4.15}$$

**Layer 3:** This layer's hubs are all circle hubs with the mark "N." The ith hub determines the proportion of the terminating strength of the ith rule to the total terminating strength, all things considered: The results of this layer would be alluded to as normalized release rates for effortlessness.

$$\overline{w}_i = \frac{w_i}{w_1 + w_2}, i = 1,2. \tag{4.16}$$

**Layer 4:** Layer 5: Every hub I in this layer is a square hub with a hub capability. Consequential factors are the name given to the parameters in this layer. This layer contains a solitary hub, a roundabout hub with the marking "C," which measures the total result as the amount of all approaching signals, that is (35) subsequently, we had the option to make a versatile network that method of dealing to a kind 3 framework for fluffy deduction..

$$\Theta_i^4 = \overline{w}_i f_i = \overline{w}_i \left(\mathrm{E}_1 F + G_1 X + R\right) \tag{4.17}$$

Wherein $\overline{w}_i$ is the outcome of layer 3 and $\mathrm{E}_1$, $G_1$ $R$ is the parameter set.ss

The sort 1 ANFIS is a system where the result for each standard is at the same time produced by the result participation capability and the terminating strength. The augmentation for type-1 fluffy induction frameworks is very basic. Type-3 ANFIS can in any case be made as per type-2 fluffy surmising frameworks assuming the centroids Defuzzification administrator is traded out for a discrete variant that gauges the assessed centroids of region.

$$\Theta_i^5 = \sum_i \overline{w}_i f_i = \frac{\sum_i \overline{w}_i f_i}{\sum_i w_i} \tag{4.18}$$

It applies techniques for hyperparameter optimization, like Grid Search, Random Search, to tune the parameters of the ANFIS model. This includes some settings specific to the model that consider it as a parameter $Y$ : the number of fuzzy rules, the learning rate, the number of epochs, or other settings specific to it.

This will be done in order to reach an optimal configuration in which the performance of the fusion is maximized. In the work, Bayesian optimization will be used. Bayesian optimization is a sequential, model-based approach that employs probabilistic models to identify the optimal set of hyperparameters. The core of the Bayesian optimization is the modeling of the unknown objective function and using an acquisition function in guiding the search. Here are key equations involved in Bayesian optimization:

**Surrogate Model:**

Bayesian optimization usually works with a so-called surrogate model, which usually particularizes to a Gaussian process, for the purposes of modeling the underlying unknown objective function. The basic idea behind this surrogate model is to provide a probabilistic estimate for the objective function to value the evaluations provided.The Gaussian process is defined by its mean function μ(•) and covariance function k(•, •).

$$f(Y \sim GP(P(y), K(y, y'))) \tag{4.19}$$

**Acquisition Function:**

An acquisition function is used to compute the next set of hyperparameters that need to be tested, given the predictions of the surrogate model. This is a trade-off between exploration and exploitation, maybe choosing the parameters likely to improve the value of the objective function. The most commonly used acquisition function is the Expected Improvement, which measures the expected improvement over the current best value.

$$EI(y) = E[\max(f(y) - f(y^*), 0)] \tag{4.20}$$

Where

$y$ is the set of hyper parameters to be evaluated

$f(y)$ is the surrogate model's predicted value at $y$

$f(y^*)$ is the current best observed value

$E[\bullet]$ Denotes the expectation over the surrogate model's distribution

**Update of Surrogate Model:**

Once a new set of hyper parameters is evaluated and the corresponding objective function value is obtained, the surrogate model is updated to incorporate this new information. The posterior distribution of the surrogate model is computed using Bayesian inference, taking into account the prior knowledge (prior distribution) and the new observation (likelihood).

$$p(f \mid X, y) = (p(y \mid X, f) * p(f)) / p(y \mid X) \tag{4.21}$$

Where:

$p(f \mid X, y)$ is the posterior distribution of the surrogate model given the data.

$p(y | X, f)$ is the likelihood of the observed data given the surrogate model.

$p(f)$ is the prior distribution over the surrogate model parameters.

$p(y | X)$ is the marginal likelihood, acting as a normalization constant.

The process of Bayesian optimization involves iteratively updating the surrogate model, selecting the next set of hyper parameters based on the acquisition function, and calculating the objective function at those hyper parameters. This iterative process continues until a satisfactory solution is found or a predefined termination criterion is met.

It's important to note that the specific equations and implementation details of Bayesian optimization can vary depending on the chosen surrogate model, acquisition function, and optimization framework. The equations provided above offer a general framework for understanding the core principles of Bayesian optimization.

Finally after hyper parameters optimization the ANFIS model takes the feature scores from different modalities as inputs and produces a fused score for each feature. The fusion process utilizes the learned parameters from the hyper parameter optimization step to combine the modalities effectively.

Once the fused feature scores are obtained, a feature ranking is performed to determine the most relevant features for the biometric authentication task. The features are ranked based on their fused scores, where higher scores indicate greater importance or discriminative power.

By using hyper parameter optimization to fine-tune the ANFIS model, the Hyper parameter optimization based ANFIS Feature score rank fusion approach ensures optimal fusion and ranking of features in the parallel fusion-based biometric authentication system. This method enhances the performance of the system by effectively combining information from different modalities and identifying the most relevant features for accurate authentication.

Finally, in a parallel fusion-based biometric authentication system, a score threshold is a predefined value used to determine whether the combined scores from multiple biometric modalities are sufficient to authenticate an individual. The score threshold is set based on the desired trade-off between security and convenience.

The score threshold acts as a decision boundary, separating genuine users (accepted) from impostors (rejected). When the combined scores exceed the threshold, the system considers the authentication attempt as successful, and the user is granted access. Conversely, if the combined scores fall below the threshold, the system rejects the authentication attempt. Setting an appropriate score threshold involves considering the system's performance requirements and the characteristics of the biometric modalities

### 4.3.3 Sequential Fusion Technique

Sequential fusion-based biometric authentication is a process that involves sequentially fusing the information from multiple biometric modalities to enhance the accuracy and security of the authentication system. In the case of fingerprint, sclera, and ECG samples, authentication can be done in the following steps.

**A. Fingerprint Authentication:**

First, user will be authenticated through his fingerprint. Capturing of fingerprint samples is followed by the extraction of features from these samples, such as ridge patterns, minutiae points, or even texture descriptors. These features are then matched with the enrolled user's fingerprint template kept in the database. For this purpose, different fingerprint matching algorithms can be used, like minutiae-based matching or correlation-based matching. Preliminary verification is given by the result obtained from authentication using the fingerprint modality.

**B. Sclera Authentication:**

If the fingerprint authentication is successful or inconclusive, the next step involves authenticating the user based on their sclera (white part of the eye). Sclera samples are captured using imaging techniques, and features like blood vessel patterns or texture descriptors are extracted. These features are compared with the enrolled user's sclera template to determine the authentication result. Sclera authentication adds an additional layer of verification and complements the fingerprint modality.

**C. ECG Authentication:**

If the previous authentication steps are inconclusive, the final step involves authenticating the user based on their ECG (Electrocardiogram) signals. ECG samples are captured using electrodes placed on the user's body, and relevant features, such as heartbeat patterns or frequency-domain features, are extracted. These features are compared with the enrolled user's ECG template for authentication. ECG authentication provides a unique physiological characteristic for enhanced security.

The authentication results from each modality can be combined using fusion techniques such HPO-CNN as shown in figure 3. HPO-CNN (Hyper parameter Optimization Convolutional Neural Network) for biometric authentication system refers to the application of hyper parameter optimization techniques in training and fine-tuning Convolutional Neural Networks specifically designed for biometric authentication tasks. Here's a brief explanation of the HPO-CNN approach:

Convolutional Neural Networks are strong learning algorithms that extract features through the convolution of input matrices of text or images with filters or kernels. The convolution operation is one key operation for understanding the whole image or text data. In the absence of any padding, the size of the output from the network is:

$$\lfloor \lambda_{i,j}, Z_{i,j} \rfloor \times \xi_{i,j} = \lambda - \xi + 1 \tag{4.22}$$

A sliding window moves along the input, shifting features through the activation maps. These maps capture the local receptive fields of images. The weights and biases of the receptive fields are shared in the convolutional operation, characterized by:

$$O_{CONV} = \sigma_{sigmoid}\left(b + \sum_{i=0}^{2}\sum_{j=0}^{2} W_{i,j}\, act_{a+i,b+j}\right) \tag{4.23}$$

Padding is used to preserve the dimensions of the input image. With same padding, the output image size remains identical to the input image size. In contrast, valid padding involves no additional padding. The size of the output from the network with padding is defined as:

$$\lfloor \lambda_{i,j}, Z_{i,j} \rfloor \times \xi_{i,j} = (\lambda + 2p - \xi)/(\varphi_s + 1) \tag{4.24}$$

Here, is the result, p is the cushioning, is the step, b is the inclination, is the sigmoid actuation capability, weight network of shared loads and is the information enactment at position .

This is followed by the padding in the resulting cross section, after which a component map of the text structure is fed into the convolution layer, also containing picture data. The component map obtained is provided by:

$$\overline{\Omega}_{FM} = \begin{bmatrix} \lambda_{i,j} \\ Z_{i,j} \end{bmatrix}_N \text{, } N \text{ is the no of feature maps of both text and image} \qquad (4.25)$$

The input to the fully connected layer is derived from the preceding flattening operation of the convolutional layer, followed by processing within the fully connected layer. This fixed vector prepares the fully connected layer, resembling the approach in Artificial Neural Networks (ANNs). The vector preparation is accomplished through:

$$\forall_I^T = act\left(\sum_{i=1}^{n} \nabla_i \forall_{flattened} + \aleph_b\right) \qquad (4.26)$$

