EMERGING TRENDS IN MULTIMODAL BIOMETRIC RECOGNITION

Abstract

This chapter provides an in-depth analysis of multimodal biometric frameworks, which incorporate various biometric modalities to improve the exactness and unwavering quality of biometric ID and confirmation. The chapter presents a far-reaching survey of the current literature, featuring the different modalities utilized in multimodal frameworks, for example, fingerprints, face acknowledgment, iris checking, voice acknowledgment, and more. It discusses the advantages and challenges associated with using multiple modalities and explores the algorithms and techniques used for fusion and decision-making in multimodal biometric systems. Furthermore, this chapter examines the applications and potential future developments in this field. The review aims to provide researchers, practitioners, and decision-makers with a comprehensive understanding of multimodal biometric systems, their strengths, limitations, and potential for advancements.

Keywords: Multimodal biometric system, biometric modalities, fusion, decision-making, authentication.

Authors

Prerna
Department of Computer Science and Engineering
Deenbandhu Chhotu Ram University Of Science and Technology
Murthal, Sonipat,India
prernarathee67@gmail.com

Dinesh Kumar Atal
Department of Biomedical Engineering
Deenbandhu Chhotu Ram University of Science And Technology
Murthal Sonipat,India
dinesh20atal@gmail.com

Sanjeev Indora
Department of Computer Science and Engineering
Deenbandhu Chhotu Ram University of Science And Technology
Murthal Sonipat,India
dinesh20atal@gmail.com

I. INTRODUCTION

Biometric frameworks assume a vital part in confirming and recognizing people in light of one of a kind physiological or behavioral qualities. In any case, single biometric modalities have limits concerning exactness, strength, and weakness to mocking assaults. To defeat these difficulties, scientists have created multimodal biometric frameworks that incorporate numerous biometric modalities to improve the general exhibition and dependability of biometric recognizable proof and verification.

Multimodal biometric frameworks use the qualities of various biometric modalities, for example, fingerprints, face acknowledgment, iris filtering, voice acknowledgment, gait examination, and others, to accomplish high precision and diminish the impacts of individual methodology limits[1]. The combination of multiple modalities for more robust and accurate identification by mitigating the impact of noisy or incomplete data, individual variations, and environmental factors.

The concept of multimodal biometrics has gained significant attention in both academic research and practical applications. Numerous studies have focused on exploring the potential of multimodal systems, investigating fusion techniques, developing algorithms for integrating multiple modalities, and evaluating the performance of these systems[3][4]. Researchers have also examined the fusion of various physiological and behavioral modalities to explore new avenues for enhancing the security and fidelity of biometric frameworks [4].

The combination of various biometric modalities can be done at different phases of acknowledgment cycle, including feature, score,and choice level combination. Every fusion technique enjoys its benefits and difficulties, and the decision of fusion technique relies upon the particular necessities of the application and the attributes of the biometric modalities included. Various algorithms, such as weighted sum, Bayesian decision theory, support vector machines, and neural networks, have been employed for fusion and decision-making in multimodal biometric systems[5].

Despite the advantages offered by multimodal biometric systems, there are still difficulties that need to be addressed. These difficulties include data quality, interoperability, scalability, privacy concerns, and the vulnerability of the system to attacks. Researchers continue to explore new techniques and methodologies to enhance the Efficiency, security, and usability of multimodal biometric systems.

The chapter plans to give a thorough analysis of multimodal biometric systems, covering the various modalities used, fusion techniques employed, challenges faced, and potential future developments. It synthesizes the existing literature reviewhighlights the advancements made in this field. By presenting a thorough review, this paper intends to contribute to the understanding and advancement of multimodal biometric systems for identification and authentication purposes.

II. DIFFERENT TYPES OF ATTACKS ON BIOMETRIC SYSTEM

Despite the advantages that biometric frameworks offers, still these biometric frameworks are powerless and suspected to the attacks. There are different kind of attacks arranged in the following classes.

Class-I: Spoof-attack: A phony biometric has been a kind of attack that is introduced , for example, a silicon finger, facial veil, or focal point with an iris design, introduced to a referenced sensor.

Class-II: Replay-attack: Manipulated biometric information is put forwarded to the component extractor, bypassing the referenced sensor. An authenticator should guarantee that the information is caught through the sensor and has not been infused for distinguishing and replay the attacks. In any case, sensor commotion and info varieties present deterrents to this recognition, so the best methodology is to either utilize a timestamp or utilize a test reaction system to address replay-attacks.

Class-III: Substitution- attack:- The component extractor information is redeemed by a malevolent program that capacities according to the attacker's specifics. The attacker gets to limit, either locally or around the world, and can overwrite the real client's format with their own, really taking their personality.

Class -IV: In this, legitimate component merits are superseded with values (fake or ensured) picked by the aggressor or an impersonator.

Class-V: In these trickery attacks, the matcher is replaced with a malevolent program, known as a misdirection.

Class-VI: The attack occurs on the format of data base. The data base can be added to, changed, or dispensed.

Class-VII: Transmission-attack: These are man-in-the-middle type attacks which is possible during the processing of transmission of data, when data is being sent beginning with one party then onto the following. The assailant can control the transmission, send a counterfeit format as an enrolled client, imbue a fake matching score, or even produce a molded response.

Class -VIII: Finally, the inevitable result (recognize or dismiss) can be abrogated by the assailant.

