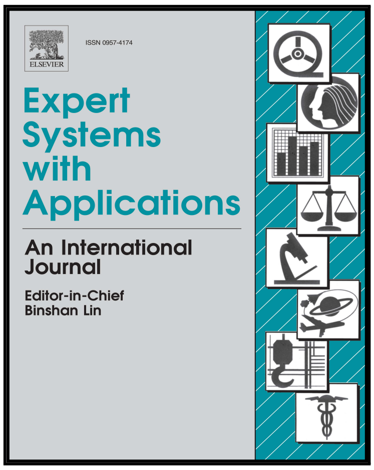
Journal Pre-proof



A Comprehensive Survey on the Biometric Recognition Systems based on Physiological and Behavioral Modalities

Shaveta Dargan , Munish Kumar

PII: S0957-4174(19)30831-0
DOI: https://doi.org/10.1016/j.eswa.2019.113114
Reference: ESWA 113114

To appear in: *Expert Systems With Applications*

Received date: 30 August 2019
Revised date: 29 November 2019
Accepted date: 30 November 2019

Please cite this article as: Shaveta Dargan , Munish Kumar , A Comprehensive Survey on the Biometric Recognition Systems based on Physiological and Behavioral Modalities, *Expert Systems With Applications* (2019), doi: https://doi.org/10.1016/j.eswa.2019.113114

A Comprehensive Survey on the Biometric Recognition Systems based on Physiological and Behavioral Modalities

SHAVETA DARGAN[1], MUNISH KUMAR[2] (Corresponding Author)

[1,2]Department of Computational Sciences, Maharaja Ranjit Singh Punjab Technical University, Bathinda, Punjab, INDIA

E-mail: shavetagnc@gmail.com[1], munishcse@gmail.com[2]

Abstract

Biometrics is the branch of science that deals with the identification and verification of an individual based on the physiological and behavioral traits. These traits or identifiers are permanent, unique and can separate one individual from another. Biometric recognition systems integrate complex definitional, technological and operational selection under various contexts. The systems are not going to replace the authentication tools and technologies, but the combination of biometric approaches and authentication methods to help in improving the security aspects of the applications where user cooperation can be inferred. Biometric based recognition methods and tools have become popular for the development of many useful, challenging and widely accepted applications such as security issues, surveillance, forensic investigations, fraudulent technologies, identity access management and access control. These systems also help to identify an individual in group of industrial networks, home/office building and control system. For the successful implementation of the biometric systems, deep artificial neural networks are in great demand. These systems can be built up either on the single modality or multiple modalities. This article explicates the comprehensive and deep survey that compactly and systematically summarizes the literature work done on unimodal and multimodal biometric systems and analyzes the feature extraction techniques, classifiers, datasets, results, efficiency and reliability of the system with high and multi-dimensional perspectives. This article also justifies in detail the classical methods, influential methods and taxonomy based on the biometric attributes. The goal is to aware the researchers of this area regarding various dimensions for the development of biometric systems to enhance the security aspects. The article begins with the fundamentals, types, need of system, challenges, uncertainties, motivations and then to the survey work. The tabular representation prepares for each biometric trait shows the author, year, major findings and results achieved with the synthesis analysis and the evaluation. The article finally ends up with the 3D biometric, a future perspective and concluding remarks.

Keywords

Biometric; Applications of biometric; Biometric traits; Feature Extraction; Classification.

1. Background and Introduction

Biometric systems are also called Identity Verification (IV) systems that refer to the art of building up authentication techniques with the help of biometric features to automatically identify, measure and validation of a living individual. Biometric system relies on the fact that every individual is different in terms of physical and behavioral aspects in various ways. Biometric identifiers are permanent, unique and separate one from another. The goal of developing such systems is to enhance the safety and security issues in the digital world. For maintaining the authentication and identification of the user for the forensics, defense, surveillance, personal identification and banking, there is a great need of biometric recognition systems. It is not easy for an impostor to identify and spoof the biometric modality of a registered person which leads to the growth and popularity of the biometric systems. To achieve robustness, high accuracy rates and difficult to spoof are the main factors that generally distinguish from the traditional methods for the security.

The general recognition systems can be categorized into two main categories such as geometric and photometric that deals with the differentiation of the features, whereas statistical approach deals with the division of an image into values and the comparison will be done with the templates. These two approaches can be categorized into two broad classes called holistic class and feature class. Holistic class identifies the entire face, whereas the feature-based class divides into low level components in accordance with the features and analyze them with respect to spatial location. Various examples based on these approaches include principal component analysis, linear discriminant analysis, hidden Markov model, elastic bunch graph matching using the Fisher face algorithm, the multi linear subspace learning using tensor representation etc.

1.1 Framework of biometric systems

Biometric recognition systems initiate with uploading the biometric pattern of an individual for the purpose of identification and then the verification of an individual. The framework for the biometric system consisting of the sequence of the various processes on which the working of biometric systems depends. The processes required are from the input of biometric traits then to pre-processing, finding the area of interest, feature extraction algorithms, designing and finally implementing matching algorithms followed by decision making process. The flow chart showing the sequence of modules is as described below in the Fig.1. After preprocessing on the input of the biometric trait or traits, the next step is to concentrate on the area of interest for applying the feature extraction methods and matching techniques. There are many feature extraction methods and classification methods that are available as per the requirement of the biometric trait and the user can develop a novel feature extraction method and the classifier for the same. So, the goal is to use either isolated classifier or hybrid classifiers with multiple feature extraction methods for improving the accurate recognition rates. Fig.1. depicting the processes in sequence that shows the working of a biometric system.

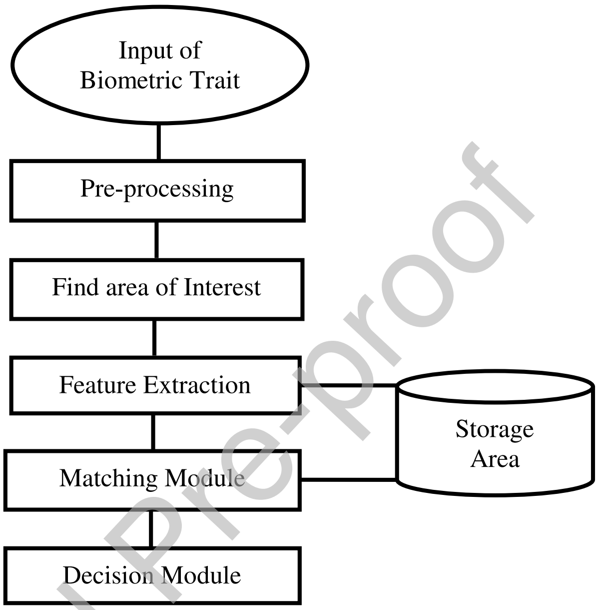


Fig. 1. General Framework of Biometric System

The biometric recognition system can be used for the forensic investigation in the following ways:

- It can be used as a tool by helping in the investigation and identifying suspects.
- It can also be used for, the evidence purpose in a court of law.
- For the forensic queries and investigations, the following requirements may arise such as
  - Speed and accuracy of biometric recognition systems, tolerable errors, effective presentations of biometric evidence having a statistical base.
  - Reliable estimation of the biometric traits concentrates on the application requirement, algorithmic details and privacy issues.
  - High computing power, effective usage of signal processing, pattern recognition and machine learning algorithms.