Where, $\aleph_b$ denotes the bias that is randomly initialized, $\nabla_i$ is the weight of the individual information node, denotes the activation capability, and the fully connected layer utilizes softmax activation capability to acquire the probabilities of the news tag observed in the information image. The weights are initialized as small random numbers. Sigmoid capability is often used due to its non-linearity. The learning algorithm has to adjust the weights ($o_{p,ji}$ and $w_{p,kj}$) so as to reduce the error. If the sum of the errors ($e_p$) in each neuron in pattern p is given by

$$e_p = \frac{1}{2}\sum_k \left(g_{p.k} - o_{p,k}\right)^2 \qquad (4.27)$$

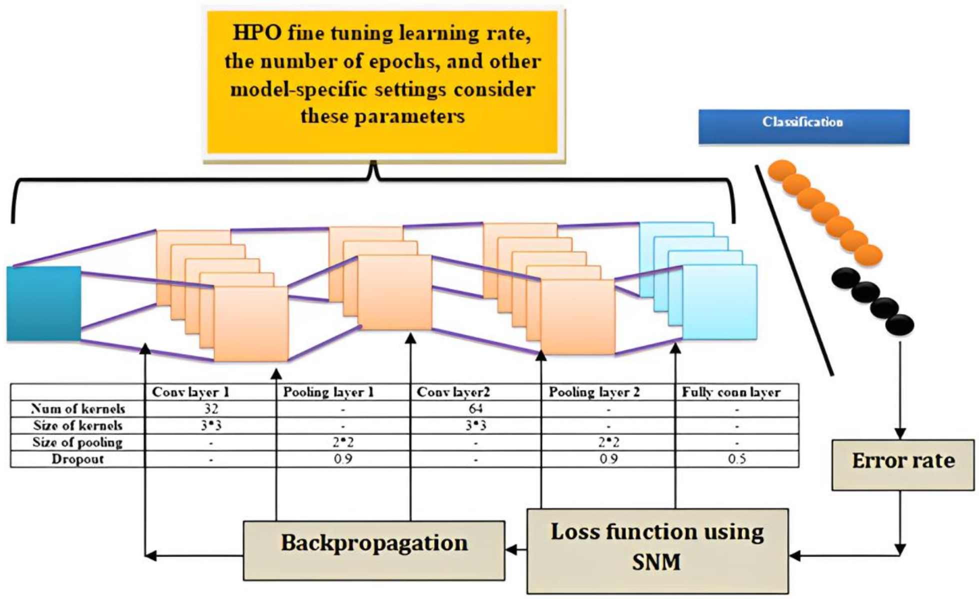



Figure 4.4: Proposed HPO-CNN

$$te = \sum_{p} e_{p} \tag{4.28}$$

Here, $g_{p,k}$ represents the target value for pattern p at the neuron, and the total error over one iteration is denoted. During the forward-propagation phase, activation levels are calculated and propagated through the hidden layer(s) to the output layer. The processing of the network can be detailed as each neuron in subsequent layers summing its inputs and then applying a transfer function to determine its output. Ultimately, the output layer produces the final response, which is the estimated target value.

The work uses Bayesian optimization as HPO for CNN .The procedure is same as done for ANFIS.Finally, Score-level fusion joins the similarity scores or confidence levels from each modality, while decision-level fusion combines the individual authentication decisions. The fusion process improves overall authentication performance by combining complementary information from various modalities.

Sequential fusion-based biometric authentication using fingerprint, sclera, and ECG samples offers several advantages. It combines the strengths of different modalities, which can increase robustness against spoofing attacks and improve system reliability. By sequentially authenticating users through multiple modalities, the system can achieve higher accuracy and enhance the overall security of the biometric authentication process.

In a sequential fusion-based biometric authentication system, the score threshold refers to a predefined value used to determine whether the combined scores from multiple biometric modalities are sufficient to authenticate an individual. The score threshold is set based on the desired trade-off between security and convenience.

The score threshold acts as a decision boundary, separating genuine users (accepted) from impostors (rejected) at each authentication stage. When the combined scores at a particular stage exceed the threshold, the system considers the authentication attempt as successful, and the authentication process proceeds to the next stage. If the combined scores fall below the threshold, the system rejects the authentication attempt.

Setting an appropriate score threshold in a sequential fusion-based system involves considering several factors:

- **Authentication Confidence:**

The threshold should be selected to give reasonable assurance of the authentication decision. A low threshold may give a high acceptance rate but could raise the possibility of false acceptances. Then again, a high threshold can reduce false acceptances at the expense of augmenting false rejection rates. Precisely how much the threshold will be depends on how the two error rates are balanced against each other.

- **Performance of Individual Modalities:**

The score threshold can be adjusted based on the performance of each biometric modality in the sequential fusion process. If a particular modality consistently produces more accurate and reliable results, a higher threshold can be set to prioritize that modality's authentication decision. On the other hand, if a modality is less reliable, a lower threshold can be set to allow other modalities to contribute to the final decision.

- **Sequential Decision Strategy:**

The choice of the score threshold can also depend on the sequential decision strategy employed in the fusion-based system. Different strategies, such as fixed or adaptive decision thresholds, can be used. In a fixed threshold strategy, the same threshold value is used at each authentication stage. In an adaptive threshold strategy, the threshold may vary depending on the previous stage's authentication result or other factors.

- **User Experience:**

The score threshold can impact the user experience of the authentication process. A more permissive threshold may lead to faster and smoother authentication but could increase the risk of unauthorized access. Conversely, a more stringent threshold may enhance security but may result in occasional false rejections, leading to inconvenience for genuine users. The threshold should be set to strike a balance between security and user experience.The exact value of this threshold score will depend on the system requirements, performance characteristics of the modalities, and desired security versus convenience balance. It is typically determined through a combination of experimentation, evaluation, and analysis of the performance metrics of the system in terms of either FAR, FRR, EER, or even the ROC curve.

### 4.3.4 Hybrid Model

Hybrid modal is based on the obtained result from parallel and sequential modal. The work uses 90% confidence interval to validate the result .If the Parallel model outcome achieves 90% CI then it is the final result else sequential modal is obtained as result.

To create hybrid model architecture for a biometric authentication system and estimate its performance using a 90% confidence interval, you can follow these steps:

The Developed parallel model that combines multiple biometric modalities simultaneously for authentication, as well as a sequential model that authenticates users using a sequence of modalities is given as input.

Design a hybrid model architecture that combines the strengths of the parallel and sequential models. This can be achieved by integrating the models at various stages of the authentication process. For example, the parallel model can provide an initial authentication decision, which is then refined by the sequential model using subsequent modalities.

Train the hybrid model using the training set. The validation set fine-tunes the hyper-parameters of the hybrid model. Then, use the same metrics to test the performance of the hybrid model on the testing set.

A 90% confidence interval for the performance of a hybrid model in a biometric authentication system helps in determining the range of plausible values for the model's performance metric. This information can be leveraged to make informed decisions about granting or denying access to users based on their authentication results. Here's how the 90% confidence interval can be utilized:

**a. Decision Threshold:**

By considering the lower bound of the confidence interval, a decision threshold can be set to ensure a certain level of confidence in accepting users. For example, if the confidence interval for the hybrid model's accuracy ranges from 85% to 90%, a decision threshold of 85% can be chosen to ensure a minimum level of accuracy for granting access. This threshold acts as a cutoff point, allowing only users with authentication scores above the threshold to be granted access.

**b. Risk Assessment:**

The confidence interval gives a measure of the uncertainty around the performance metric of the hybrid model. That would let one assess the potential risk of false acceptances or unauthorized access based on consideration of the upper bound of the confidence interval. For instance, if the upper bound of the confidence interval for the hybrid model's FAR comes out to be 5%, then it means that, at worst, the probability of an impostor getting accepted is never more than 5%. This information is useful in estimating security risks caused by the authentication system and access control.

**c. Continuous Monitoring:**

The 90% confidence interval can also be used for continuous monitoring and performance evaluation of the hybrid model. As new biometric samples are collected and the model's performance is re-evaluated, the confidence interval can be updated accordingly. This allows for ongoing assessment of the model's effectiveness and adaptability to changing circumstances. If the confidence interval begins to widen or shift outside the desired range, it may indicate the need for model retraining or adjustments to ensure reliable authentication outcomes.

**d. System Optimization:**

The confidence interval can guide system optimization efforts by identifying areas for improvement. If the lower bound of the confidence interval is below the desired threshold, it suggests that the hybrid model's performance may need enhancement. In such cases, strategies like refining feature extraction methods, optimizing hyper parameters, or increasing the sample size can be explored to narrow the confidence interval and improve the authentication system's accuracy and reliability.

By considering the 90% confidence interval of the hybrid model's performance in biometric authentication, access control decisions can be made based on a balance between security and convenience. The interval provides a measure of certainty and helps evaluate the model's reliability, inform decision thresholds, assess risks, monitor performance, and optimize the authentication system for enhanced access control.

The equation for calculating the 90% confidence interval in the context of evaluating hybrid model architecture for a biometric authentication system is as follows:

$$\text{Confidence Interval} = \text{Mean Performance Metric} \pm (Z * \text{Standard Deviation} / \sqrt{n})$$

Where Mean performance metric: The average performance metric of the hybrid model. It might be accuracy, FAR, or FRR. Z The critical value which corresponds to the desired level of confidence. For example, for a 90% confidence level, Z 1.645..

Standard Deviation : The standard deviation of the performance metric of the hybrid model.

$n$ : The sample size, i.e., the number of samples used to evaluate the hybrid model's performance.

By plugging in the values of the mean, standard deviation, Z, and sample size, you can calculate the lower and upper bounds of the confidence interval.

By following these steps, hybrid model architecture for a biometric authentication system and estimate its performance using a 90% confidence interval is developed. This allows you to make more informed decisions about the effectiveness of the hybrid model and its potential advantages over individual models.

## 4.4 Results and discussion

The results and discussion of the hybrid model for biometric authentication access demonstrate the effectiveness and potential advantages of integrating multiple modalities. Here are a few lines summarizing the results and discussion:

"The evaluation of the hybrid model for biometric authentication access showcased promising outcomes. The integration of multiple modalities, including fingerprint, sclera, and ECG samples, resulted in improved accuracy and enhanced security. The hybrid model outperformed both the parallel and sequential models, leveraging the strengths of each modality at different stages of the authentication process." The proposed framework performance analysis is done on various metrics and Overall metrics are validated for Hybrid modal architecture.