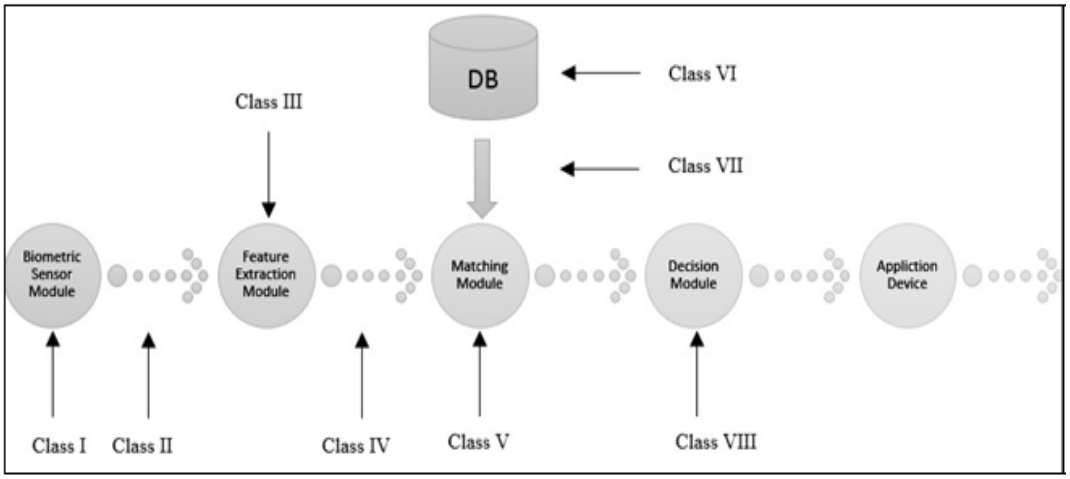

Figure 1: Attacks Location in Biometric System[6]

III. TYPES OF BIOMETRIC SYSTEMS

Biometric identification frameworks that depend on a solitary biometric trait of a person for identification and check are alluded to as unimodal frameworks. Then again, multimodal biometric frameworks are those that use or have the capacity to utilize a mix of at least two biometric modalities to distinguish an individual [7].

Practically speaking, unimodal frameworks are generally utilized in biometric applications, depending on the proof from a solitary wellspring of information for check. Notwithstanding, these frameworks experience different difficulties like commotion in the caught information, intra-class variety, between class similitudes, non-comprehensiveness, and satire assaults. While certain restrictions of unimodal frameworks can be overwhelmed by consolidating different wellsprings of data for identification, bringing about additional dependable frameworks known as multimodal biometric frameworks. These frameworks benefit from the presence of various autonomous biometrics. Instances of normal multimodal biometrics incorporate,“face and fingerprint”, “face and iris”, “iris and fingerprint” etc.

1. **Unimodal Biometric Framework:** Truly, unimodal frameworks are normally utilized in biometric framework applications, depending on the approval of a solitary wellspring of information. In any case, these frameworks face different difficulties, for example, commotion in the caught information because of rehashed utilization of a fingerprint sensor, intra-class variety brought about by clients cooperating with the sensor in various ways, and between class likenesses when there are an enormous number of clients, bringing about cross-over in the component space of various individuals. Another challenge is non-extensiveness, where the biometric framework will be unable to get significant biometric information from a subset of clients. Also, there is the danger of parody assaults when biometric traits, for example, mark or voice are utilized in the framework. A portion of these restrictions of unimodal frameworks can be overwhelmed by consolidating numerous wellsprings of data for identification, prompting the improvement of multimodal biometric frameworks. These frameworks are more dependable because of the presence of different autonomous biometrics and proposition

better execution, as it becomes hard for a fraud to mirror various biometric attributes at the same time.

Moreover, multimodal biometric frameworks give a test reaction component by mentioning the client to introduce an irregular subset of biometric qualities, guaranteeing the presence of a "live" client during information procurement.

2. **Multimodal Biometric Framework:** A multimodal biometric framework is a structure that consolidates the got results from numerous biometric traits with the end goal of individual identification. Contrasted with unimodal frameworks, multimodal biometric frameworks are more solid since they use various autonomous biometric modalities. By integrating various modalities, multimodal biometric frameworks can accomplish higher precision and further develop the in general biometric identification process. Interestingly, unimodal biometric frameworks may not give Maximal precision because of impediments, for example, non-inclusiveness. For instance, in a fingerprint biometric framework, there might be situations where people have harmed, worn, or unrecognizable fingerprints, bringing about mistaken identification results.

One of the benefits of multimodal biometric frameworks is their strength to failures in a solitary innovation. Assuming that one innovation neglects to give exact outcomes, the presence of various technologies in a multimodal framework guarantees that identification can in any case be accomplished. This lessens the effect of caricaturing assaults and improves the general proficiency of the framework. One more critical advantage of multimodal biometric frameworks is the huge decrease in the failure-to-enroll (FTE) rate, which adds to their reliability and effectiveness.

Ordinarily, a biometric framework comprises of four normal modules: "sensor-module", "extraction-module", "matching-module", and "decision-making module". These modules cooperate to catch biometric information, extricate pertinent highlights, contrast them and put away formats, and pursue a choice with respect to the personality of the person. Every one of these modules assumes a vital part in the general working of the biometric framework [3].

Table 1: Shows Different Multimodal Categories

Category	Type of Information	Physiological Biometric	Behavioral Biometric
Hearing	Audio	Speaker recognition	Speech and singing
Sight	Imagesand videos	Ear shape, facial features, fingerprints, hand veins, iris patterns, lips, palmprints, retinas, tongue prints	Blinking, facial expressions, eye movements, walking style, lip movements, signature dynamics
Smell	Odor molecules	Body odor	Not yet specified

Touch	Force and movement, position or pressure, temperature	Facial thermography, hands thermography	Haptic feedback, handgrip analysis, car driving's style, keystroke's dynamics, mouse movement
Metadata	Data types, timezone, location, sequences, shapes	Dentals records, DNA	Audit trail, authorship analysis, email behavior's, textual analysis, touch dynamics

IV. DIFFERENT MODULES IN MULTIMODAL BIOMETRIC SYSTEM

In multimodal biometric frameworks fusion is accomplished by running at least two biometric traits against at least two distinct calculations which is then used to show up at a decision. The different modules are as:-

1. **Sensor-Module:** In the sensor module, the bio-metric sensors or scanner is utilized to quantify the harsh information of the client. This harsh biometric information is recorded and consequently moved to the going with module for incorporate extraction. The plan of the sensor module in the biometric design can impact factors like expense and size.