1.2 Biometric Trait/ Modality

Biometric trait includes the measurement of the characteristics of an individual for the unique identification and the verification. These traits are also called as modalities or identifiers and act as the foundation stone for the development of the system. These are the special attributes on which the biometric recognition system is developed. Face, palm print, iris, retina, fingerprint, voice, signature, gait, hand geometry, handwriting, ECG, brainprint and keystroke dynamics are the various examples of biometric traits which include biological, physiological and behavioral aspects. Biometric traits are of two types, called physiological and behavioral traits.

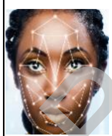
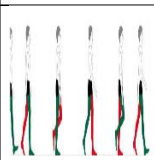
Fingerprint		Iris	
Finger Vein		Retina	
Facial		Gait	
Palm Vein		Hand Geometry	
Handwriting		Speech	

Fig. 2. Biometric Traits

- Physiological traits are the physical traits of an individual, such as fingerprint, hand and palm geometry, ear, facial pattern, deoxyribonucleic acid (DNA), retina, palm vein and finger vein authentication, voice/speech, Odor, ECG, Iris. These traits are widely accepted because of the characteristics such as collectability, uniqueness, permanence and inexpensive for achieving the verification and identification.

- Behavioral traits are the attributes describing the personality and behavior of an individual, e.g. gait, keystroke, signature, handwriting and speech.

Fig. 2. Describing the images of the various physiological and the behavioral biometric traits and the Table 1 represents various behavioral and psychological biometric traits along with the characteristics, features and the applications.

Table 1. Biometric Modalities, features, Characteristics and Applications

Nature of Biometric Modality	Important Features and Characteristics	Applications
Fingerprint	• Contemporary, Secure, Reliable, highly accurate and inexpensive • Matching Process is fast • Consumes less memory space • May create obstacles with absence, cuts, scars, dust, dirt, twists • Requires physical contact with the system	• Driver Authentication • Law Enforcement Forensics • License and Visa Authentication • Access control
Face	• Requires no physical contact • Storage of templates is easy • Convenient, less complex statistics • Identification process is fast • With time, age, accidental happenings, facial traits may change. • For the twins, differences may or may not be cleared • Lightning effects are more important • Illumination and 2D limits the clarity obstacles	• Access Control Verification • Human Computer Interaction • Criminal Identification • Surveillance
Retina	• This trait has the advantage that it cannot be forged • Very less chances of errors as no two people even twins cannot have same retina patterns • Produces high accuracy, most security, quick verification and less chance of error occurrence • Expensive to use but diseases such as cataract, hypertensions produce some error situations • Uncomfortable as it requires direct contact	• Security agencies such as FBI, CIA, and NASA

Ear	• Most stable and less computational complexity • Identification process is fast • Error generally occurs due to haircut, jewelry, hats etc.	• Law Enforcement • Forensics Surveillance.
Iris	• High scalability, accuracy and more protective • Small sample size • Speed of processing is fast but costly to use • High degree of randomness • Requires no physical contact but user cooperation • Challenges at a large distance • Diseases may affect the accuracy	• Identification as Aadhaar card in India • Access Control • National security on land, air and seaports
Hand Geometry	• More durable to use • Small size of template • Less processing • Injuries and jewels may harm the results.	• Military access control
Palm Print	• Large variety of features • High reliability and permanent • Good recognition even with low resolution scanners and cameras	• Personal Identification • Medical Diagnosis • Blood relation Identification • Selection of athletes
Lip Motion	• Different and unchangeable • Size of template is small • User interaction is not required	• Criminal Police training • Forensic Professional • Authentication transaction
Hand Vein	• Noninvasive • More accurate and difficult to forge • Unique and Unfamiliar • Affected by body temperature • Heat driver Identification System	• Door Security system • Financial systems and Banks • Login Authentication • Travel and Transportation • Hospitals, Schools and other Construction areas
Voice	• Easy implementation • Less expensive and convenient to use • Dependent on the quality of microphone and noise • Throat disease can affect the accuracy	• Web based transactions • Voice Response based health and banking systems.
Gait	• Non-invasive • Easy to capture the image	• Medical diagnose • Osteopathic and Chiropractic

	• No distance problem and convenient to use • Lack of accuracy and computationally expensive	• Comparative biomechanics
Signature	• Less false acceptance rate • More accuracy • Retrieval is easy	• Banking system

1.3 Comparison of biometric traits

Biometric traits are useful for the development of various biometric recognition systems. These are important in one sense or the other. But the choice of the biometric traits always depends upon the application, the availability of the dataset's samples, level of complexities and the value of tolerance accepted. For an ideal biometric authentication system, false error rate and false accept rate should exceed 0.1 percent. The various parameters that effects the choice of biometric trait are distinctness, permanence, collectability, performance, rate of spoofing, speed and cost efficiency of system.

Table 2. Comparison of Biometric Traits

Biometric Identifier	Universal	Distinct	Permanence	Collectability	Performance	Acceptability
Ear	H	M	H	M	M	H
Face	H	L	M	H	L	H
Fingerprint	M	H	H	M	H	M
Gait	M	L	L	H	L	H
Facial	H	H	L	H	M	H
Iris	H	H	H	M	M	L
Hand Geometry	M	M	M	H	M	M
Hand Vein	M	M	M	M	M	M
Retina	H	H	M	L	H	L
Signature	L	L	L	H	L	H
Voice	M	L	L	M	L	H
DNA	H	H	H	L	L	L

Table 2 shows the various traits against various attributes such as acceptability, performance, universal, distinct, permanence and collectability. The values such as high, low and medium represents H, L and M, respectively. E.g. for the ear biometric trait, survey reports high for universal, medium distinctness, high permanence, medium collectability, medium performance and high acceptability. Table 2 also presents the values for the other physical and behavioral biometric traits also shows the researchers that working with the biometric traits is rely a challenge in terms of attacks, security, complexities, distinctness and so on.

1.4 Persistence of the traits

Persistence of a biometric trait refers to the impact of aging and other changes in the biometric trait with the time span. The persistence affects the accuracy of a biometric system. Two types of aging are trait aging and template aging.

- Trait aging deals with the biological changes in the trait with the time span and the change is inevitable, which means it cannot be easily controlled by an individual. Changes in a person's appearance and facial structure, are the examples of biological aging that affects the accuracy rates.
- Template aging deals with the change in biometric template with the span of time. For example, if we see fingerprints and the friction ridge pattern, it varies over time due to age related and occupation related changes in the outer skin, etc. The way of extracting invariant features can also mitigate the effect of trait aging and template aging.

1.5 Attacks and Threats on biometric data

Although biometric systems have great advantages over traditional systems such as id cards and password but there are various attacks on the biometric data. Direct attacks and indirect attacks are the examples of attacks on the biometric systems. Direct attacks include the attacks on the system without the knowledge of the system such as system operation, feature extraction methods, matching algorithm used. These direct attacks are also called sensor attacks. Indirect attacks on the biometric systems require the knowledge of the inner working of the system such as an attack on the feature extraction module, the attack on the communication system, an attack on the matching module etc. These attacks are also called replay attack. Other factors include:

- Fake biometric: Fake values are fed to the sensor for fooling the system and producing the false results and these can be very easily visible from the several successful demonstrations.
- Resubmitting the pre recorded and pre stored signals: The biometric signal is pre-recorded and pre-stored in the system to perform serious attacks.
- Overriding: The original feature set is compromised and changed with the required one by an attacker.
- The template representing the biometric trait is replaced with the required one by the wish of the attacker.