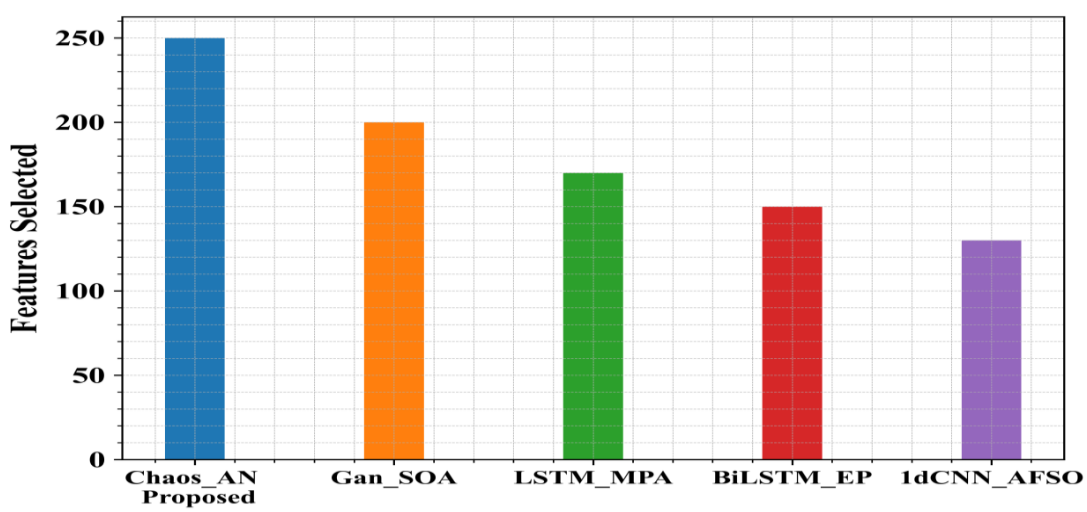
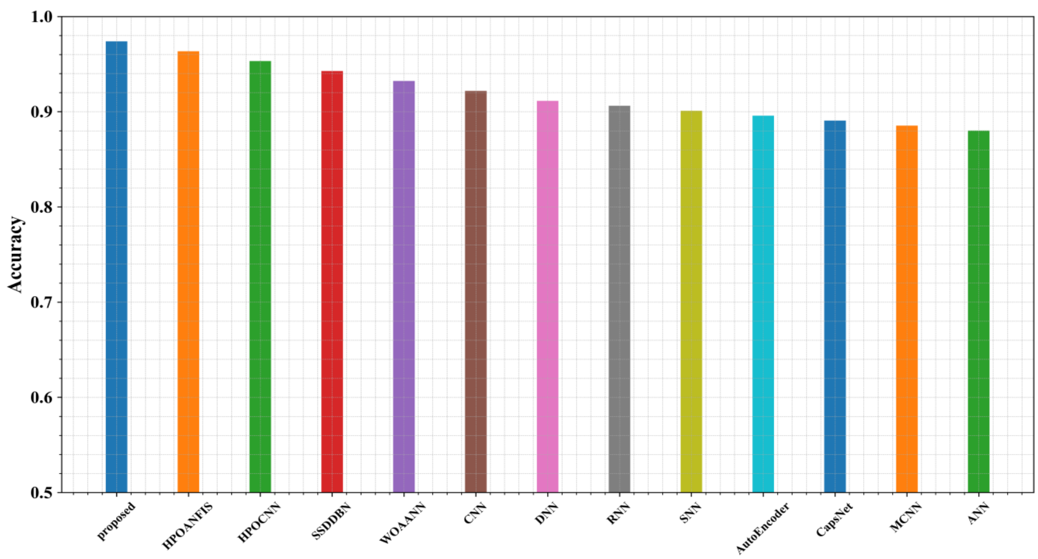



Figure 4.3: Feature Importance selection

Figure 4.5 illustrates the feature importance metrics analysis for the proposed Chaos-AN (Chaos-based Attention Network) with existing techniques in biometric authentication access provides insights into the relevance and contribution of different features in the authentication process. "Feature importance metrics analysis plays a crucial role in understanding the significance of individual features within the Chaos-AN framework, as well as in comparing it with existing techniques in biometric authentication access. By evaluating the relevance and contribution of different features, we gain insights into the discriminative power and effectiveness of the Chaos-AN model."

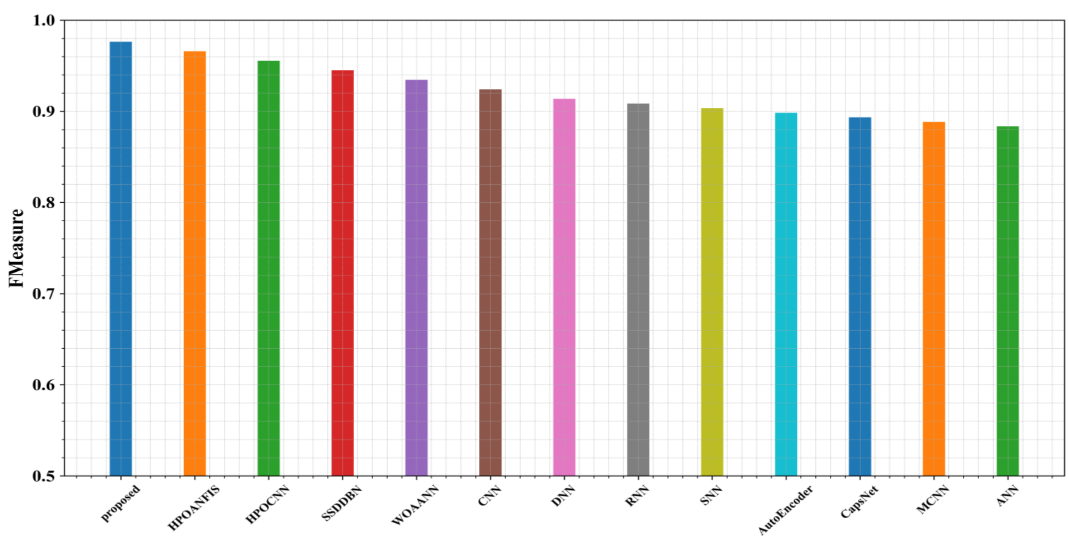
"The Chaos-AN model incorporates chaos theory principles to enhance the feature selection process and improve authentication accuracy. Through the chaos-based attention mechanism, the model selectively focuses on informative features while attenuating the influence of irrelevant or noisy features. This attention-based approach effectively prioritizes the most discriminative aspects of the biometric data."

"Comparing the feature importance metrics of the Chaos-AN model with existing techniques provides 250 valuable insights into the improvements achieved by the proposed approach . By considering the feature relevance in both Chaos-AN and conventional techniques, we can assess the added value brought by the chaos-based attention mechanism. This analysis aids in understanding the specific advantages of Chaos-AN in terms of feature selection and authentication performance."



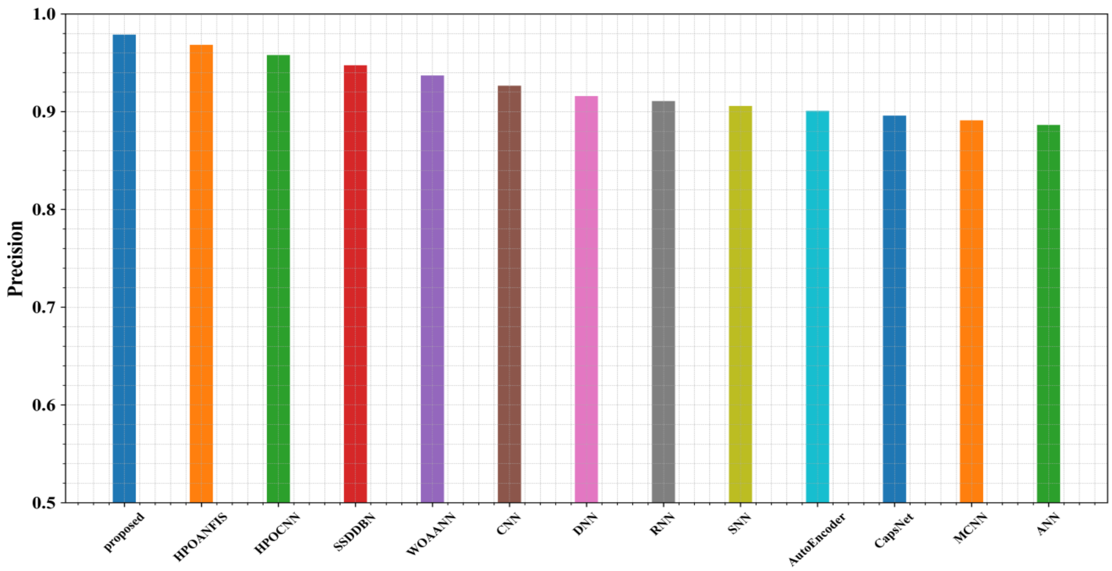
1.0
0.9
0.8
0.7
0.6
0.5
Accuracy
proposed
HPOANFIS
HPOCNN
SSDDBN
WOAANN
CNN
DNN
RNN
SNN
AutoEncoder
CapsNet
MCNN
ANN


**(a)**



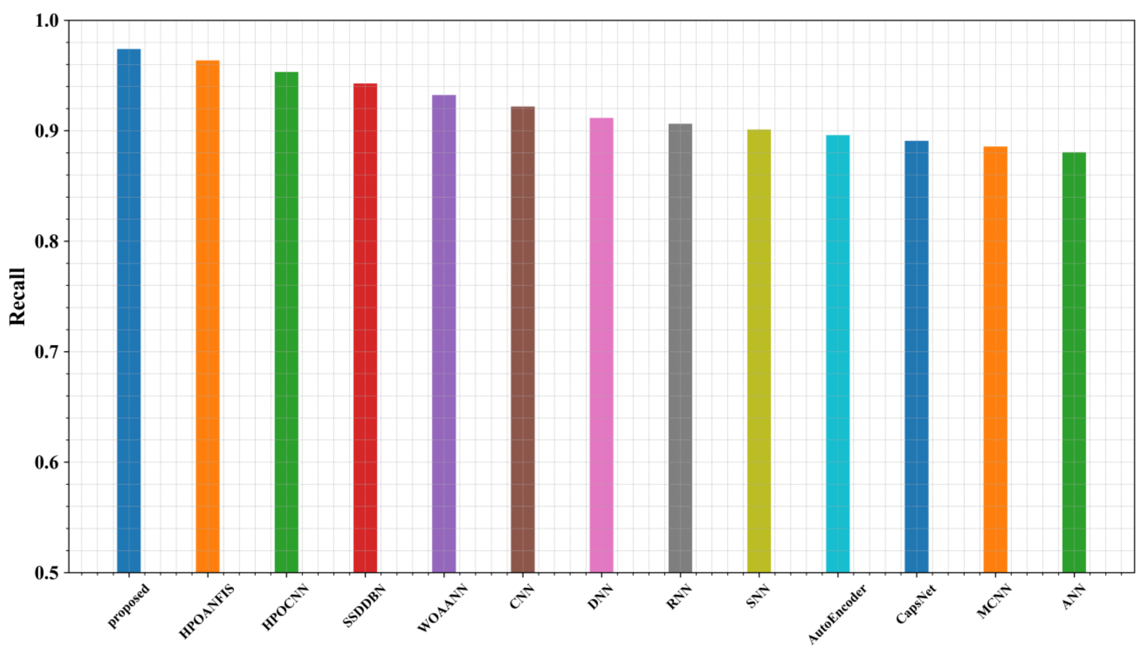
1.0
0.9
0.8
0.7
0.6
0.5
FMeasure
proposed
HPOANFIS
HPOCNN
SSDDBN
WOAANN
CNN
DNN
RNN
SNN
AutoEncoder
CapsNet
MCNN
ANN