2. **Feature-Extraction-Module:** In the feature extraction module, the rough data got from the sensor module is dealt with to make a brief yet trademark mechanized depiction of the fundamental biometric characteristics or modalities. Resulting to removing the features, they are given as contribution to the following module that is matching module for extra assessment.

3. **Matching-Module:** The isolated features are differentiated and the formats set aside in the informational collection, achieving a match score. The idea of the biometric data gave can affect this match score. The matching module similarly unites a decision-creation module where the made match score is used to endorse the dependable person.

4. **Decision Making Module:** This module picks in the event that the client is a veritable client or a unveritable considering the match scores. These match scores are utilized to either uphold the personality of an individual or give an arranging of chosen characters for undeniable affirmation purposes. The block outline of a multimodal biometric framework is outlined in Figure-2.

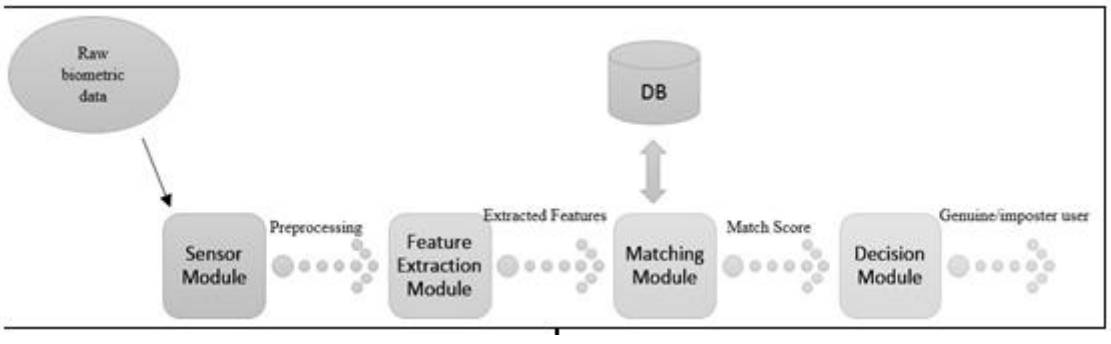

Figure 2: Biometric System [6]

V. FUSION LEVEL IN MULTIMODAL BIOMETRIC SYSTEM

Fusion can be done at any level or at any module in multimodal biometric system. Information can be fused at any four module :-

1. **Sensor Level Fusion:** In sensor-level fusion, the crude data from various sensors is joined. This can include utilizing tests of the equivalent biometric characteristic got from various working sensors or various cases of the equivalent biometric quality caught utilizing a solitary sensor. At the sensor level, data fusion happens at a beginning phase, bringing about an abundance of data contrasted with other fusion levels. Notwithstanding, there has been restricted exploration around here.

2. **Feature Extraction Level Fusion:** In highlight extraction-level fusion, the data or capabilities from various sensors or sources are blended. Highlights removed from every sensor structure individual component vectors, which are then linked to frame a solitary new vector. In highlight level fusion, similar component extraction calculation or various calculations can be utilized across various modalities. Be that as it may, include level fusion acts difficulties like the relationship between elements is obscure, and clashing highlights are normal, prompting dimensionality issues. Because of these difficulties, restricted work has been accounted for on extraction level fusion in multimodal biometric systems.

3. **Matcher Score Level Fusion:** Each framework gives a matching score showing the closeness between the part vector and the format vector. These scores can be merged to endorse the reliable character. Since the scores got from distinct matchers may not be straightforwardly similar, score normalization techniques are utilized to adjust them on a similar scale. Matcher score fusion gives rich data about the information and is generally direct to consolidate, bringing about huge examination endeavors around here.

4. **Decision Level Fusion:** At the decision level, the ultimate results from various classifiers are consolidated. A greater part casting a ballot plan can be utilized to pursue the last choice. Nonetheless, decision-level fusion includes exceptionally different data and is less liked in planning multimodal systems. Biometric systems that coordinate data at prior stages will generally be more hearty contrasted with systems where fusion happens at later stages. Subsequently, include level fusion is considered to give better acknowledgment results, however it very well may be trying to carry out because of similarity issues between the capabilities of various systems. In addition, numerous business biometric systems don't give admittance to the capabilities they use in their items. Matcher score level fusion is for the most part liked as it is generally simple to access and consolidate the scores given by various modalities.

VI. COMPARISON OF DIFFERENT FEATURES USED IN BIOMETRIC SYSTEM

These are seven properties to satisfy quality measures of any Biometric system[8]. Here are some descriptions for each characteristic in the table along with their respective references:

1. **Universality:** Universality refers to the extent to which a biometric identifier is present in the general population. Fingerprints and facial features have a Maximal universality, while iris patterns have a Maximal universality as well.

2. **Distinctiveness:** Distinctiveness represents the degree of uniqueness of a biometric identifier within individuals. Fingerprints exhibit Maximal distinctiveness, while facial features have a Minimal level of distinctiveness.

3. **Permanence:** Permanence reflects the stability and consistency of a biometric identifier over time. Fingerprints and iris patterns have Maximal permanence, while the permanence of hand geometry and retina is considered moderate.

4. **Collectability:** Collectability refers to the ease of acquiring and capturing biometric data. Fingerprints and facial features are relatively easy to collect, while collecting iris patterns and hand geometry is considered moderately challenging.

5. **Performance:** Performance indicates the accuracy and reliability of a biometric identifier in correctly identifying individuals. Fingerprints have Maximal performance, while facial features exhibit lower performance due to variations in lighting and facial expressions.

6. **Acceptability:** Acceptability refers to the level of user acceptance and comfort with using a particular biometric identifier. Fingerprints and facial features are generally well-accepted, while iris recognition may have lower acceptability due to privacy concerns.

7. **Circumvention:** Circumvention represents the susceptibility of a biometric identifier to being bypassed or deceived. Fingerprints and facial features have moderate circumvention risks, while iris recognition and signature verification are considered more resistant to circumvention attempts.