- Corrupting the matching process: The matching module is altered, and the attacker generates a matching score as required.
- Compromising stored templates: An attacker uses and access the stored templates to steal these templates and spoofing the identity of the user.
- Communication interception: If the attacker interrupts, the data communicated between the matcher and the database can be altered.
- Overriding the decision: Spoofer overrides the final decision being taken by the matcher.

1.5.1. Security and Privacy Issues in Biometric

There are many privacy and security issues that are associated with the biometric technology. It is mandatory to follow such issues before using the biometric systems. As spoofing attacks are very common with the people, so control mechanism is required for ensuring the system to produce accurate results. Below mentioned are the various privacy and security issues:

- Biometric is not a hidden and a secret technology.
- Biometric traits can be trapped by a third individual very easily.
- Even the user may not know about the intelligent biometric data.
- Voice recording at the time of telephonic conversation in any event by the surveillance cameras can trace the user's voice and a user's face or gait traits.
- Biometric data cannot be changed or revoked.
- Biometric traits are permanent traits, but with exception of aging, certain incidents and biological changes.
- User can never be dissociated with the compromised data.

1.6 Characteristics of Biometric system

Biometric systems are called person identification system. It is essential and better to understand the characteristics of biometric systems in order to better understand the systems. Following are the characteristics of the biometric systems: -

- Biometric systems integrate complex technological, definitional and operational selection under various contexts.
- System level features are important and critical for the success and growth of biometric systems.
- Analysis of biometric systems in terms of trustworthiness, performance, suitability and effectiveness should be the broader perspective.

- For the specific and intended purpose, biometric systems are to be designed and evaluated and can be judged based on the underlying operational environment, technology, systems engineering and testing regimes.
- Rigorous and comprehensive methods for the systems development, evaluation, and interpretation also affect the quality and performance of the biometric system.
- Assumptions, Presumptions and overhead of the proofs shouldbe based on solid, peer-reviewed studies of the performance of biometric recognition mechanisms.

1.7 Unimodal and Multimodal Biometric System

Depending on the number of modalities used, biometric system is categorized into two types:

- **Unimodal Biometric System**: Biometric recognition system which is developed using the single modality for the identification and authentication process is called a unimodal biometric system. These systemsare capable of uniquely identifying a person, but as it is based on single identifier, these systems must face the challenges such as high security, poor recognition, less accurate results and robustness against spoofing attack as these are based on the single biometric trait. Also, the performance of the system is greatly affected by the physical and environmental factors, e.g. noisy data and small sample size. Another drawback is ineffective in the case of physically challenged persons. To overcome the issues associated with unimodal trait, multimodal biometric recognition systems are a better choice.
- **Multimodal Biometric Systems**: Multimodal biometric systems employ multiple or complementary traits, which are extracted with the help of many unique approaches. In contrast to unimodal systems, these systems are more secure from the spoofing attacks and highly reliable and robust under a dynamic environment. If we take the example of fingerprint which is considered as a very popular biometric trait for recognition and verification, the systems will face many problems such as scars, distorted images, cuts, dirty or oily images dead cells. Sometimes spoofing attacks lead to distortion of that pattern.

Differences between Unimodal and Multimodal biometric recognition systems: -

➢ Unimodal systems worked with single biometric trait and hence it is easy to develop as compared to multimodal systems, but the chances of spoofing attacks and retrieving less recognition rates are more in Unimodal systems.

- Multimodal biometric systems in contrasts with unimodal systems can fulfill challenges because they can handle problems of non-universality and can restrict imposters from spoofing biometric attributes of authentic people. The systems provide the users with the indexing and filtering of datasets, having large-scale biometric features.
- Multimodal biometric systems give the user high recognition rates, less error rates, less sensitive to the impact of the environment, increase robustness and reliability.
- Introducing authentication techniques in multimodal biometric system help these systems in their performance with less false acceptance rates and rejection rates.
- Multimodal biometric systems can out-perform single modal systems and proved best.
- Multimodal biometric systems are developed by the fusion of many modalities on the various levels, e.g. feature level, decision level and score level.
- Gad *et al.* (2015) proposed a comprehensive survey on the multimodal biometric systems and stated that multimodal biometric systems are best suited for the recognizing an individual and enhancing security standards. Multimodal systems resolve the issues and hence tradeoff related to the unimodal or single modal systems. For the successful development of a biometric system, the system must be in accordance with the specified requirements/characteristics such as availability, distinctiveness, permanence, robustness, collectability, accessibility, universality, performance, acceptability, diversity, security, performance and revocability.
- Delac and Grgic (2004) presented a survey on biometric techniques for both the unimodal and multimodal systems. They focused on the importance of biometric systems in numerous applications such as computer systems security, health and social services, credit cards, secure electronic banking system, mobile phones, secure access to buildings.

1.8 Operating Modes of Biometric System

Depending on the nature of application, biometric systems can work in two modes such as verification mode and the identification mode defined as below:

- Verification mode means verifying the identity of a person by comparing the enrolled modality with the stored one i.e. (1:1). This mode is called positive.
- Identification mode deals with the comparison of the given sample with all existing biometric templates stored in the central database, i.e. (1: M) and hence is complex to handle.
- Identification mode operates with negative recognition, i.e. searching single user from multiple identities.

- The verification mode is less expensive and more robust in terms of computation, searching and complexity as compared with identification.
- The identification mode is more convenient and less obtrusive.

1.9 Impact of Deep learning on theBiometrics system:

Deep learning approaches with stacking multiple layers of learning algorithms are mainly used in the development of the biometric systems. Biometric systems use supervised learning approach for the identification process. Deep learning is not based on any single method and approach rather it is a group of algorithms and topologies which are used to solve a variety of issues. Deep learning algorithms work on the hierarchical features and representations of the data. With the efficient optimization methods and powerful computational resources, deep learning methodologies are going to replace hand engineered approaches. But due to its scarce theories, these architectures are still ignored by the researchers. Undoubtedly deep learning has proven to be highly successful in the supervised learning and trained discriminatively to learn subtle features from the dataset. These algorithms can also handle intra class variations and noisy data. But for deep learning algorithms to handle such complexity and to segment biometric data from the noise, large amount of training data is to be required. Various architectures of deep learning that help in the development of biometric systems are Convolutional Neural Network (CNN), Deep Belief Network (DBN), Recurrent Neural Network (RNN), Long Short-Term Memory (LSTM), Gated Recurrent Unit (GRU), Deep Stacking Network (DSN). It is observed from the literature survey that for all the biometric modalities, CNN is the most commonly used architectures that helps in achieving high accuracy in the development. Important and highly simulating factors that help deep learning to use in the biometric development are: Feature learning, hierarchical representation, distributed representation, computational resources and large-scale datasets. This section shows the impact of deep learning, their features and characteristics on the development of biometric systems and in the other sections that work on the separate modalities also shows thebenefits given by the deep learning methodologies to improve the accuracy rates for the individual identification. Waisy *et al.* (2017) proposed a novel method for the multiple traits based biometric system based on the deep learning methodologies. They used deep belief networks (DBN) and RBM to extract facial features and for multi class classification and for Iris based biometric system, they used Convolutional Neural Network (CNN) and softmax classifier and achieved superior results on the FERET, CASIA 1.0 and MMU1 datasets. Qin and Wang (2019) proposed a deep learning for the development of finger vein based biometric system to extract finger vein characteristics. They used

Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) along with handcrafted techniques and used SVM for the classification purpose. The experiment performed on the public datasets and using deep learning architectures significantly improved accuracy rates. Ezeobiejesi and Bhanu (2017) presented a deep neural network-based model for the latent fingerprint image segmentation technique. They used deep artificial neural network (DANN) that uses fingerprint patches using restricted Boltzmann machine RBMfor the segmentation of fingerprint images. The first phase is unsupervised pre-training and second is fine tuning and gradient updates. The resultant model is used to classify the fingerprint images from the noise and produced accurate identification rates.