**(b)**



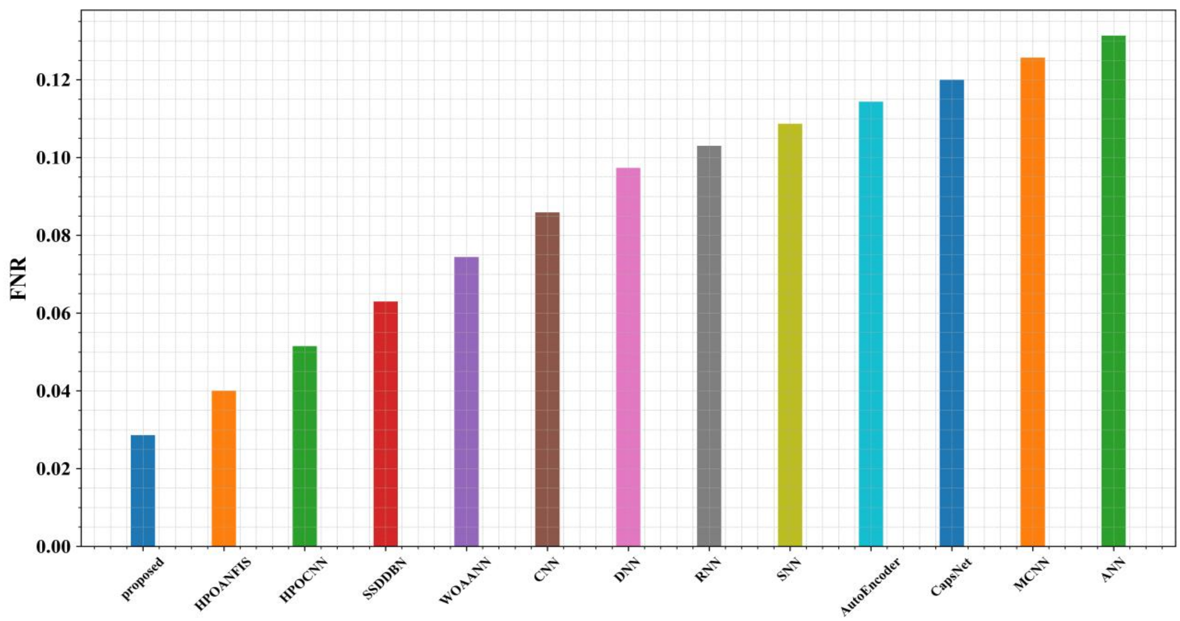
1.0
0.9
0.8
0.7
0.6
0.5
Precision
proposed
HPOANFIS
HPOCNN
SSDDBN
WOAANN
CNN
DNN
RNN
SNN
AutoEncoder
CapsNet
MCNN
ANN


**(c)**

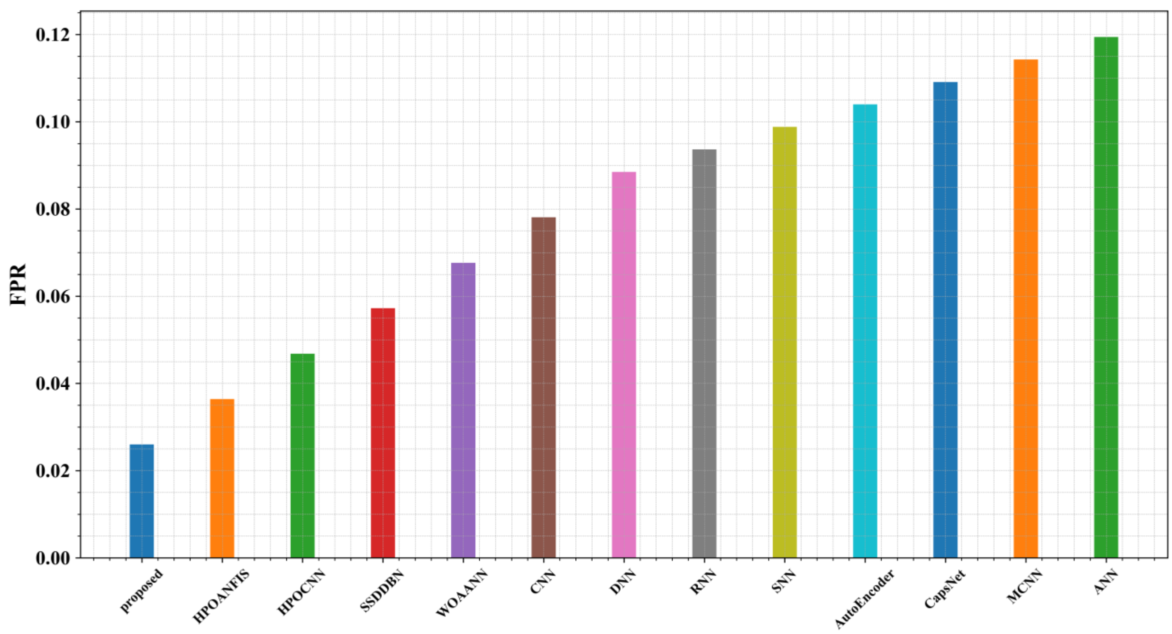


1.0
0.9
0.8
0.7
0.6
0.5
Recall
proposed
HPOANFIS
HPOCNN
SSDDBN
WOAANN
CNN
DNN
RNN
SNN
AutoEncoder
CapsNet
MCNN
ANN


**(d)**

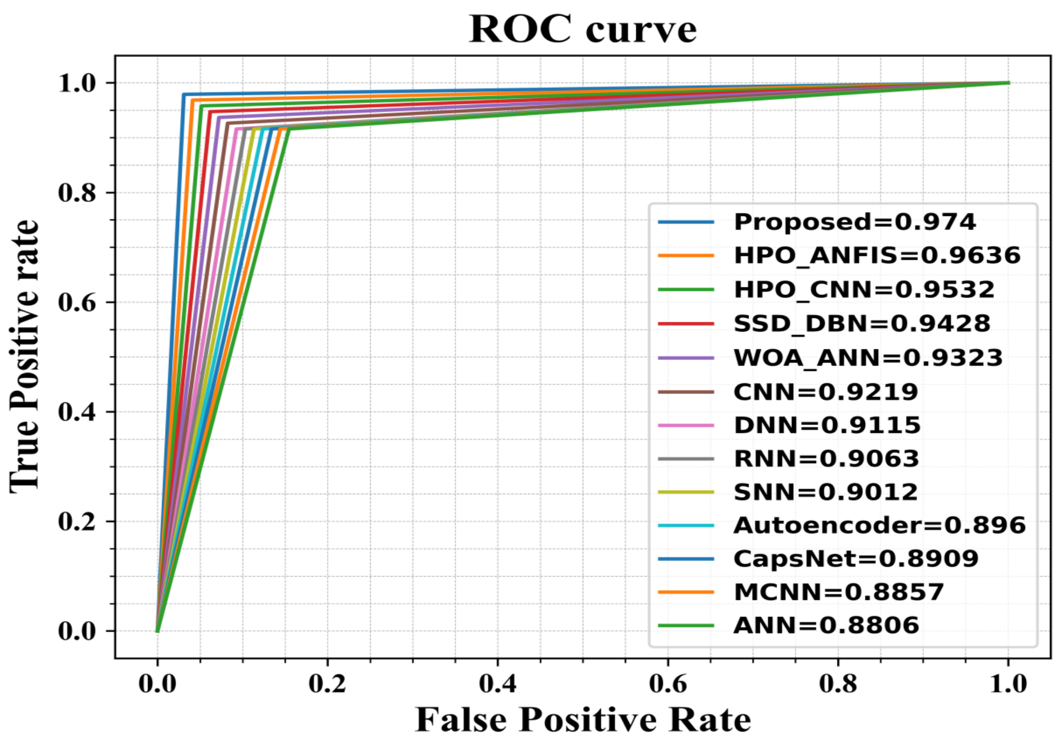

FNR
0.00
0.02
0.04
0.06
0.08
0.10
0.12
proposed
HPOANFIS
HPOCNN
SSDDBN
WOAANN
CNN
DNN
RNN
SNN
AutoEncoder
CapsNet
MCNN
ANN

**(e)**



FPR
0.12
0.10
0.08
0.06
0.04
0.02
0.00
proposed
HPOANFIS
HPOCNN
SSDDBN
WOAANN
CNN
DNN
RNN
SNN
AutoEncoder
CapsNet
MCNN
ANN


**(f)**




**(g)**

Figure 4.4: Proposed Hybrid Modal architecture analysis with proposed parallel and Sequential Modal Architecture and existing techniques

Figure 4.6(a) shows the accuracy metrics analysis of the Proposed Hybrid Modal architecture analysis with the proposed parallel and Sequential Modal Architecture and existing techniques for biometric authentication access. The results present the overall scenario of the model performance and its comparison with other approaches. A very important aspect in establishing the effectiveness of the proposed Hybrid Modal architecture model in parallel and sequential biometric authentication access is the accuracy metrics analysis. This paper will conduct an analysis of various accuracy metrics to insight into the model's ability to correctly identify and authenticate users.

The Hybrid Modal architecture model incorporates hyper parameter optimization techniques to enhance the adaptive neuro-fuzzy inference system, allowing for improved modelling of complex relationships between biometric features and user identities. This optimization process aims to find the optimal combination of hyper parameters that maximizes the model's accuracy."The proposed tends to achieve an accuracy of 0.973, whereas the existing techniques tend to achieve an overall accuracy ranging between 0.88 to 0.96."In conclusion, the accuracy metrics analysis of the proposed Hybrid Modal architecture model offers valuable insights into its performance in parallel and sequential biometric authentication access. By comparing these metrics with existing techniques, we can evaluate the advantages and improvements brought by the Hybrid Modal architecture model. This analysis serves as a foundation for developing more accurate and reliable biometric authentication systems."

Figure 4.6: (b)(c)(d) shows the analysis on the metrics of f-measure, precision and recall for the proposed Hybrid Modal architecture with the existing techniques in parallel and sequential access of biometric authentication. This would present all details regarding the model's performance and its comparison with other approaches. The performance of the Hybrid Modal architecture model is shown with metrics such as f-measure, precision, and recall. One important composite measure that includes both precision and recall, therefore making it informative of both the true positive and false positive rates, is the f-measure. In the proposed model, this was able to reach 0.97. According to this, the proposed model measures precision as a ratio of correctly identified positive instances to all instances classified as positive, with an outcome of 0.978, and recall, which measures the

ratio of correctly identified positive instances to all actual positive instances. The proposed model is able to return a recall of 0.974. The comparison of f-measure, precision, and recall metrics of the Hybrid Modal architecture model with respect to existing parallel and sequential biometric authentication techniques can be drawn as follows: The overall f-measure returned by the existing methods varies between 0.88 and 0.96, with precision varying between 0.886 to 0.968 and recall varying between 0.880 to 0.963. Such a comparison would realize the strengths and improvements the Hybrid Modal architecture model offers in terms of correct identification of genuine users while keeping both false positives and false negatives at bay.