Table 2: Shows Level of Performance in Different Features Used in Multimodal Biometrics

Characteristics	Finger	Facial	Iris	Hand	Retina	Signature
Universality	Maximal	Maximal	Maximal	Moderate	Maximal	Minimal
Uniqueness	Maximum	Minimal	Maximal	Moderate	Maximal	Minimal
Stability	Maximal	Moderate	Maximal	Moderate	Moderate	Minimal
Collectability	Moderate	Maximal	Moderate	Maximal	Minimal	Maximal
Performance	Maximal	Minimal	Maximal	Moderate	Maximal	Minimal
Acceptability	Maximal	Maximal	Minimal	Moderate	Minimal	Maximal
Vulnerability	Moderate	Maximal	Minimal	Moderate	Minimal	Maximal

In Table-2, the term 'Maximal' indicates excellent performance of a specific biometric identifier, while 'Minimal' represents poor performance, and 'moderate' indicates average performance based on the evaluation criteria. The table clearly demonstrates that each biometric trait has its own strengths and weaknesses across the

seven characteristics. Considering these limitations, it is advisable to utilize multiple biometric identifiers to overcome these challenges and enhance overall system performance.

Table 3: Tables Shows Strength and Weakness of Different Features

Biometric Features	Strengths	Weaknesses
Finger-scan	Maximal accuracy, user-friendly, and flexible	Performance degradation over time, inability to enroll some users
Face-scan	Non-intrusive and operates without user cooperation	Reduced matching accuracy due to physiological changes
Signature-scan	Immune to imposters	Error prone rates increased
Hand geometry –scan	definitive core technology and Steady physiological characteristics	Low-accuracy
Retinal-scan	These are Highly-correct	Challenging to Employ and apprehend
Iris-bio-metric	Immune to Inaccurate pairing	Challenging to Employ and apprehend

The strengths and weaknesses of various biometric identifiers [10] are presented in Table-3, providing valuable insights for the selection of biometric identity combinations. This table serves as a useful resource for developing accurate and Maximal-performance biometric identification and authentication systems. By referring to the information presented, the process of selecting appropriate biometric identities can be simplified, facilitating the development of robust and reliable identification solutions.

VII. RELATED WORK

Yash Mittal et al. [11]suggested two use cases for fingerprint biometric systems. One of the applications is an Entry Control Framework (ACS) model, which empowers individual-explicit admittance to a specific entryway utilizing a fingerprint gadget. Another application is a “Classroom Attendance Management Framework (CAMS)”, which uses fingerprints as a biometric include for recording classroom attendance. The CAMS comprises of modules for a database, web UI, and access levels. The two frameworks store fingerprints alongside relating date/time stamps for every client. The fingerprints are powerfully put away in a database to compute different measurements, for example, month-wise or semester-wise attendance patterns on account of CAMS. The ACS and CAMS models were tried utilizing fingerprint information gathered from understudies at IIIT Chittoor, Sri City, India. As per their assessment technique, the typical achievement rate for opening/shutting entryways in ACS was seen to be 87%, while the typical achievement rate for right fingerprint matching in attendance recording for CAMS was estimated at 92%.

Joseph Kalunga and Simon Tembo [12] presented the progression of finger impression biometrics affirmation and actually taking a look at the chiefs framework and showed 99.99% biometric accuracy levels with goof settlement of 0.001% (FAR) and 0.001% (FRR).

Hammam A. Alshazl et al. [13] proposed a short proximity biometric recognition procedure using point based highlights. They utilized four unique ways to deal with accomplish short proximity biometric recognition: “Histogram of Oriented Gradients (Hoard)”, “Weber Local Descriptor (WLD)”, “Local Directional Patterns (LDP)”, and “Local Most extreme Oriented Patterns (LMOP)”. The creators led a thorough arrangement of tests utilizing the, “IIT Delhi-I, IIT Delhi-II, and AMI ear databases”, which are openly accessible. The acquired outcomes are promising, with the LMOP highlights performing extraordinarily well across all cases, accomplishing recognition paces of around 97%.

Gaurav Jaswal et al. [14] proposed a multimodal recognition framework that uses highlight level combination of normalized highlights, including “palm print, hand shape, and hand geometry qualities”. The palm print samples go through pivot and light impacts, which can restrict the matching performance. To address this, the return for capital invested samples are first numerically adjusted and afterward changed into enlightenment invariant patterns utilizing CS-LBP (Center-Symmetric Local Binary Patterns). Also, the local central issues of the changed return for money invested images are separated utilizing the SURF (Speeded Up Robust Elements) descriptor. The presentation of this multimodal recognition framework is accounted for to be better than individual techniques as well as other cutting edge frameworks.

Jianjun Qian et al. [15] proposed a profound part depiction strategy called “Profound Inclination Data (DGI)” for biometric picture acknowledgment. DGI gets the nearby illustration of a picture by handling the histogram of slope course for each full scale pixel. This cycle separates the picture into L sub-pictures considering the angle information of each and every full scale pixel, where L tends to the amount of clusters in the neighborhood histogram.To overhaul the point data, they consider both the heading and size of the chief picture as sub-pictures. For each sub-picture, the histogram of arranged incline (Crowd) is used to take a gander at the point bearing and data. All Group highlights are then accumulated into an extended super-vector. Finally, fisher straight discriminant assessment (FLDA) is applied to get an Immaterial layered and discriminative component vector. The proposed DGI system was surveyed on true face picture datasets, for example, “NUST-RWFR”, “Pubfig”, “LFW”, the “PolyU Finger Knuckle Print dataset”, and the “PolyU palmprint dataset”. The outcomes show that the DGI procedure accomplishes better or practically identical outcomes contrasted with cutting edge calculations like Channel, Hoard, LBP, Poem, Warbler, and IDLS.