1.10 Handcrafted approaches Vs Deep learning approaches

Handcrafted approaches are used for the development of many applications of machine learning and undoubtedly boost the development process, but deep learning methodologies when added to the traditional techniques have been proving wonders. Following are some important points that can differentiate handcrafted approach vs deep learning approach:

1. Data dependency: Deep learning algorithm work well for large datasets as compared to traditional handcrafted rules and methods that fit with small datasets.
2. Hardware Dependency: Deep learning methods require high end machines to work that include GPUs and need large operations such as matrix multiplications. Handcrafted methods work with the low-end machines.
3. Feature Engineering: Deep learning incorporated feature engineering that generally put domain knowledge to the feature extractors. The idea is to reduce the complexities and more visibility of the patterns.
4. Execution Time: As deep learning methodologies believe in a few parameters and hence time to execute the problem is also more as compared to traditional methods.
5. Interpretability and problem-solving approach for both deep and handcrafted approaches.

1.11 Applications of Biometric System

There are numerous applications of biometric recognition systems. Basically, these are used for the surveillance, law enforcement, time and attendance, logic access control and physical access control. Other applications include:

- Biometric systems are used to secure the systems for the surveillance and also for the physical buildings for various applications such as access control, computer networks, verification, investigations, authentication, parenthood determination, online banking, border control, e-commerce, medical records management, security monitoring and welfare disbursement.
- For improving confidence level after the verification of authenticated individual with all rights and privileges.
- For the safe, secure, efficient and convenient working of transactions using reliable methods.
- To identify an individual and control access to information, physical spaces and services.
- Improving safety, reducing fraud and national security.
- Provides uniqueness, strong immunity and stability to forgery.

1.12 Advantages and Disadvantages of Biometric Systems

Biometric systems facilitate the users with various advantages as compared to the traditional systems in a few ways such as:

- ✓ Biometric systems facilitate with the prospect of close linked recognition of an individual.
- ✓ Successfully satisfying the security requirements in the digital world.
- ✓ Systems are used for the authentication and identification in the complex applications like banking, defense, forensics, personal identification and surveillance.
- ✓ Based on the information from the human traits, only the realization of biometric systems is possible.
- ✓ Biometric recognition techniques no doubt overcome the complexities and failures with traditional personal identification technologies, but new algorithms and solutions for the higher accuracy rates are still waiting.
- ✓ Multi biometric systems fuse multiple biometric features from two or more sources, and hence chances of success are more with less effect of spoofing.
- ✓ These systems are more reliable indicators of proving the identity than traditional methods as rely on the use of smart cards, passwords, magnetic swipe cards, personal identification numbers (PINs), keys etc are less with biometric systems.
- ✓ Less security threat and financial frauds.
- ✓ Facilitate personalization and convenience.

Disadvantages of biometric systemsinclude:

- ✓ Sensitivity of biometric data
- ✓ Security threats
- ✓ Leakage of identity information
- ✓ Direct and Indirect Attacks
- ✓ Weak feature extraction and classification algorithms
- ✓ Weak communication channel
- ✓ Due to the presence of oil, dirt, moisture, direct contact of the finger with the fingerprint-image-extracting sensor leads to lack in performance.
- ✓ in Iris/Retina recognition systems, thesmall gap between the eye and the scanner produces uncomfortable and harmful effects on the user.
- ✓ In the case of hand shape recognition, problems occur with the arthritis or rheumatism diseases that affects the accuracy of the system.
- ✓ Lack of distinctiveness, low recognition accuracy, data variation, and spoof attacks are the problems faced by the singlemodal biometric systems.
- ✓ Problem of high dimensionality leads to difficulty in the classification and makes the computational and storage requirement very complex.
- ✓ Small sample size recognition problem with biometric systems leads to satisfactory recognition performance.
- ✓ Security in case of multi-biometric templates arecomplex and crucial because of handling multiple traits.
- ✓ Privacy and security risks give unauthorized access to the system.

2. Motivations and Need for the Biometric system

Biometric systems are developed and used increasingly for the recognition of an individual and it also helps in the regulation of physical space, services, information, rights or benefits. The motivation behind the development includes increasing the convenience and efficiency of transactions, decreasing frauds, improving safety measures, and above all, the national security level.

Biometric systems are required and developed to recognize an individual distinctiveness and the achievement, which has been widely accepted. The motivation for the development of biometric systems lies in the uniqueness given by the different biometric traits. The various functional, constructive and interesting applications based on the biometric traits are another source of motivations. Major applications include security, authentication, surveillance and kind of suspects. The motivational force for the development of biometrics is the easy and repeated recognition of an individual so that automated actions can be taken based on the recognition. Another motivational aspect of the biometric systems is the tendency to achieve reduced error rates, improved accuracy, less frauds and many options for reducing costs, improving scalability, physical safety and convenience.

Previously passwords, social security numbers, names, personal identification numbers and tokens have been employed to recognize a person or to verify that individual and access its benefits or services. Passwords can be shared indiscriminately, or a physical token can be given away or lost. So, the main failure is that, a system may be confident about the right password or token for the access to sensitive services, but it cannot be sure regarding the presence of that correct individual which causes serious problems. Jain *et al.* (2016) explained in detail regarding the basics, traits, survey, challenging issues and incompleteness and the future directions of the biometric recognition systems. Authentication methods are generally based on passwords, physical key and security token. Unlike token-based systems and passwords, biometric systems work without taking active input and cooperation of the user or knowledge. Biometric systems are not the replacement of authentication and security tools and technologies but combining biometric approaches with these tools can increase the security aspects. Another important difference is of probabilistic nature, i.e. growth of the biometric systems, is based on the confidence in achieving the reliability.

3. Uncertainties and Challenges faced during the development

Biometric systems assume that an individual is different from one another based on the behavioral and physical attributes in number of ways. Selection of the attribute plays an incredible role during the development of a system. The systems are probable, and the performance of these systems are can be accessed based on the critical and fundamental characteristics. Also, during the development of biometric systems, many challenges pose obstacles and discourage the capabilities of the developer. It is very difficult if we want to replace the trait with another one once after selection. The most prominent are data integrity rules, development of datasets, feature selection and extraction methods, classifiers and the preprocessing methods. Working of sensors and a selection of matching algorithms greatly affects the accuracy rates.