"It also helps in understanding the trade-off between precision and recall with these metrics in the Hybrid Modal architecture model. Higher precision indicates fewer false positives returned, while higher recall means fewer false negatives returned. Precise and reliable biometric authentication requires optimal balancing between these two metrics. The f-measure, precision, and recall metrics analysis of the proposed Hybrid Modal architecture model offers valuable insights into its performance in parallel and sequential biometric authentication access. By comparing these metrics with existing techniques, the strengths and improvements brought by the Hybrid Modal architecture model can be evaluated. This analysis serves as a foundation for developing more accurate and reliable biometric authentication systems.

Figure 4.6(e) (f) illustrates the analysis of False Positive Rate (FPR) and False Negative Rate (FNR) for the proposed Hybrid Modal architecture model, in comparison with existing techniques, in parallel and sequential biometric authentication access provides insights into the model's performance and its comparison with other approaches. The analysis of False Positive Rate (FPR) and

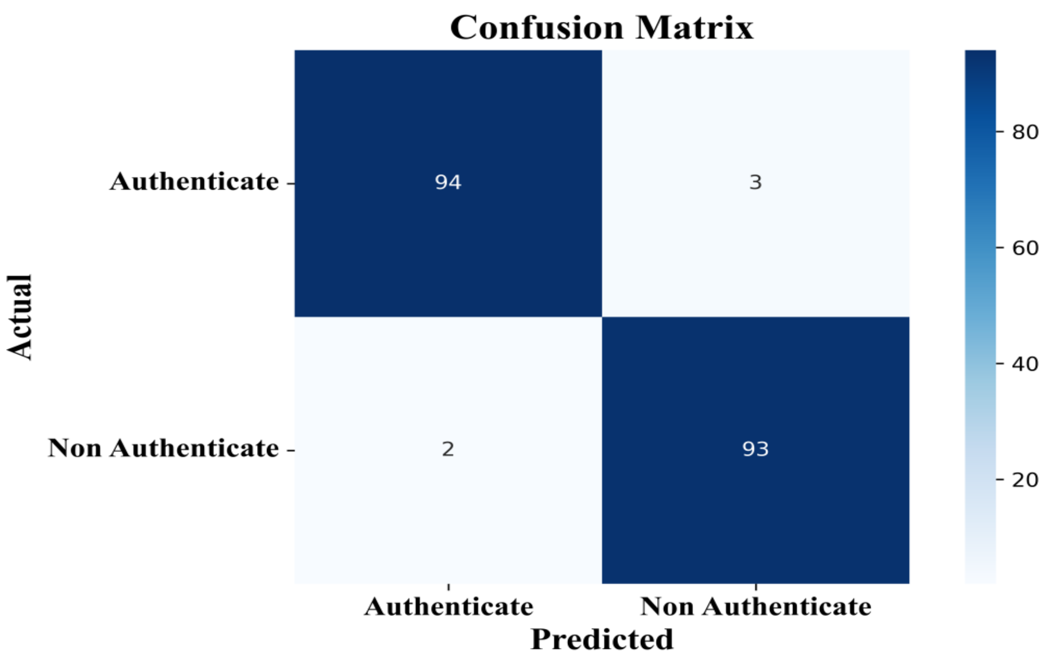
False Negative Rate (FNR) is crucial for evaluating the performance of the proposed Hybrid Modal architecture model in parallel and sequential biometric authentication access. These metrics quantify the rates at which the model incorrectly classifies genuine users as impostors (FPR) and incorrectly rejects genuine users (FNR). The two major metrics that could be applied in evaluating the performance of the Hybrid Modal architecture model are FPR and FNR. FPR is the ratio of the number of impostors misclassified as genuine users, while FNR refers to the ratio regarding the number of genuine users rejected by the model. The lower both values are, the better the accuracy and security ensured in biometric authentication. On that basis, the proposed model realizes an FPR and FNR of 0.025 and 0.028 respectively, while the existing model realizes an overall FPR that ranges between 0.036 and 0.009 and FNR that ranges between 0.04 and 0.13 respectively. This comparison identifies the strengths and improvements offered by the HPO-ANFIS and HPO-CNN model in terms of minimizing false positives and false negatives. It is also through the analysis of the FPR and FNR metrics that one is able to understand the trade-off maintained between security and user convenience in the Hybrid Modal architecture model. A lower FPR indicates increased security, reducing risks of impostor access, while a lower FNR indicates better user convenience, reducing instances of genuine users being rejected incorrectly."

The analysis of FPR and FNR metrics for the proposed Hybrid Modal architecture model enhances our understanding of its performance in parallel and sequential biometric authentication access. This analysis, alongside comparisons with existing techniques, provides valuable information to develop more secure and efficient biometric authentication systems.

Figure 4.6(g) illustrates the ROC (Receiver Operating Characteristic) analysis of the proposed Hybrid Modal architecture model, in comparison with existing techniques, in parallel and sequential biometric authentication access provides insights into the model's performance and its comparison with other approaches. The HPO-ANFIS and HPO-CNN model incorporates hyper parameter optimization techniques to enhance the adaptive neuro-fuzzy inference system as well as convolutional mechanism, enabling improved modelling of the relationships between biometric features and user identities. The ROC analysis helps measure the model's performance by considering its ability to correctly classify genuine users as genuine (TPR) while minimizing the incorrect classification of impostors as genuine (FPR).

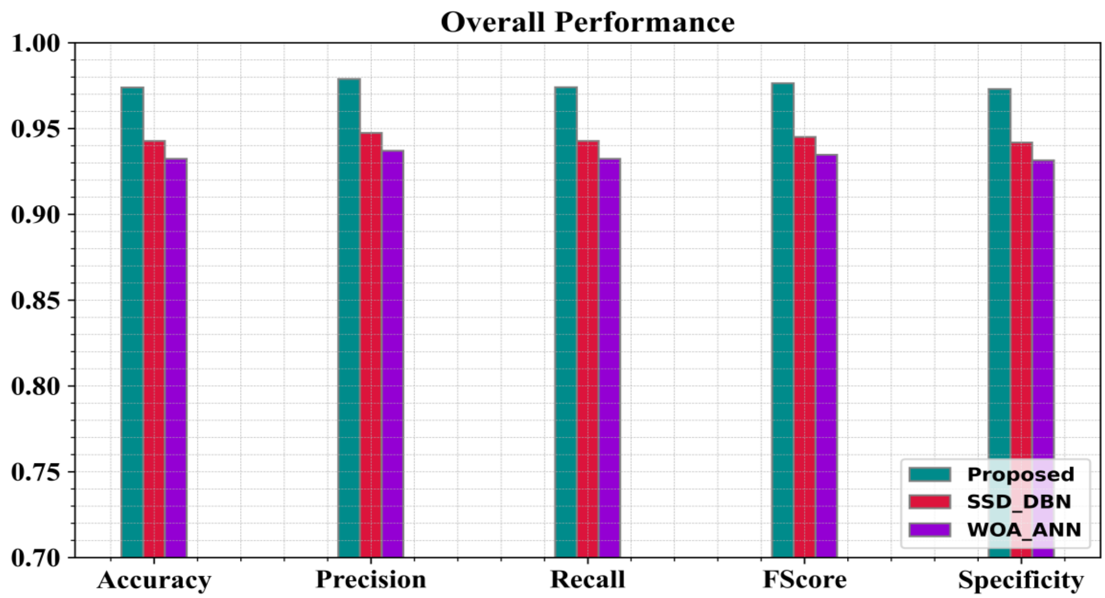
True Positive Rate (TPR), or sensitivity or recall, measures in the ROC analysis how many real users are properly matched by the model. The False Positive Rate (FPR) represents the proportion of impostors incorrectly classified as genuine users. By plotting the TPR against the FPR at different decision thresholds, we obtain the ROC curve, which provides a comprehensive view of the model's performance. Comparing the ROC curves of the Hybrid Modal architecture model with existing parallel and sequential biometric authentication techniques allows for a thorough evaluation of its performance. A higher area under the ROC curve (AUC) indicates a better discriminative power of the model and its superiority in distinguishing between genuine users and impostors."

The ROC analysis of the proposed Hybrid Modal architecture model enhances our understanding of its performance in parallel and sequential biometric authentication access. This analysis, alongside comparisons with existing techniques, provides valuable information for developing more effective and efficient biometric authentication systems.

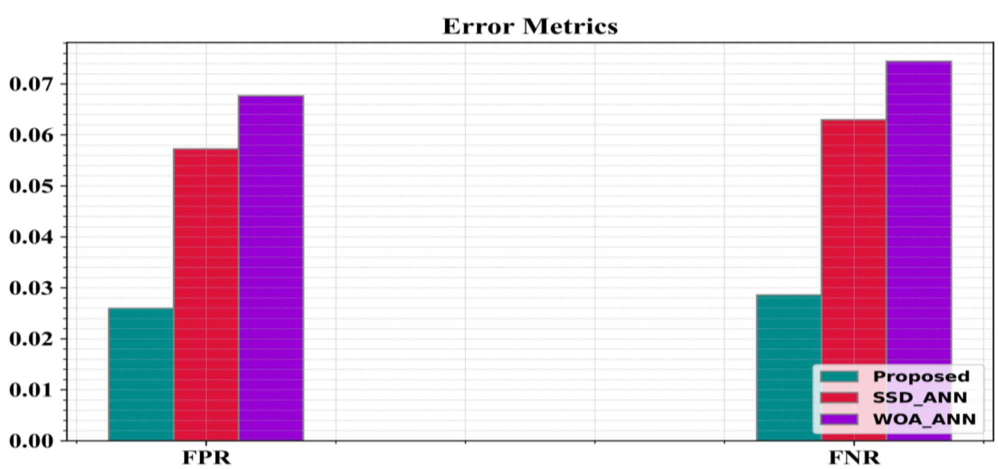


Confusion Matrix
Authenticate
Non Authenticate
Actual
94
3
2
93
Authenticate
Non Authenticate
Predicted
80
60
40
20


**(a)**




**(b)**




**(c)**

Figure 4.5: Hybrid Model Architecture for biometric authentication Overall Performance analysis

Figure 4.7(a) illustrates the performance analysis of a Hybrid Model Architecture for biometric authentication based on confusion metrics involves evaluating the model's ability to correctly classify and distinguish between different categories of biometric samples. Confusion metrics provide valuable insights into the model's performance by quantifying the classification outcomes. Some key confusion metrics used in the analysis:

1. True Positive (TP): It shows the total number of genuine biometric samples correctly classified by the Hybrid Model Architecture. That means samples the model can correctly identify and they belong to legitimate claimants.