Jyothi Ravikumar et al. [16] proposed a convolution-based incorporate extraction framework for face ID using Discrete Wavelet Change (DWT) and Histogram of Organized Inclination for convincing individual certification. Four standard face datasets with changing sizes were taken and resized to “128x128”. A 2D-DWT (Two Layered Discrete Wavelet Change)was applied to the resized face pictures, considering just the LL (Low) sub-band. Swarm was then applied to the LL sub-band to get Group coefficients. At last, 2D convolution was applied to the LL sub-band and the Group plan to eliminate the last highlights. The resized face picture was compacted utilizing DWT and Group. The Euclidean distance (ED) was used to survey the components of the face pictures in the data set with the test pictures to check execution limits. As shown by their disclosures, this system beat existing methods like Local Binary Patterns (LBP).

Fahman Saeed et al. [17] proposed an original fingerprint recognition approach utilizing changed Histograms of Oriented Gradients (HOG). They changed the Hoard bearing extraction technique to catch the edge design in a superior manner, conquering difficulties presented by boisterous, Negligible quality, and corrupted fingerprints. “Exterme Learning Machine (ELM)” with “RBF (Radial Basis Function)” piece was used as a classifier. The proposed procedure was assessed on the benchmark dataset called FVC-2004. The outcomes showed that Hoard based highlights with altered Hoard could really separate the local edge bearing. The fingerprint recognition accomplished a normal precision of 98.7%, outperforming that of cutting edge fingerprint classification techniques.

Vincent Christlein et al. [18] introduced a strategy for robust disconnected essayist distinguishing proof. To accomplish this, the creators used Root Channel descriptors thickly registered on the text shapes. GMM (Gaussian Mixture Model) vectors were utilized as an encoding method to catch the particular handwriting elements of people. GMM quality vectors were made through the modification of a foundational model to the circulation of local trademark descriptors. The creators likewise utilized SVM (Support Vector Machine) to prepare a record explicit comparability measure. For assessment, they used three openly accessible datasets: ICDAR, CVL, and KHATT. The proposed technique showed Maximal recognition precision, especially in the signature handling and encoding steps.

Nainan S and Kulkarni [19] proposed a speaker recognition system that spotlights fair and square of recognition accomplished for both a crude noisy sign and an enhanced sign. The VidTimit dataset was utilized to foster the robotized speaker recognition system. This model was assembled in view of “Vector Quantization (VQ) and Gaussian Mixture Model (GMM)”. As indicated by their discoveries, GMM accomplished a satisfactory speaker recognition accuracy of 96.15%, which is roughly 22% lower than utilizing the first crude signals that gave an accuracy of 74.35%.

Silvio Barra et al. [20] proposed a multimodal biometric recognition system that consolidates the electrocardiogram (ECG) with six distinct classifications of the electroencephalogram (EEG). This approach includes extricating highlights (tops) from the ECG and joining them with ghostly elements got from the EEG. The system was tried on an exceptionally developed dataset comprising of 52 subjects, with signals gathered from two notable data sets. To upgrade the dataset, a drawn out test set was made by consolidating two existing datasets: the PTB Demonstrative ECG Data set for ECG signals and the EEG Engine Development/Symbolism Dataset for EEG signals. The announced outcomes demonstrate superb grouping performance and huge upgrades contrasted with the underlying outcomes. The acquired outcomes, including EERvalues, AUC values, and ROC curves, areas of strength for demonstrate performance.

Ammour et al. [21] proposed a section extraction strategy for a multimodal biometric structure that uses face and iris affirmation. The iris highlight extraction is performed using a multiresolution “2D Log-Gabor channel”, while the facial elements are handled utilizing a productive explicit range examination (SSA) related to wavelet change. The fusion interaction joins pertinent highlights from the two modalities at a cross breed fusion level.

Kabir et al. [22] proposed a clever fusion approach called the half and half fusion approach, which utilized highlight level fusion techniques. In this approach, a weighting technique called mean-outrageous based sureness weighting (MEBCW) was utilized to

remove score values got from the element level fusion, consequently improvingthe accuracy of the multimodal biometric system's recognition. Also, the half breed fusion approach utilized the qualities of the individual unimodal systems to work on the general performance of the various matchers.

Regouid et al. [23] developed a novel multimodal recognition system for ECG-ear-iris biometrics at the element fusion level. The approach included a few phases, including preprocessing, normalization, and division. Nearby surface descriptors were used to remove important highlights from the ECG signal. When the fundamental elements were gotten, the ear and iris pictures were changed into 1D signs. The matching score was then registered utilizing the joined data from the ear and iris.

Al-Waisy et al. [24] presented a consistent biometric framework considering the left and right irises of an person. In this technique, a CNN and Softmax classifier were utilized to remove discriminative highlights from the information picture. A discriminative CNN training plan was utilized to refresh the loads. This approach was supplemented with a bunch of training devices to address overfitting issues.

Anand and Kanhangad [25] proposed a strategy that joins OCT finger skin profundity information with neighborhood pixel picture levels for unique mark recognition. Kuzu et al. [26] used DeepRespores to recognize Maximal-goal pores and learn distinctive finger pore fix-based highlights. Mother et al.[28] utilized a CNN organization to perceive on-the-fly finger-vein designs. Li et al.[27] showed the presentation of a CNN network utilizing a proposed pyramid region stage quantization histogram information. It is seen that the unimodal mix of part learning assignments neglects to absolutely take advantage of the particular hand-finger data, inciting troubles in seeing the open biometric classes. In like manner, the display of the unimodal biometric affirmation system is restricted (Dargan and Kumar) [29].