Despite a few challenges and uncertainties, biometric systems are not the general replacement of the other authentication technologies but combining these two can improve the security standards and prove wonders. Below mentioned is the list of challenges and various uncertainties that one can face during the development of the biometric systems:

- Variation within persons.
- Change in age, disease, occupational factors, stress, training, intentional alterations, socio cultural aspects, environment and changes in human interface with the system will surely affect the recognition rate.
- Sensor age and calibration and the sensitivity of sensor performance.
- Selection of feature extraction and matching algorithms.
- Choice of comparison, scoring mechanisms and interaction with the sources of information also contribute to performance rates.
- Data integrity rules.
- Information may be lost and degrade through wrong data manipulations, security breaches, inappropriate compression, mismanagement or some other challenges to the development.
- Sometimes there may be vulnerabilities to attacks by the biometric system itself.
- There is a need to design the robust algorithms for representing and matching biometric patterns under unconstrained environmental conditions.
- To access and verify the feasibility, reliability and effectiveness of the system.
- Datasets collection is also very difficult and challenging task.
- Biometric data can be captured while using Internet of Things (IoT) devices without user intention and causes threat to a biometric system.
- Complexity to handle a variety of datasets.
- Selection of the methods for the feature extraction and the classification along with the risks and merits is another challenge.
- Difficult to replace biometric trait once used.
- If the biometric modality can be used by one system and failure in one lead to the strength of the other system with the same trait.
- Variability and Uncertainty in the data can affect the accuracy rates achieved.
- Several forms of biometric patternscan also be captured through a smartphone and poses risk to privacy.

- It poses great challenge to maintain the security from the Spoofers in case of unimodal systems.
- To capture multiple human traits for multimodal is itself a challenge to develop.
- Information and results affected by changes in stress, age, environment, occupational which is also a challenging task.
- Working of sensors and their sensitivity towards performance is another challenge of variability.
- Selection of matching algorithms and comparison scoring mechanisms also affects the performance.
- Control of environment and sensitivity of technologies to different environment.
- Temperature, ambient lighting level, ambient noise level and uniformity, electromagnetic field noise level, geographic location are the challenges of the biometric systems.
- Active, Passive and semi passive technologies also play a challenging role in improving the accuracy rates.
- Distinctness and persistence of biometric traits.
- Designing algorithms for controlling spoofing and obfuscation attacks also pose serious threats.
- Nguyen *et al.* (2018) presented a comprehensive survey involving super-resolution methodsunder four major biometric modalities such as iris, fingerprint, face (2D+3D) and gait traits. They used these methods by considering several different perspectives such as spatial, frequency domain, learning-based, reconstruction-based approaches, single and multiple input images. The hybrid approach of biometrics and super resolution methods helped in the deep and critical analysis of the visual databases and public databases.

4. State-of-the-art-work, Critical Evaluation and Analysis based on single modality

Biometric data is generally different from the basic personal information and the templates that are used to access personal information cannot be reverse engineered. The functioning of biometric systems will also be affected by the location, spatial relationships and shape of the nose, lips, eyes and chin. The time gap between the enrollment of the trait sample and the recognition affects the accuracy rates. The choice of modality and other factors such as age, environment, stress and some accidents affect the system design and the performance. In this section, the author is presenting the current state-of-the-art work based on either the single modality or then multiple traits and also covering considering behavioral and psychological traits. Buciu *et al.* (2016) presented a survey on the biometric systems and the technologies with the focus on the nature of modalities open issues and the problems. The performance associated with the biometric systems depends upon the external environment, operating conditions and the best results can be achieved only with the strict and controlled conditions. The survey also emphasized on the spoofing and the biometric attacks that degrade the performance of the biometric systems. Yan *et al.* (2011) presented a novel framework for feature extraction algorithm based on the quadratic projection. They formulated the quadratic matrix learning as a semi definite programming problem called dual QML for the extraction of nonlinear features and which also depends upon the Lagrange duality theory. An experiment was performed based on the face, palmprint and ear traits and proved the superiority of the dual QML based feature extraction method.

Nguyen *et al.* (2018) presented a deep survey of the super resolution methods for the four traits such as iris, face, gait and the fingerprints. They used super resolution approaches by considering various perspectives such as a single image, multiple images, spatial domains, frequency domains, reconstruction and learning based approaches. The goal is to highlight the feature domain and deep learning based super resolution approaches for improving recognition rates and the success of biometric systems. It is believed that there is a huge demand of these systems for maintaining the security, disciplined and privacy aspects and still the progress and growth have been in demand to develop accurate, precise and authenticated systems. Based on behavioral and psychological traits, various types of biometric systems are depicted in Fig. 3. The goal of this paper is to analyze and study the approaches, datasets used or developed, features extraction methods, classification methods, performance, reliability, robustness, benefits and drawbacks. The survey also covers the variety of applications with the type of biometric system. Before going through the literature survey, the necessary fundamentals, merits, demerits, diagrams representing the process are also represented with every modality.

4.1. Fingerprint based Biometric recognition System

The fingerprint is the most widely used and well researched biometric trait. In view of the information security, fingerprint biometric trait attained great popularity with the success in granting and denial of permit, user authentication and access control privileges to system and data resources. Attendance systems, border cross control, door access control and financial security are the important applications of the biometric systems. The choice of modality and other factors such as age, environment, stress and some accidents affect the system design and the performance. Fingerprint identification system consists of three phases:

- Image Acquisition and Processing
- Feature Extraction
- Pattern Recognition.