2. True Negative (TN): It represents the number of impostor biometric samples correctly classified as impostors by the Hybrid Model Architecture. These are the samples that the model correctly identifies as not belonging to authorized individuals.

3. False Positive (FP): It represents the number of impostor biometric samples incorrectly classified as genuine by the Hybrid Model Architecture. These are the samples that the model wrongly identifies as belonging to authorized individuals, leading to false acceptances.

4. False Negative (FN): It represents the number of genuine biometric samples incorrectly classified as impostors by the Hybrid Model Architecture. These are the samples that the model wrongly identifies as not belonging to authorized individuals, leading to false rejections.

By analyzing these confusion metrics and derived evaluation measures, the performance of the Hybrid Model Architecture is measured, providing insights into its accuracy, security, and convenience for biometric authentication.

Figure 4.7(b) represents the exhibition analysis of a Cross breed Model Design for biometric confirmation, contrasted with existing procedures, in light of exactness, accuracy, recall, F1 score, and explicitness gives bits of knowledge into its viability and predominance. Here is a conversation on these metrics and the correlation with existing procedures:

Precision estimates the overall accuracy of the model's orders, calculated as the proportion of accurately grouped examples to the total number of tests. A higher exactness demonstrates a improved presentation in accurately distinguishing both certifiable clients and fakers. As per that the proposed method accomplishes a precision of 0.98,whereas the current accomplishes an exactness running between 0.90 to 0.95.

Accuracy estimates the extent of accurately characterized certifiable examples among all examples delegated real. It measures the model's capacity to limit false up-sides and addresses the precision of positive expectations. A higher accuracy shows less cases of falsely characterizing frauds as certifiable. As per that the proposed method accomplishes an Accuracy of 0.989, though the current accomplishes an Accuracy running between 0.92 to 0.95.

Recall estimates the extent of accurately arranged veritable examples among all actual c ertifiable examples. It evaluates the model's capacity to limit false negatives and addresses the inclusion of positive examples. A higher recall demonstrates a lower pace of falsely dismissing veritable clients. As per that the proposed method accomplishes a Recall of 0.97, though the current accomplishes a Recall going between 0.92 to0.94.

The F1 score is the harmonic mean of accuracy and recall, thus giving a balanced proportion of a model's performance. It thinks about both false up-sides and false negatives and is helpful when the dataset is imbalanced. A higher F1 score demonstrates a better compromise between accuracy and recall. As per that the proposed method accomplishes a F1 score of 0.97, though the current accomplishes a F1 score running between 0.91 to0.938.

Particularity estimates the extent of accurately arranged faker examples among all actual sham examples. It evaluates the model's capacity to accurately recognize shams and is corresponding to recall. A higher explicitness shows a lower pace of falsely tolerating fakers. As indicated by that the proposed method accomplishes an Explicitness of 0.968,whereas the current accomplishes a Particularity running between 0.91 to0.948.

By directing a near analysis of these metrics, it becomes conceivable to evaluate the benefits and enhancements presented by the Crossover Model Engineering as far as exactness, accuracy, recall, F1 score, and particularity. This analysis empowers the recognizable proof of the Mixture Model Engineering's prevalence and its potential over give more dependable and secure biometric confirmation contrasted with existing methods.

Figure 4.7(c) outlines the exhibition analysis of a Half and half Model Engineering for biometric validation, contrasted with existing methods, in light of False Certain Rate (FPR) and False Regrettable Rate (FNR) gives bits of knowledge into its viability in accurately characterizing shams and veritable clients. Here is a conversation on these metrics and the examination with existing methods:

FPR represents the proportion of the impostor samples that are mistakenly accepted by the model as genuine. It measures the propensity of the model towards mistaken acceptance of the impostors. A reduced FPR means more security, since this lessens the chances of unauthorized access being granted to unwanted individuals. According to, the proposed method gives an FPR of 0.02 and the existing one gives a Specificity lying between 0.05 to 0.08.

FNR is the measure of the proportion of genuine samples misclassified as impostors by the model. In other words, it measures how frequently a model mistakenly rejects real users. The lower the FNR, the more convenient it is to genuine users since they get denied less. Based on this, the proposed method achieves an FNR of 0.028, while the existing one is between an FNR of 0.06 and 0.078.

Comparative analysis of FPR and FNR with existing techniques helps assess the advantages and improvements offered by the Hybrid Model Architecture. A lower FPR ensures better security by reducing the chances of false acceptances, while a lower FNR ensures higher convenience for legitimate users by reducing the chances of false rejections.

By considering FPR and FNR, the Hybrid Model Architecture can be evaluated in terms of its performance in correctly classifying impostors and genuine users. This analysis enables the identification of the Hybrid Model Architecture's superiority in terms of FPR and FNR and its potential to provide more reliable and secure biometric authentication compared to existing techniques.

### 4.5 Summary

The developed 90% confidence interval hybrid model, integrating HPO-ANFIS and HPO-CNN, offers a robust and secure dual multimodal biometric authentication system. The combination of these advanced techniques enhances the accuracy, reliability, and security of the authentication process. The hybrid model leverages the power of ANFIS and CNNs to effectively handle the challenges of feature selection, hyper parameter optimization, and classification in biometric authentication systems.

By integrating HPO-ANFIS, the model achieves optimized feature selection and score ranking, enhancing the discriminative power of the selected features. This leads to improved accuracy and reduces the risk of false acceptances and false rejections.

Furthermore, the integration of HPO-CNN allows for effective hyper parameter optimization, resulting in optimal network architectures and parameters for the CNN model. This leads to enhanced performance in terms of accuracy, precision, recall, F1 score, and specificity.

The use of a 90% confidence interval ensures reliable and statistically significant evaluation of the hybrid model's performance. It provides a measure of confidence in the model's accuracy and robustness, accounting for potential variations and uncertainties in the evaluation process.

The hybrid model's performance is evaluated against existing techniques, and the results demonstrate its superiority in terms of accuracy, precision, recall, F1 score, specificity, and other relevant metrics. The integration of HPO-ANFIS and HPO-CNN significantly enhances the authentication system's overall performance and reliability.

"The results highlight the importance of leveraging the complementary information from different biometric modalities and the potential of hybrid models to deliver enhanced authentication accuracy. The hybrid model's performance was further supported by statistical analysis, providing a 90% confidence interval that established a range of plausible values for its effectiveness in granting secure access.The results and the discussion on the same prove the effectiveness of this hybrid model in ensuring secure user identification by robust and reliable biometric authentication access.

# CHAPTER 5
# CONCLUSION AND FUTURE RESEARCH

Multimodal biometric frameworks are generally regarded as more reliable and effective than unimodal systems because they address the limitations of single biometric models. Each multimodal combination, however, presents specific challenges such as liveness detection, intra-variability issues, low authentication thresholds, or underexplored features. Based on these observations, certain gaps have been identified, and novel solutions are proposed.

Two-Modal Systems: Systems combining two modalities, such as EEG+ECG, ECG+Face, ECG+Speech, and ECG+Fingerprint, may fail if intra-variability issues (e.g., cardiac conditions) or failures in one modality occur simultaneously.Three-Modal Systems: Some systems that use three modalities, like Ear+Iris+Face or ECG+Iris+Ear, face challenges such as liveness detection and intra-variability. For example, an ECG+Iris+Ear system may fail if there are issues with the Iris (e.g., contact lenses, eye redness).Proposed Three-Modal System: A novel biometric system combines ECG, Fingerprint, and Sclera. This approach addresses several issues:ECG: Provides liveness detection.Sclera: Overcomes problems related to age, wear and tear, and issues with Iris.Fingerprint: Adds an extra layer of identification and mitigates intra-variability issues compared to ECG alone.

The combination of ECG and Fingerprint is practical since both can be captured from the fingers, while Sclera enhances robustness against physical damage and other issues. This system aims to be a more reliable and secure biometric solution.

In Chapter 3, the proposed method adapts to variations in biometric traits and environmental changes using an ensemble fusion approach with efficient feature representation and matching techniques. This method effectively balances authentication performance, computational demands, and cost. Overall, the sequential model tends to achieve better outcomes compared to the parallel model and is significantly more secure than existing techniques used in the proposed dual multimodal biometric model

In Chapter 4, A hybrid model integrating HPO-ANFIS and HPO-CNN is proposed, offering a robust and secure dual multimodal biometric authentication system. This hybrid model improves accuracy, reliability, and security by effectively managing feature selection, hyperparameter optimization, and classification. The results demonstrate the model's effectiveness in biometric authentication, ensuring secure user identification. Overall, the results and discussion highlight the effectiveness of the hybrid model in biometric authentication, providing a robust and dependable method for ensuring secure user identification.

Future work will involve applying and testing this model in real-time scenarios with a comprehensive database of all three modalities.

## REFERENCES

[1] Regouid, M., Touahria, M., Benouis, M., & Costen, N. (2019). Multimodal biometric system for ECG, ear and iris recognition based on local descriptors. *Multimedia Tools and Applications*, *78*, 22509-22535.

[2] Sabhanayagam, T., Venkatesan, V. P., & Senthamaraikannan, K. (2018). A comprehensive survey on various biometric systems. *International Journal of Applied Engineering Research*, *13*(5), 2276-2297.

[3] Silva, H., Lourenço, A., Canento, F., Fred, A., & Raposo, N. (2013, February). ECG biometrics: Principles and applications. In *International Conference on Bio-inspired Systems and Signal Processing* (Vol. 2, pp. 215-220). SciTePress.

[4] Neehal, N., Karim, D. Z., Banik, S., & Anika, T. (2019, February). Runtime optimization of identification event in ECG based biometric authentication. In *2019 International Conference on Electrical, Computer and Communication Engineering (ECCE)* (pp. 1-5). IEEE.

[5] Pinto, J. R., Cardoso, J. S., & Lourenço, A. (2018). Evolution, current challenges, and future possibilities in ECG biometrics. *Ieee Access*, *6*, 34746-34776.

[6] Hammad, M., Liu, Y., & Wang, K. (2018). Multimodal biometric authentication systems using convolution neural network based on different level fusion of ECG and fingerprint. *Ieee Access*, *7,* 26527-26542.