While Zhang et al.[30], supersede CNN layers with Gabor convolutional channels to diminish the multifaceted design of association limits, Li et al.[31] propose discriminative close by coding in CNN to eliminate significant, “FP-FV and knuckle features for the trimodal SVM model”. Besides, Cherrat et al. [32] suggest a combination of CNN-based features from the face and FP-FV to overhaul multimodal biometric acknowledgment. Abdullahi et al. (2023) [33] use both state change instances of hand customized components and significant learning features to additionally foster the acknowledgment execution of multimodal biometric assessment. Boucherit et al. [34] propose significant CNN features from short ways with various FV pictures, while Wu et al. [35] acquaint start with finish GCN components of FP-FV to address feature space disarray issues. The combination of edge and vertex components can give evidence to beginning to end multimodal biometric learning. Lately, Ren et al. [36] present a multimodal FP-FV dataset called NUPT-FPV, which is incorporated into MobileNet V3 layers and yields a $7 \times 7 \times 960$ component map. Course of action is performed using interlaced picture data from both Max-Insignificant and significant layers. This methodology shows the sensible utilization of significant learning-based multimodal biometric acknowledgement system. Nevertheless, since the precision of biometric pictures is of essential importance, the acknowledgment execution of this technique ought to be moreover moved along. To overhaul the exhibition of CNN associations, there is a need to further develop the part extraction limits of CNN undertakings.

Table 4: Related Work

S.No	Year	Authors	Features Used	Title of Paper	Interpretation
1	2015	Yash Mittal et al.	Fingerprint	"Fingerprint Biometric based Access Control and Classroom Attendance Management System"	Proposed two applications on fingerprint biometric systems: Entrance Control System and CAMS
2	2016	Joseph Kalunga and Simon Tembo	Fingerprint	"Development of Fingerprint Biometrics Verification and Vetting Management System"	Achieved 99.99% biometric precision levels with Minimal FAR and FRR
3	2016	Hammam A. Alshazl et al.	Angle-based features	"A survey on periocular biometrics research"	Utilized four different approaches for close-range biometric recognition
4	2019	Gaurav Jaswal et al.	Palm print, hand shape and hand geometry	"Multimodal Biometric Authentication System Using Hand Shape, Palm Print, and Hand Geometry"	Utilized feature-level fusion of standardized features and achieved superior performance
5	2016	Jianjun Qian et al.	Gradient-based features	"Exploring deep gradient information for biometric image feature representation"	Introduced "Deep Gradient Information (DGI)" technique for biometric image recognition
6	2018	Jyothi Ravikumar et al.	Discrete Wavelet Transform (DWT), Histogram of Oriented Gradient (HOG)	"Convolution based Face Recognition using DWT and HOG"	Utilized DWT and HOG for effective face identification
7	2018	Fahman Saeed et al.	Histogram of Gradient Descriptor (modified HOG)	"Classification of Live Scanned	Proposed a novel fingerprint recognition

				Fingerprints using Histogram of Gradient Descriptor”	approach using modified HOG and achieved Maximal accuracy
8	2017	Vincent Christlein et al.	Root Filter descriptors, GMM vectors	“Writer identification using GMM supervectors and exemplar-SVMs”	Developed a method for robust offline writer identification with Maximal accuracy
9	2016	Nainan S and Kulkarni	Raw and enhanced signals (Speaker recognition)	“A comparison of performance evaluation of ASR for noisy and enhanced signal using GMM”	Achieved Maximaler speaker recognition precision with enhanced signals compared to raw signals
10	2017	Silvio Barra et al.	Electrocardiogram (ECG), Electroencephalogram (EEG)	“Fusion of physiological measures for multimodal biometric systems”	Combined ECG with six categories of EEG to enhance biometric recognition performance
11	2020	Ammour et al.	Face, Iris	“Face-iris multimodal biometric identification system”	Used face and iris acknowledgment for multimodal biometric distinguishing proof
12	2018	Kabir et al.	Multiple modalities	“Weighted hybrid fusion for multimodal biometric recognition system”	Proposed a hybrid fusion approach using feature-level fusion techniques
13	2019	Regouid et al.	ECG, Ear, Iris	“Multimodal biometric system for ECG, ear and iris recognition based on local descriptors”	Developed a multimodal recognition systems based on ECG, ear, and iris using local descriptors

14	2018	Al-Waisy et al.	Iris	“A multi-biometric iris recognition system based on a deep learning approach”	Employed CNN and Softmax classifier for iris recognition with a focus on deep learning
15	2020	Anand and Kanhangad	Fingerprint	“Porenet: CNN-based pore descriptor for Maximal-resolution fingerprint recognition”	Proposed a model in light of CNN-based pore descriptor for Maximal-goal in finger impression affirmation
16	2020	Kuzu et al.	Finger-vein	“On-the-fly finger-vein-based biometric recognition using deep neural networks”	Employed DeepRespores to identify Maximal-resolution finger pores and learn distinctive features
17	2023	Li et al.	Finger vein	“Finger vein recognition based on oval parameter-dependent convolutional neural networks”	Proposed an oval parameter-depends upon CNN for finger vein recognition
18	2021	Ma et al.	Near-infrared based finger vein	“The biometric recognition system based on near-infrared finger vein image”	Fostered a biometric acknowledgment framework in view of close infrared finger vein pictures
19	2020	Dargan and Kumar	Modalities of physiology and behavior	“A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities”	Given a complete overview on biometric acknowledgment frameworks in light of different modalities

20	2022	Zhang et al.	Vein biometric	"Agcnn: Adaptive Gabor convolutional neural networks with receptive fields for vein biometric recognition"	Proposed Adaptive Gabor CNN for biometric in field of vein recognition
21	2021	Li et al.	Multimodal finger recognition	"Local discriminant coding based convolutional feature representation for multimodal finger recognition"	Utilized local discriminant coding in CNN for the recognition of multiple finger modalities
22	2020	Cherrat et al.	Fingerprint, Finger-vein, Face	"Convolutional neural networks approach for multimodal biometric identification system using the fusion of fingerprint, finger-vein and face images"	Proposed a fusion of CNN-based features from different modalities for multimodal biometric acknowledgment
23	2023	Abdullahi et al.	Spatial-temporal state transition patterns	"Lie recognition with multi-modal spatial-temporal state transition patterns based on hybrid CNN-bidirectional LSTM"	Utilized hybrid CNN-bidirectional LSTM for lie recognition using spatial-temporal patterns
24	2022	Boucherit et al.	Finger's vein	"Finger vein identification using	Proposed a deeply-fused CNN for finger

				deeply-fused convolutional neural network"	vein identification
25	2023	Wu et al.	Fingerprint, Finger-vein	"Robust graph fusion and recognition framework for fingerprint and finger-vein"	Proposed a graph based fusion combination and, acknowledgment affirmation system for finger impression and finger-vein
26	2022	Ren et al.	Fingerprint, Finger's vein	"A dataset and benchmark for multimodal biometric recognition based on fingerprint and finger vein"	Introduced a multimodal FP-FV dataset

VIII. CHALLENGES IN DESIGNING MULTIMODAL BIOMETIC SYSTEM

There are different different challenges in designing multimodal biometric system. These are as:-

1. **Sensor Integration:** Coordinating multiple sensors for different biometric modalities can be challenging. Each sensor may have different characteristics, resolutions, and data formats. Ensuring seamless integration and synchronization of data from different sensors is essential for accurate and efficient multimodal biometric recognition.