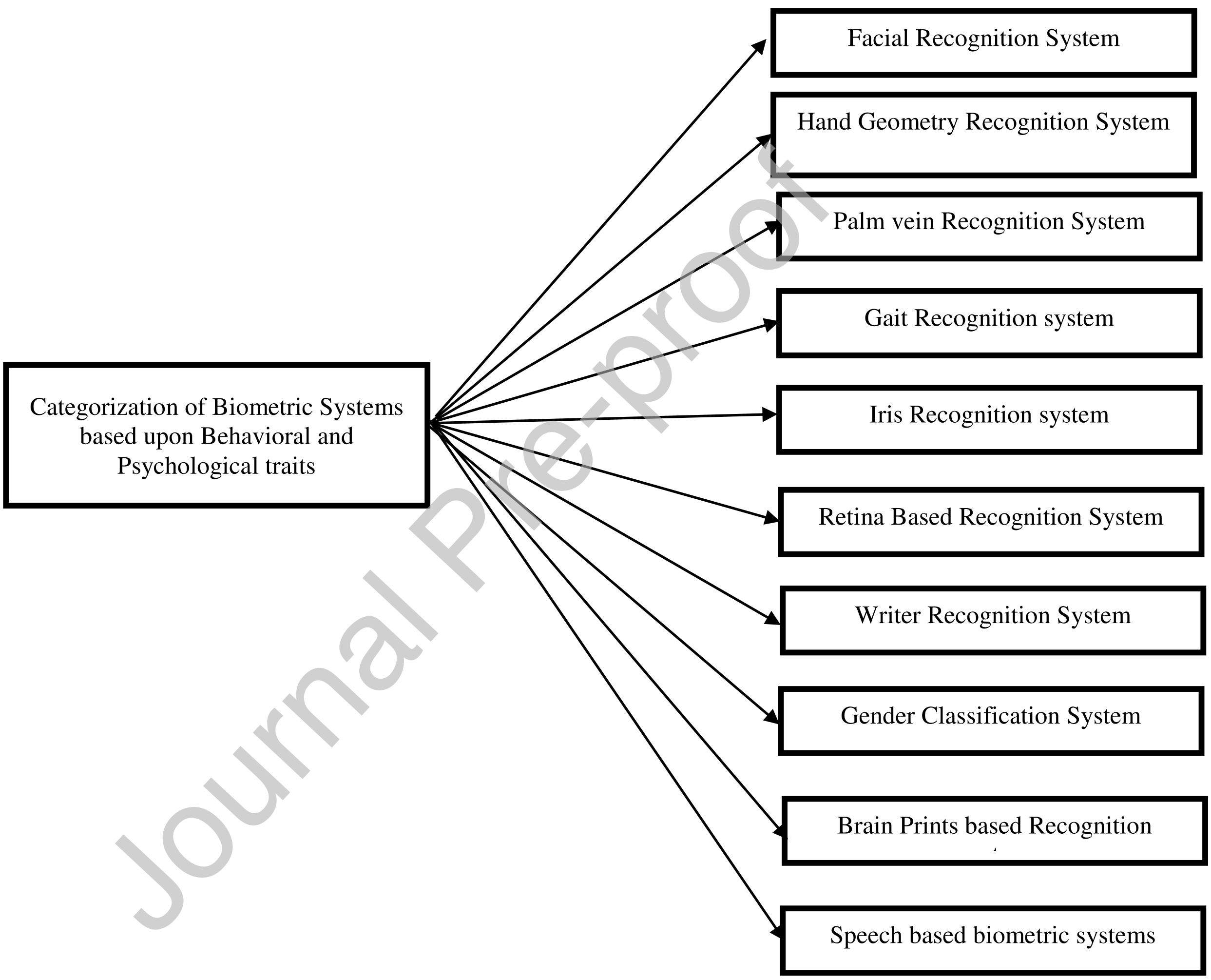


Fig. 3. Types of Biometric Systems

Fingerprint images are captured with the help of an optical fingerprint reader (OFR). The scanner matches the samples of the ridge and valley of a given image with the database and hence performs the required identification. Lin *et al.* (2011) presented that the advantage with fingerprint biometric trait is that the attribute is not guessed as the passwords, cannot be forgotten and misplaced. But the drawback is that the fingerprints are easily exposed to others as compared to finger vein and exhibit some excellent advantages. The ways of spoofing the fingerprint data, such as: -

- Fingerprint of a person can be easily taken from a mobile phone or any other surface.
- Lifted fingerprint image can be employed to make a dummy finger.
- The dummy finger can be uploaded on the sensor to claim the identity.

Process of fingerprint identification: Below is the Fig. 4 that shows the process of fingerprint identification with binary outcomes.

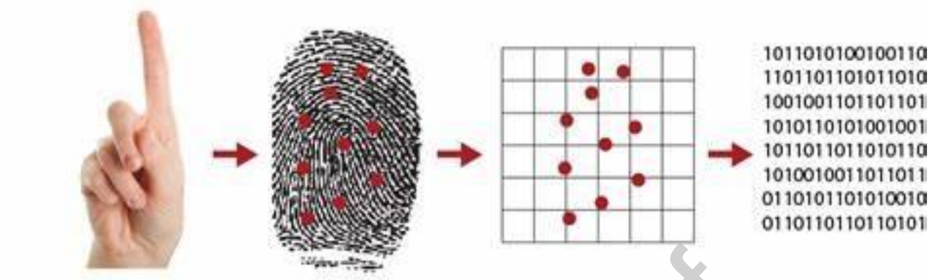


Fig.4. Fingerprint biometric recognition system

4.1.1. Finger Vein based Biometric Recognition System

Finger Vein based biometric system is more robust than fingerprint-based systems because the spoofing with finger-veins are difficult as the finger-vein is not visible, is embedded inside the finger and only captured by an infrared sensor. Also finger vein biometrics positively not leaving any traces behind, so the finger-vein biometrics is highly resilient to spoofing. The fingerprint and finger-vein based multi-biometric system holds richer and more discriminative information than unimodal biometric systems based on either fingerprint or finger vein and therefore hence recognition performance is greatly improved, enhance system security and reliability.

4.1.2. Study of Finger Vein pattern

Qiu *et al.* (2016) mentioned that the finger vein pattern is present in between the roots of the five fingers and the wrist of the palm-dorsum and under the skin surface. This biometric trait is stable and can only be identified with a live body. It is hard to be forged or stolen and safe because the vein is hidden in the skin surface. Vein pattern biometrics mainly include dorsal hand vein, palm vein and finger vein. If we compare all three patterns, then dorsal hand vein is more distinctly visible and the only few vein minutiae can be found on the dorsal hand. With the finger vein recognition, enough vein information can be easily obtained by using multiple fingers. The device used to capture the finger vein pattern has small volume and best suited for real application such as mobile applications. Fig. 5. shows the process of finger vein identification.

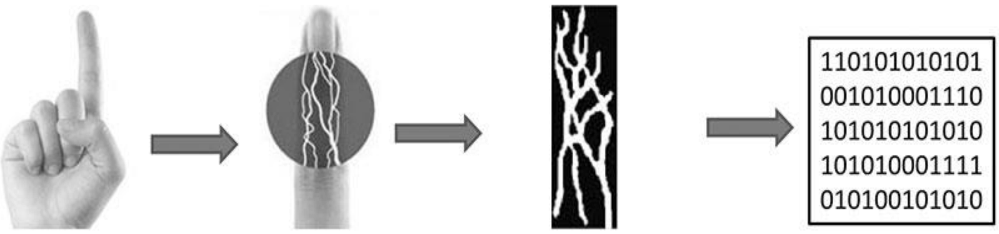


Fig.5. Finger Vein Biometric Process

4.1.3. Stages for Finger vein Identification System

A finger vein recognition system consisting of two main stages named enrollment stage and verification stage as reported by Yang *et al*. (2018). On the enrollment stage firstly finger vein images are taken and then the image processing methods are applied for enhancing the quality of vein images. After getting the enhanced and improved vein images, feature extraction methods are employed for extracting the features and then stored as the templates. For the verification stage, finger vein sample of the user is taken for the testing followed by the image preprocessing method and feature extraction methods. At last we got the verification result by comparing the results of testing feature and stored templates.

4.1.4. Reported work on fingerprint and finger vein biometric identifiers:

Lin *et al.* (2011) proposed a fractal pattern classifier for the fingerprint recognition based on the Grey Relational Analysis (GRA). By using an optical fingerprint reader, fingerprint images were taken. For refining noise, image enhancement, conversions to binary image and location of reference point, digital image preprocessing technique is used for the estimation of Fractal Dimension (FD) for the 2D binary image, they used Katz's algorithm and Weierstrass Cosine Function (WCF) for extracting biometric characteristics. Thisnovel research exhibitedgreater efficiency and higher accuracy. Yang *et al.* (2018) presented a novel approach for biometric system based on the fingerprint and finger vein patterns that will provide template protection and revocability. The multi biometric system was based on the minutia-based fingerprint features and image-based finger vein features and the feature level fusion options were used for improving the security strength. Their proposal of Enhanced Partial – Discrete Cosine Transform (EP-DFT) was based upon non-invertible transformation that provides the usersystem security strength and substantial improvement.