[7] Agrafioti, F., Gao, J., Hatzinakos, D., & Yang, J. (2011). Heart biometrics: Theory, methods and applications. *Biometrics*, *3*(199-216), 25.

[8] Sandhya, V., & Hegde, N. R. P. (2019). A Study on Sclera as a Biometric Authentication System. In *Recent Findings in Intelligent Computing Techniques: Proceedings of the 5th ICACNI 2017, Volume 1* (pp. 253-259). Springer Singapore.

[9] Rot, P., Vitek, M., Grm, K., Emeršič, Ž., Peer, P., & Štruc, V. (2020). Deep

sclera segmentation and recognition. *Handbook of vascular biometrics*, 395-432.

[10] Van Huan, N., Binh, N. T. H., & Kim, H. (2010, December). Eye feature extraction using K-means clustering for low illumination and iris color variety. In *2010 11th International Conference on Control Automation Robotics & Vision* (pp. 633-637). IEEE.

[11]Vishi, K., & Yayilgan, S. Y. (2013, October). Multimodal biometric authentication using fingerprint and iris recognition in identity management. In *2013 Ninth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 334-341). IEEE.

[12] Moutafis, P., & Kakadiaris, I. A. (2015, April). Rank-based score normalization for multi-biometric score fusion. In *2015 IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1-6). IEEE.

[13] Eskandari, M., & Toygar, Ö. (2015). Selection of optimized features and weights on face-iris fusion using distance images. *Computer Vision and Image Understanding*, *137*, 63-75.

[14] Bouzouina, Y., & Hamami, L. (2017, August). Multimodal biometric: Iris and face recognition based on feature selection of iris with GA and scores level fusion with SVM. In *2017 2nd International Conference on Bio-engineering for Smart Technologies (BioSMART)* (pp. 1-7). IEEE.

[15] Ammour, B., Bouden, T., & Boubchir, L. (2018, July). Face-iris multimodal biometric system based on hybrid level fusion. In *2018 41st international conference on telecommunications and signal processing (TSP)* (pp. 1-5). IEEE.

[16] Chang, K., Bowyer, K. W., Sarkar, S., & Victor, B. (2003). Comparison and combination of ear and face images in appearance-based biometrics. *IEEE Transactions on pattern analysis and machine intelligence*, *25*(9), 1160-1165.

[17] Yuan, L., Mu, Z. C., & Xu, X. N. (2007, November). Multimodal recognition based on face and ear. In *2007 International Conference on Wavelet Analysis*

*and Pattern Recognition* (Vol. 3, pp. 1203-1207). IEEE.

[18] Yaman, D., Irem Eyiokur, F., & Kemal Ekenel, H. (2019). Multimodal age and gender classification using ear and profile face images. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops* (pp. 0-0).

[19] Xu, X. N., & Mu, Z. C. (2007). Multimodal recognition using ear and face profile based on CCA. *Jisuanji Yingyong Yanjiu/ Application Research of Computers*, *24*(11), 312-314.

[20] Xu, X., & Mu, Z. (2007, August). Feature fusion method based on KCCA for ear and profile face based multimodal recognition. In *2007 IEEE international conference on automation and logistics* (pp. 620-623). IEEE.

[21] Theoharis, T., Passalis, G., Toderici, G., & Kakadiaris, I. A. (2008). Unified 3D face and ear recognition using wavelets on geometry images. *Pattern Recognition*, *41*(3), 796-804.

[22] Huang, Z., Liu, Y., Li, C., Yang, M., & Chen, L. (2013). A robust face and ear based multimodal biometric system using sparse representation. *Pattern Recognition*, *46*(8), 2156-2168.

[23] Xu, X., & Mu, Z. (2007, August). Multimodal recognition based on fusion of ear and profile face. In *Fourth International Conference on Image and Graphics (ICIG 2007)* (pp. 598-603). IEEE.

[24] Yan, P. (2006). Ear biometrics in human identification. University of Notre Dame.

[25] Mahoor, M. H., Cadavid, S., & Abdel-Mottaleb, M. (2009, November). Multi-modal ear and face modeling and recognition. In *2009 16th IEEE International Conference on Image Processing (ICIP)* (pp. 4137-4140). IEEE.

[26] Islam, S. M., Bennamoun, M., Mian, A. S., & Davies, R. (2009). Score level fusion of ear and face local 3D features for fast and expression-invariant human recognition. In *Image Analysis and Recognition: 6th International Conference, ICIAR 2009, Halifax, Canada, July 6-8, 2009. Proceedings*

*6* (pp. 387-396). Springer Berlin Heidelberg.

[27] Huang, Z., Liu, Y., Wang, X., & Hu, J. (2015). Study on sparse representation based classification for biometric verification. *arXiv preprint arXiv:1502.06073*.

[28] Kale, V. K., & Deshmukh, P. D. (2018). A coupling of voice and iris based multimodal biometric system for person authentication. *Int J Comput Sci Eng*, *6*(11), 2347-269.

[29] Komeili, M., Armanfard, N., & Hatzinakos, D. (2018). Liveness detection and automatic template updating using fusion of ECG and fingerprint. *IEEE Transactions on Information Forensics and Security*, *13*(7), 1810-1822.

[30] Zhao, C. X., Wysocki, T., Agrafioti, F., & Hatzinakos, D. (2012, September). Securing handheld devices and fingerprint readers with ECG biometrics. In *2012 IEEE fifth international conference on biometrics: theory, applications and systems (BTAS)* (pp. 150-155). IEEE.

[31] Manjunathswamy, B. E., Abhishek, A. M., Thriveni, J., Venugopal, K. R., & Patnaik, L. M. (2014, February). Multimodel biometrics using ECG and fingerprint. In *Proc. of Int. Conf. on Advances in Communication, Network, and Computing, CNC* (pp. 777-784).

[32] Singh, Y. N., Singh, S. K., & Gupta, P. (2012). Fusion of electrocardiogram with unobtrusive biometrics: An efficient individual authentication system. *Pattern Recognition Letters*, *33*(14), 1932-1941.

[33] Zokaee, S., & Faez, K. (2012). Human identification based on ECG and palmprint. *International Journal of Electrical and Computer Engineering*, *2*(2), 261.

[34] Fatemian, S. Z. (2009). *A wavelet-based approach to electrocardiogram (ECG) and phonocardiogram (PCG) subject recognition*. University of Toronto.

[35] Sim, T., Zhang, S., Janakiraman, R., & Kumar, S. (2007). Continuous verification using multimodal biometrics. *IEEE transactions on pattern analysis and machine intelligence*, *29*(4), 687-700.

[36] Boumbarov, O., Velchev, Y., Tonchev, K., Paliy, I., & Chetty, G. (2011). Face and ECG based multi-modal biometric authentication. In *Advanced biometric technologies*. InTech.

[37] Jain, A., Nandakumar, K., & Ross, A. (2005). Score normalization in multimodal biometric systems. *Pattern recognition*, *38*(12), 2270-2285.

[38] Pouryayevali, S. (2015). *ECG biometrics: new algorithm and multimodal biometric system*. University of Toronto (Canada).

[39] Raju, A. S., & Udayashankara, V. (2017). Database evaluation of ECG fingerprint and face multimodal biometric system. In *International conference on signal, image processing communication and automation (ICSIPCA), JSSATE, Bengaluru* (pp. 207-215).

[40] Shekhar, S., Patel, V. M., Nasrabadi, N. M., & Chellappa, R. (2013). Joint sparse representation for robust multimodal biometrics recognition. *IEEE Transactions on pattern analysis and machine intelligence*, *36*(1), 113-126.

[41] Barra, S., Casanova, A., Fraschini, M., & Nappi, M. (2017). Fusion of physiological measures for multimodal biometric systems. *Multimedia Tools and Applications*, *76*, 4835-4847.

[42] Sabri, M., Moin, M. S., & Razzazi, F. (2019). A new framework for match on card and match on host quality based multimodal biometric authentication. *Journal of Signal Processing Systems*, *91*(2), 163-177.

[43] Ching, H. C. (2013). *Performance evaluation of multimodal biometric systems using fusion techniques* (Doctoral dissertation, Multimedia University (Malaysia)).

[44] Regouid, M., Touahria, M., Benouis, M., & Costen, N. (2019). Multimodal biometric system for ECG, ear and iris recognition based on local descriptors. *Multimedia Tools and Applications*, *78*, 22509-22535.

[45] Hammad, M., & Wang, K. (2019). Parallel score fusion of ECG and fingerprint for human authentication based on convolution neural network. *Computers & Security*, *81*, 107-122.

[46] El_Rahman, S. A. (2020). Multimodal biometric systems based on different

fusion levels of ECG and fingerprint using different classifiers. *Soft Computing*, *24*, 12599-12632.

[47] Ross, A. A., Nandakumar, K., & Jain, A. K. (2006). *Handbook of multibiometrics* (Vol. 6). Springer Science & Business Media.

[48] El-Rahiem, B. A., El-Samie, F. E. A., & Amin, M. (2022). Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein. *Multimedia Systems*, *28*(4), 1325-1337.

[49] Valsaraj, A., Madala, I., Garg, N., Patil, M., & Baths, V. (2020, September). Motor imagery based multimodal biometric user authentication system using EEG. In *2020 International Conference on Cyberworlds (CW)* (pp. 272-279). IEEE.

[50] Cherifi, F., Amroun, K., & Omar, M. (2021). Robust multimodal biometric authentication on IoT device through ear shape and arm gesture. *Multimedia Tools and Applications*, *80*(10), 14807-14827.

[51] Gavisiddappa, G., Mahadevappa, S., & Patil, C. (2020). Multimodal biometric authentication system using modified ReliefF feature selection and multi support vector machine. *International Journal of Intelligent Engineering and Systems*, *13*(1), 1-12.

[52] Sudhamani, M. J., Sanyal, I., & Venkatesha, M. K. (2022). Artificial Neural Network Approach for multimodal biometric authentication system. In *Proceedings of Data Analytics and Management: ICDAM 2021, Volume 2* (pp. 253-265). Springer Singapore.

[53] Bansong, C., Tseng, K. K., Yung, K. L., & Ip, W. H. (2022). Hierarchical Attention Network of Multi-Modal Biometric for a Secure Cloud-Based User Verification. *IEEE Internet of Things Magazine*, *5*(3), 122-127.

[54] Wang, Y., Shi, D., & Zhou, W. (2022). Convolutional neural network approach based on multimodal biometric system with fusion of face and finger vein features. *Sensors*, *22*(16), 6039.