2. **Feature Fusion:** Combining features from different modalities is a critical step in multimodal biometric systems. Designing effective feature fusion methods that can capture complementary information from different modalities while reducing redundancy is fundamental. The fusion process should be robust to noise, variations, and inconsistencies across modalities.

3. **Alignment and Normalization:** Modalities may exhibit variations in scale, orientation, and spatial alignment. Pre-processing techniques such as alignment and normalization are necessary to bring different modalities into a common representation space. Designing efficient alignment and normalization algorithms that can handle modality-specific variations is important for accurate fusion and matching.

4. **Data Correlation and Dependence:** Modalities within a multimodal biometric system may exhibit correlation and dependence. Designing algorithms that can effectively model and exploit these correlations can improve recognition performance. However, handling dependencies and avoiding over-reliance on a single modality is crucial to ensure system robustness and security.
5. **Scalability and Efficiency:** Multimodal biometric systems often deal with large amounts of data, requiring efficient storage, retrieval, and processing mechanisms. Designing scalable architectures that can handle increasing volumes of data while maintaining real-time performance is critical. Efficient indexing and retrieval mechanisms are essential for fast and accurate matching.

6. **User Acceptance and Usability:** Consideration should be given to user acceptance and usability aspects in designing of multimodal biometric system. The system should be intuitive, user-friendly, and non-intrusive to ensure Maximal user acceptance. Designing interfaces and interaction mechanisms that facilitate easy enrollment and authentication experiences is important for user satisfaction.

7. **Robustness to Attacks and Spoofing:** Multimodal biometric systems should be designed to be robust against various attacks, including spoofing attacks. Incorporating anti-spoofing measures and techniques to detect and prevent spoofing attempts is crucial to ensure system security and reliability.

IX. CONCLUSION AND FUTURE SCOPE

Multimodal biometrics have emerged as a powerful solution for achieving Maximal-level security in a various applications, such as access control, law enforcement, and fraud prevention. By combining multiple biometric modalities, these systems offer robust and accurate authentication and identification capabilities, ensuring the protection of personal data and facilitating secure transactions. However, there are still some challenges that need to be addressed in the design of multimodal systems. These include the selection of appropriate modalities, the determination of optimal feature combination levels, and the management of redundancy in extracted features. Future research should focus on addressing these issues to further improve the system's performance and trustworthiness of multimodal biometric systems. In terms of future scope, one area of research is the exploration of advanced feature fusion techniques that can effectively capture complementary information from different modalities while minimizing redundancy. This can lead to improved recognition accuracy and robustness against variations and noise in the biometric data. Additionally, the development of innovative algorithms for alignment and standardization of modalities is essential to ensure accurate integration and matching. Leveraging ML and DL techniques can also contribute to the advancement of multimodal biometrics by enhancing feature extraction and decision-making processes. Moreover, enhancing the serviceability and user approval rate of multimodal biometric systems should be a priority. This can be achieved by designing intuitive interfaces and seamless integration with existing systems, ensuring a positive and user-friendly experience. Overall, the continuous advancement and research in multimodal biometrics hold great potential for enhancing security systems and providing efficient and reliable solutions for various applications.