Xi *et al.* (2016) proposed a framework for the biometric system on the finger vein modality. They presented a novel learning method which is called discriminative binary code (DBC). The method involved the construction of subject relation graph followed by the transformation of binary templates to represent the vein characteristics. With the help of supervised information and SVM, it was observed that DBC were more discriminating and shorter. For the experiment, PolyU database and MLA database were selected and achieved effective and efficient results. Wang *et al.* (2016) presented a reliable and efficient framework for the fingerprint recognition mainly for the resource limited applications. This was based on the partial hadamard transform method for the designing of cancelable fingerprint templates. This approach was based on the cancelable fingerprint templates and stochastic distance preservation that provide revocability, diversity, non-invertibility and performance and proved favorable as compared with state-of-art work.

Asaari *et al.* (2014) proposed a new approach based on the finger based biometric system using a fusion of finger vein and finger geometry pattern. They employed Band Limited Phase Only Correlation (BLPOC) which was occlusions, resilient to noise and rescaling factors. The method was based on the Width Centroid Contour Distance (WCCD), a kind of geometrical feature that combines the width of the finger with Centroid Contour Distance (CCD) and improved the accuracy of finger geometry recognition. The method was based on the integration of finger vein and finger geometry recognitions by a score-level fusion method plus weighted SUM rule that worked on the dataset of 123 volunteers resulted in the 77% recognition accuracy and the equal error rate (EER) was 1.78% with a total processing time of 24.22 ms. Escobar *et al.* (2015) proposed a novel fingerprint-based recognition system and protection scheme that depends upon the chaotic encryption by using Murillo-Escobar's algorithm and the logistic map. They used 32-bit micro controller for secure authentication systems and embedded expert systems and presented a complete security analysis at both the implementation and statistical level. Applications include the real secure access control systems in banks, offices, factories, universities, homes, hospitals, personal systems, e-commerce, cellphones and others.

Pakutharivu and Srinath (2015) presented a comprehensive survey on the fingerprint recognition system with many applications such as terrorist identification, criminal investigation and other security aspects of the successful implementation of fingerprint biometric system, a good quality fingerprint image is required. The authors performed a deep and detailed survey on the fingerprint recognition systems and focused on the image enhancement techniques to achieve good accuracy rates. Qiu *et al.* (2016) proposed a new method for the fingervein biometric recognition system based on the pseudo elliptical transformer and dual sliding window localization. Here, planar imaging and dual sliding window helped in the capturing of the finger vein images and accurately detecting the position of the finger veins. Pseudo Elliptical sampling was used to retain the spatial distributions of vein patterns and for eliminating the redundant information. The experiment was implemented on three different dataset such as SDUMLA HMT, FVUSM and THU FVFDT3 and got effective, reliable and improved results as compared to the state-of-the-art work. Yoo *et al.* (2015) presented a framework based on the face biometric recognition system in which Active Shape Model (ASM) and Principal Component Analysis (PCA) methods were used and a CCD (Charge Coupled Device) camera was employed to capture a facial pattern. They used AdaBoost and Histogram Equalization (HE) for improving the quality of the image. For the classification, Radial Basis Function Neural Network performed the identification. All the essential parameters for the design of the network such as learning rate, fuzzification coefficient and momentum coefficient used by the FCM are evaluated and optimized by using Differential Evolution (DE) and produced promising output and accuracy rates.

4.1.5. Summary of the survey work:

The below Table 3 represents the summarized findings and the results with the name of the author and the year to have the quick view on the researches completed.

Table 3. Major Findings and Results of Fingerprint/FingerVein Biometric Systems

Author/s	**Year**	**Major Findings**	**Results**
Lin *et al.*	2011	➢ Fractal Pattern Classification methods ➢ Grey relational Analysis ➢ Kat'z algorithm for fractal dimensions ➢ Weierstrass Cosine Fnction (WCF)	➢ Greater efficiency and higher accuracy
Yang *et al.*	2018	➢ Fingerprint and finger-vein based cancelable multi-biometric ➢ Feature-level fusion strategy ➢ Partial – Discrete cosine transform based on non-invertible transformation	➢ Template protection and revocability ➢ Substantial improvement over the original P-DFT
Xi *et al.*	2016	➢ Discriminative Binary Codes (DBC) ➢ Subject Relation Graph ➢ Relational graph is formed ➢ Binary templates are created ➢ PolyU database and MLA database ➢ SVMs are trained	➢ DBC are more discriminative and shorter ➢ Effective and efficient results
Wang *et al.*	2016	➢ Partial hadamard transform ➢ Stochastic distance preservation ➢ Cancelable fingerprint templates	➢ Revocability, diversity, non-invertibility and performance and proved favorable

			➢ Highly reliable, efficient
Asaari*et al.*	2014	➢ Fusion of finger geometry and finger vein recognition ➢ Band Limited Phase Only Correlation (BLPOC) ➢ Width Centroid Contour Distance (WCCD) ➢ Scorelevel fusion method	➢ Resilient to noise, occlusions and rescaling factors ➢ Centroid Contour Distance (CCD) ➢ improve the accuracy by 77% ➢ EER was 1.78%
Escobar *et al.*	2015	➢ Chaotic encryption ➢ Murillo-Escobar's andLogistic map algorithm	➢ Secure, effective and at low cost ➢ Real secure access control systems ➢ Embedded expert systems

4.2. Facial Recognition System

The human face is anotherimportant biometric trait that is used in a wide variety of applications, i.e. criminal identification, security system, forensics, surveillance systems and credit card verification, etc. Nguyen *et al.* (2018) described in the introduction that face is a passive biometric and face images are usedfor the effective development with or without the interaction of the person. The facial recognition system is a biometric artificial intelligence system that performs the identification by analyzing patterns from the person's facial textures and shape. In face biometrics, mainly visible imagery is used that is not affected by temperature and goggles. The following sections shows the advantages, disadvantages and the applications of the facial recognition system.

4.2.1. Advantages of the facial recognition system

- Due to its contactless and non-invasive process, this technology is widely adopted, but as compared to iris recognition and fingerprint recognition, the accuracy achieved is generally less.
- Help in the mass identification.
- Used in airports, multiplexes, and other public places for the identification of an individual with or without awareness.
- Quality measures are more important in facial recognition system.
- Yadav *et al.* (2018) also showed that the expressions, Illumination, pose and noise affects the performance and hence the recognition rates.
- Facial recognition givesthe highest false acceptance and rejection rates.

- Railway and airport security are the useful applications.

4.2.2. Disadvantages of the facial recognition system

- Face recognition is less effective with the variations in the facial expressions, even with the big smile.
- Inconsistency in the datasets also affects the performance.
- Data privacy is the main concern.
- Facial data stores can be easily accessed by anyone if not stored properly or hacked.

4.2.3. Applications

- Commercial Identification and Marketing Tool
- National Security
- Mobile Platforms Social Media
- Video Surveillance
- Automatic Indexing of Images and Video Database
- Advanced Human-Computer Interaction

4.2.4. Techniques for Developing the Facial Recognition System: Following are some helpful techniques for the development of facial features based biometric system as presented by Jalali *et al.* (2017).