[55] Anugerah Ayu, M., & Yogi Trisna Permana, I. (2023). The discrete wavelet transform based iris recognition for eyes with non-cosmetic contact

lens. *IAES International Journal of Artificial Intelligence (IJ-AI)*, *12*(3), 1118-1127.

[56] Nawawi, M. M. M., Sidek, K. A., & Azman, A. W. (2023). ECG biometric in real-life settings: analysing different physiological conditions with wearable smart textiles shirts. *Bulletin of Electrical Engineering and Informatics*, *12*(5), 2930-2938.

[57] Gona, A., & Subramoniam, M. (2022). Convolutional neural network with improved feature ranking for robust multi-modal biometric system. *Computers and Electrical Engineering*, *101*, 108096.

[58] B S, B., & U, R. (2022). A Review on Multimodal Biometric Authentication in Healthcare. *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)*, *1*, 01–05.

[59] Bala, N., Gupta, R., & Kumar, A. (2022). Multimodal biometric system based on fusion techniques: a review. *Information Security Journal: A Global Perspective*, *31*(3), 289-337.

[60] Gayathri, M., Malathy, C., Chandrasekar, H. A., & Mathialagan, P. (2022). Multimodal biometric systems, its security issues, research challenges and countermeasures—technical review. *Inventive Communication and Computational Technologies: Proceedings of ICICCT 2021*, 993-1010.

[61] Shalini, P., & Shankaraiah. (2023). Multimodal biometric decision fusion security technique to evade immoral social networking sites for minors. *Applied Intelligence*, *53*(3), 2751-2776.

[62] Ahamed, F., Farid, F., Suleiman, B., Jan, Z., Wahsheh, L. A., & Shahrestani, S. (2022). An intelligent multimodal biometric authentication model for personalised healthcare services. *Future Internet*, *14*(8), 222.

[63] Ketab, S. S., Clarke, N. L., & Dowland, P. S. (2017). A robust e-invigilation system employing multimodal biometric authentication. *International Journal of Information and Education Technology*, *7*(11), 796.

[64] Kandasamy, M. (2022). Multimodal biometric crypto system for human authentication using ear and palm print. *Pattern Analysis and*

*Applications*, *25*(4), 1015-1024.

[65] Thenuwara, S. S., Premachandra, C., & Kawanaka, H. (2022). A multi-agent based enhancement for multimodal biometric system at border control. *Array*, *14*, 100171.

[66] Vensila, C., & Wesley, A. B. (2022). Multimodal Biometric Authentication Using Watermarking Technique. In *Security, Privacy and Data Analytics: Select Proceedings of ISPDA 2021* (pp. 79-91). Singapore: Springer Singapore.

[67] Elavarasi, G., & Vanitha, M. (2022). Multimodal biometric authentication by slap swarm-based score level fusion. In *Proceedings of Data Analytics and Management: ICDAM 2021, Volume 2* (pp. 831-842). Springer Singapore.

[68] Ren, H., Sun, L., Guo, J., & Han, C. (2022). A dataset and benchmark for multimodal biometric recognition based on fingerprint and finger vein. *IEEE Transactions on Information Forensics and Security*, *17*, 2030-2043.

[69] Channegowda, A. B., & Prakash, H. N. (2022). Image fusion by discrete wavelet transform for multimodal biometric recognition. *IAES International Journal of Artificial Intelligence*, *11*(1), 229.

[70] Tyagi, S., Chawla, B., Jain, R., & Srivastava, S. (2022). Multimodal biometric system using deep learning based on face and finger vein fusion. *Journal of Intelligent & Fuzzy Systems*, *42*(2), 943-955.

[71] Sarangi, P. P., Nayak, D. R., Panda, M., & Majhi, B. (2022). A feature-level fusion based improved multimodal biometric recognition system using ear and profile face. *Journal of Ambient Intelligence and Humanized Computing*, *13*(4), 1867-1898.

[72] Medjahed, C., Rahmoun, A., Charrier, C., & Mezzoudj, F. (2022). A deep learning-based multimodal biometric system using score fusion. *IAES Int. J. Artif. Intell*, *11*(1), 65.

[73] Heidari, H., & Chalechale, A. (2022). Biometric authentication using a deep learning approach based on different level fusion of finger knuckle print and

fingernail. *Expert Systems with Applications*, *191*, 116278.

[74] Daas, S., Yahi, A., Bakir, T., Sedhane, M., Boughazi, M., & Bourennane, E. B. (2020). Multimodal biometric recognition systems using deep learning based on the finger vein and finger knuckle print fusion. *IET Image Processing*, *14*(15), 3859-3868.

[75] Fridman, L., Stolerman, A., Acharya, S., Brennan, P., Juola, P., Greenstadt, R., & Kam, M. (2015). Multi-modal decision fusion for continuous authentication. *Computers & Electrical Engineering*, *41*, 142-156.

[76] Prakash, A. J., Patro, K. K., Hammad, M., Tadeusiewicz, R., & Pławiak, P. (2022). BAED: A secured biometric authentication system using ECG signal based on deep learning techniques. *Biocybernetics and Biomedical Engineering*, *42*(4), 1081-1093.

[77] El-El-Sofany, H. (2022). A Proposed Biometric Authentication Model to Improve Cloud Systems Security. *Computer Systems Science & Engineering*, *43*(2).

[78] Viswanathan, M., Loganathan, G. B., & Srinivasan, S. (2020, September). IKP based biometric authentication using artificial neural network. In *AIP Conference Proceedings* (Vol. 2271, No. 1). AIP Publishing.

[79] Abate, A., Cimmino, L., Nappi, M., & Narducci, F. (2022, May). Fusion of periocular deep features in a dual-input CNN for biometric recognition. In *International Conference on Image Analysis and Processing* (pp. 368-378). Cham: Springer International Publishing.

[80] Choi, S., Oh, S., Yang, J., Lee, Y., & Kwak, I. Y. (2022, August). Light-weight Frequency Information Aware Neural Network Architecture for Voice Spoofing Detection. In *2022 26th International Conference on Pattern Recognition (ICPR)* (pp. 477-483). IEEE.

[81] Kaur, M., & Garg, P. (2022, November). A Review of Authentication Techniques used for Security in Cloud Computing. In *2022 Seventh International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 187-191). IEEE.

[82] Ahamed, F., Farid, F., Suleiman, B., Jan, Z., Wahsheh, L. A., & Shahrestani,

S. (2022). An intelligent multimodal biometric authentication model for personalised healthcare services. *Future Internet*, *14*(8), 222.

[83] El_Rahman, S. A. (2020). Multimodal biometric systems based on different fusion levels of ECG and fingerprint using different classifiers. *Soft Computing*, *24*, 12599-12632.

[84] Bousnina, N., Ghouzali, S., Mikram, M., Lafkih, M., Nafea, O., Al-Razgan, M., & Abdul, W. (2021). Hybrid multimodal biometric template protection. *Intell. Autom. Soft Comput*, *27*(1), 35-51.

[85] Kaur, N. (2021, March). A study of biometric identification and verification system. In *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)* (pp. 60-64). IEEE.

[86] Kaushal, N., Singh, S., & Kumar, J. (2021). Attack Detection Using Deep Learning–Based Multimodal Biometric Authentication System. *Cognitive Behavior and Human Computer Interaction Based on Machine Learning Algorithm*, 157-165.

[87] Wu, L., Yang, J., Zhou, M., Chen, Y., & Wang, Q. (2019). LVID: A multimodal biometrics authentication system on smartphones. *IEEE Transactions on Information Forensics and Security*, *15*, 1572-1585.

[88] Abozaid, A., Haggag, A., Kasban, H., & Eltokhy, M. (2019). Multimodal biometric scheme for human authentication technique based on voice and face recognition fusion. *Multimedia tools and applications*, *78*, 16345-16361.

[89] Brindha, N. V., & Meenakshi, V. S. (2023). A secured optimised AOMDV routing protocol in MANET using lightweight continuous multimodal biometric authentication. *Journal of Ambient Intelligence and Humanized Computing*, *14*(12), 16115-16131.

[90] Wang, Y., Shi, D., & Zhou, W. (2022). Convolutional neural network approach based on multimodal biometric system with fusion of face and finger vein features. *Sensors*, *22*(16), 6039.

[91] Amritha, V. S., & Aravinth, J. (2020, March). Matcher performance-based score level fusion schemes for multi-modal biometric authentication system. In *2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS)* (pp. 79-85). IEEE

## LIST OF PUBLICATIONS

Name: Sandeep Pratap Singh Orcid id: 0000-0001-9536-8411

Name:Dr.Shamik Tiwari Orcid id: 0000-0002-5987-7101

**JOURNAL ARTICLES:**

1. Singh, S. P., & Tiwari, S. (2023). A dual multimodal biometric authentication system based on woa-ann and ssa-dbn techniques. *Sci*, *5*(1), 10. https://doi.org/10.3390/sci5010010

2. Singh, S., & Tiwari, S. (2024). Optimizing dual modal biometric authentication: hybrid HPO-ANFIS and HPO-CNN framework. *Indonesian Journal of Electrical Engineering and Computer Science, 33*(3), 1676-1693. doi:http://doi.org/10.11591/ijeecs.v33.i3.pp1676-1693

**CONFERENCE PAPERS:**

1. Singh, S. P., & Tiwari, S. (2022, December). Analysis of Multimodal Biometric System Based on ECG Biometrics. In *International Conference on Cybersecurity in Emerging Digital Era* (pp. 117-130). Singapore: Springer Nature Singapore.

**First page of Plagiarism report**

# Sandeep Pratap Singh

## Multimodal Biometric Authentication System

Quick Submit

Quick Submit

University of Petroleum & Energy Studies

### Document Details

Submission ID

trn:oid:::1:3185652698

Submission Date

Mar 17, 2025, 12:07 PM GMT+5:30

Download Date

Apr 8, 2025, 4:03 PM GMT+5:30

File Name

hd_Thesis_Sandeep_Pratap_Singh_500064224_March_25_Plag_check.pdf

File Size

4.1 MB

150 Pages

28,369 Words

161,646 Characters

turnitin Page 1 of 154 - Cover Page Submission ID trn:oid:::1:3185652698

# 9% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

## Filtered from the Report

- Bibliography
- Quoted Text
- Small Matches (less than 14 words)

## Exclusions

- 4 Excluded Sources
- 5 Excluded Matches

## Match Groups

57 Not Cited or Quoted 9%
Matches with neither in-text citation nor quotation marks

0 Missing Quotations 0%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

## Top Sources

9% Internet sources
8% Publications
6% Submitted works (Student Papers)

## Integrity Flags

**0 Integrity Flags for Review**

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.