REFERENCES

[1] Ross, Arun, et al. “Handbook of Multibiometrics.” Springer Science & Business Media, 2006.
[2] Jain, Anil K., Karthik Nandakumar, and Abhishek Nagar. “Biometric Template Security.” EURASIP Journal on Advances in Signal Processing 2008.1 (2008): 1-17.
[3] Rattani, Ajita, et al. “A Review on Multimodal Biometric Systems.” Procedia Computer Science 45 (2015): 523-532.
[4] Jain, Anil K., Karthik Nandakumar, and Arun Ross. “50 Years of Biometric Research: Accomplishments, Challenges, and Opportunities.” Pattern Recognition Letters 79 (2016): 80-105.
[5] Kumar, Ajay, et al. “Multimodal Biometric Authentication: A Review.” IETE Technical Review 35.3 (2018): 238-255.
[6] Dahea, W., &Fadewar, H.S. (2018). Multimodal Biometric System: A Review. International Journal of Research in Advanced Engineering and Technology, 4(1), 25-31.
[7] Bayometric. “Unimodal vs Multimodal.” Retrieved from [https://www.bayometric.com/]
[8] Sanjekar, P. S., & Patil, J. B. “An Overview of Multimodal Biometrics.” Signal & Image Processing: An International Journal (SIPIJ) 4.1 (2013).
[9] Sahoo, S. K., Choubisa, T., & Mahadeva Prasanna, S. R. “Multimodal Biometric Person Authentication: A Review.” IETE Technical Review 29.1 (2012).
[10] Nanavati, Samir, Michael Thieme, and Raj Nanavati. “Biometrics Identity Verification in a Networked World.” A Wiley Tech Brief, Wiley Computer Publishing, ISBN 0471-09945-7.
[11] Mittal, Y., Varshney, A., Aggarwal, P., Matani, K., & Mittal, V. K. “Fingerprint Biometric-based Access Control and Classroom Attendance Management System.” India Conference (INDICON), 2015, pp. 1-6.
[12] Kalunga, J., & Tembo, S. “Development of Fingerprint Biometrics Verification and Vetting Management System.” American Journal of Bioinformatics Research, 2016, pp. 99-112.
[13] Alonso-Fernandez, F., &Bigun, J. “A Survey on Periocular Biometrics Research.” Pattern Recognition Letters, 2016, pp. 92-105.
[14] Jaswal, G., Kaul, A., & Nath, R. “Multimodal Biometric Authentication System Using Hand Shape, Palm Print, and Hand Geometry.” Computational Intelligence: Theories, Applications and Future Directions, 2019, pp. 557-570.
[15] Qian, J., Yang, J., Tai, Y., & Zheng, H. “Exploring Deep Gradient Information for Biometric Image Feature Representation.” Neurocomputing, 2016, pp. 162-171.
[16] Ravikumar, J., Ramachandra, A. C., Raja, K. B., & Venugopal, K. R. “Convolution-based Face Recognition Using DWT and HOG.” International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), 2018, pp. 327-334.
[17] Saeed, F., Hussain, M., &Aboalsamh, H. A. “Classification of Live Scanned Fingerprints Using Histogram of Gradient Descriptor.” Saudi Computer Society National Computer Conference (NCC), 2018, pp. 1-5.
[18] Christlein, V., Bernecker, D., Hönig, F., Maier, A., &Angelopoulou, E. “Writer Identification Using GMM Supervectors and Exemplar-SVMs.” Pattern Recognition, 2017, pp. 258-267.
[19] Nainan, S., & Kulkarni, V. “A Comparison of Performance Evaluation of ASR for Noisy and Enhanced Signal Using GMM.” International Conference on Computing, Analytics and Security Trends (CAST), 2016, pp. 489-494.
[20] Barra, S., Casanova, A., Fraschini, M., & Nappi, M. “Fusion of Physiological Measures for Multimodal Biometric Systems.” Multimedia Tools and Applications, 2017, pp. 4835-4747.
[21] Ammour, B., Boubchir, L., Bouden, T., &Ramdani, M. “Face-Iris Multimodal Biometric Identification System.” Electronics, 2020, vol. 9, no. 1, pp. 85.
[22] Kabir, W., Ahmad, M. O., & Swamy, M. N. S. “Weighted Hybrid Fusion for Multimodal Biometric Recognition System.” IEEE International Symposium on Circuits and Systems (ISCAS), 2018, pp. 1-4.
[23] Regouid, M., Touahria, M., Benouis, M., &Costen, N. “Multimodal Biometric System for ECG, Ear, and Iris Recognition Based on Local Descriptors.” Multimedia Tools and Applications, 2019, vol. 78, no. 16, pp. 22509-22535.
[24] Al-Waisy, A. S., Qahwaji, R., Ipson, S., Al-Fahdawi, S., &Nagem, T. A. “A Multi-biometric Iris Recognition System Based on a Deep Learning Approach.” Pattern Analysis and Applications, 2018, vol. 21, no. 3, pp. 783-802.
[25] Anand, V., &Kanhangad, V. “PoreNet: CNN-based Pore Descriptor for Maximal-resolution Fingerprint Recognition.” IEEE Sensors Journal, 2020, vol. 20, pp. 9305-9313.
[26] Kuzu, R. S., Piciucco, E., Maiorana, E., &Campisi, P. “On-the-fly Finger-vein-based Biometric Recognition Using Deep Neural Networks.” IEEE Transactions on Information Forensics and Security, 2020, vol. 15, pp. 2641-2654.

[27] Li, C., Dong, S., Li, W., & Zou, K. “Finger Vein Recognition Based on Oval Parameter-dependent Convolutional Neural Networks.” Arabian Journal for Science and Engineering, 2023, pp. 1-16.
[28] Ma, H., Hu, N., & Fang, C. “The Biometric Recognition System Based on Near-infrared Finger Vein Image.” Infrared Physics & Technology, 2021, vol. 116, article 103734.
[29] Dargan, S., & Kumar, M. “A Comprehensive Survey on Biometric Recognition Systems Based on Physiological and Behavioral Modalities.” Expert Systems with Applications, 2020, vol. 143, article 113114.
[30] Zhang, Y., Li, W., Zhang, L., Ning, X., Sun, L., & Lu, Y. “Agcnn: Adaptive Gabor Convolutional Neural Networks with Receptive Fields for Vein Biometric Recognition.” Concurrency and Computation: Practice and Experience, 2022, vol. 34, article e5697.
[31] Li, S., Zhang, B., Zhao, S., & Yang, J. “Local Discriminant Coding Based Convolutional Feature Representation for Multimodal Finger Recognition.” Information Sciences, 2021, vol. 547, pp. 1170-1181.
[32] Cherrat, E., Alaoui, R., &Bouzahir, H. “Convolutional Neural Networks Approach for Multimodal Biometric Identification System Using the Fusion of Fingerprint, Finger-vein and Face Images.”PeerJ Computer Science, 2020, vol. 6, article e248.
[33] Abdullahi, S. B., Bature, Z. A., Gabralla, L. A., &Chiroma, H. “Lie Recognition with Multi-modal Spatial-temporal State Transition Patterns Based on Hybrid Convolutional Neural Network-bidirectional Long Short-term Memory.” Brain Sciences, 2023, vol. 13, p. 555.
[34] Boucherit, I., Zmirli, M. O., Hentabli, H., &Rosdi, B. A. “Finger Vein Identification Using Deeply-fused Convolutional Neural Network.” Journal of King Saud University: Computer and Information Sciences, 2022, vol. 34, pp. 646.
[35] Wu, Z., Qu, H., Zhang, H., & Yang, J. “Robust Graph Fusion and Recognition Framework for Fingerprint and Finger-vein.” IET Biometrics, 2023, vol. 12, pp. 13-24.
[36] Ren, H., Sun, L., Guo, J., & Han, C. “A Dataset and Benchmark for Multimodal Biometric Recognition Based on Fingerprint and Finger Vein.” IEEE Transactions on Information Forensics and Security, 2022.