- Extracting features or landmarks, from the subject pattern followed by the implementation of algorithm that can analyze the shape of the eyes, nose, cheek bones, relative position, size and jaw.
- Normalization and the compression on the face images help in the face recognition.
- 3-Dimensional face recognition uses 3D sensors to retrieve the nose, chin and contour of the eye sockets from a range of viewing angles.
- Three-dimensional data can improve the precision of face recognition.
- Skin texture analysis gives the visual details of the skin such as unique lines, patterns, and spots into a mathematical space.
- Surface Texture Analysis deals with taking a picture of a patch of skin, followed by the algorithm for converting the patch into a mathematical and measurable space to distinguish lines, pores and the actual skin texture.

4.2.5. Anti-Facial Recognition System

- In 2013 Japanese researchers created privacy visor glasses which are based on the infrared light to fail the face recognition software in which titanium and light reflective frame and a mask received patterns and angles to interrupt the system by both absorbing and then bouncing back light sources.
- Chicago in 2016 developed sunglasses and anti-CCTV called reflectacles were developed that reflect infrared, visible light to make the face a white image.
- Different styles of haircuts and make-up patterns are also available that creates difficulty in recognizing the patterns.

4.2.6. Reported work on Facial Recognition System

Mamta and Hanmandhu (2014) presented a novel framework for face based biometric system by employing four feature extraction methods and two classifiers. The four methods were the effective multi quadratic information source (EMQDI) and the inverse of this feature (EIMQDI), effective Gaussian information source (EGI), effective exponential information source (EEI). Two classifiers called the Hanman classifier and the weighted Hanman classifier were applied to the results of feature extraction methods applied to the self-generated datasets with the unconstrained conditions such as less resolution, occlusion and noise and retrieved excellent results. Jalali *et al.* (2017) presented facial based biometric system by using a novel cost function with Convolutional Neural Network (CNN). This novel approach had a sensitive part, which includes the conventional error divided by the derivation of the activation function and the total error was reduced by the gradient descent method. For the detailed study the data samples were taken from both the nightand daytime facial traits. Neural network structures for measuring the small variations and high frequency components were used. The presented method of cost function with Convolutional Neural Network structures performed better and produced internal representation, general exploitation and better face recognition. Nguyen *et al.* (2018) performed a detailed survey on the super resolution of the biometric recognition systems. They showed the effect of super resolution on the vision and clarity of the biometric systems. Their survey was based on the four traits such as face, iris, fingerprint and gate keeping into consideration spatial domain, frequency domain, a reconstruction based, learning based and single and multiple input images. The goal was to facilitate the researchers of the biometrics in enhancing their knowledge, improving quality and the performance level achieved by the biometric system. It also helped to handle the complex issues such as super resolution for biometrics.

Anees *et al.* (2017) proposed a novel, robust and stable framework for generating the enrollment and cryptography keys based on the facial features without saving the facial features in the database. The framework consisted of three sections i.e. learning the facial features, followed by the quantization part and then the key generation. Linear Binary Pattern was used in the standard face databases and secondly for resolving the variations and reducing the feature size, Quantization schemes were also used. The robustness of the keys was evaluated on a set of statistical tests and the experiment released promising results. Also, the framework can be used for the multimodal biometric system to generate even more secure keys but with handling more computational complexity. Riera *et al.* (2017) presented a new method for a facial recognition system based on the facial marks using Histograms of Oriented Gradients (HoG) descriptor with self-generated corpus and manual annotations. The objectiveof this study was to use these marks for (1) improving the identification accuracy (2) reducing the search space for the fast retrieval of the patterns (3) to extract partial or off-frontal facial patterns. The proposed method based on HoG descriptor was efficient in performing very fast calculations by using a new public dataset for facial marker detection. Perumal *et al.* (2016) presented a new framework for the biometric recognition system based on the facial marks in which they used local dimensionality pattern with reduced dimensionality. This novel proposed descriptor restructured the patterns by changing the LDP coding pattern constraints. The advantage of DR-LDP was to generate compact code for efficient face recognition. The experiment was done on the datasets like FERET, extended YALE-B database and ORL and achieved a better recognition rate and proved the efficiency and accuracy rates.

Kas *et al.* (2018) presented a unique approach for the development of feature descriptor named Mixed Neighborhood Topology Cross Decoded Patterns (MNTCDP) which can be merged in different platforms and produce robust, computationally low and simple solutions. MNTCDP depends on the pattern encoding scheme and neighborhood topology used to extract the stable and a discriminative face representation. Through face alignment and detection, supervised image classification, K-Nearest Neighbor classifier, higher accuracy rates can be achieved. An experiment was conducted on the YALE, ORL, FERET and AR datasets with different illumination conditions and concluded that the proposed MNTCDP descriptor presents high performance. Yaddaden *et al.* (2018) presented an efficient facial based recognition system based on Convolutional Neural Network architecture in which they placed radio frequency identification tags with an error detection module. The experiment was executed on the five benchmark facial expression datasets and achieved promising results higher than 95% and providethe consistent improved results with false positive detection rate reduced by 20%.

Yadav *et al.* (2018) proposed a novel, advanced and efficient framework motivated from the interval type-II fuzzy membership in combination withthe kernel based sparse method. They measured the participation of pixels using Interval type-II fuzzy logic i.e. extended interval type-II membership function. Usingthe *K* nearest neighbor and Euclidean distance metric for sparse representation, the experimental analysis revealed an improvement in the accuracy from 2-10% higher than the state-of-the-art work. Jun and Kim (2012) presented a unique concept for the development of biometric system based on the face trait. They used local gradient patterns (LGP) in which each bit LGP is assigned the value one if the neighboring gradient of a pixel is greater than the average of eight neighboring gradients and 0 otherwise. LGP are insensitive to global intensity variations and has higher discriminating power than LBP and leads to a reduction in the false positive detection error. By working on the MITCMU and FDDB databases, the proposed method provided a face detection rate that is 5 to 27% better than state-of-the-art work with the least number of false positive. Yua *et al.* (2017) presented a framework based on the discriminative multi-scale sparse coding (DMSC) that used to learn dictionary to handle the occlusion variations and proved sparse, robust and highly discriminative coding and revealed great accuracyin comparison with the state-of-the-art work.

Ramaiah *et al*. (2015) presented a novel approach to the face biometric system using D-CNN that focus on the extraction of the local pattern occurred in the datasets. The symmetry of facial information used to enhance the performance level by taking the horizontal reflections of the facial images. The experiment yields improved results with deep CNN. Ozbulak *et al*. (2016) presented a model for the age and gender estimation and classification based on the deep CNN. They used ALexNet structure along with D-CNN and GilNet CNN that worked with the Adience dataset and reported 5% to 7% increase in the age and gender estimation rates. Zhu *et al.* (2016) presented a unique face detection and analysis method using contextual multi-scale, region based-convolution neural network (CMS-RCNN). The approach is based on the region proposal component and region of interest detection method that worked with tiny face areas and body contextual reasoning in the network on the WIDER FACE Dataset and Face Detection Dataset and Benchmark (FDDB) and reported promising results. Raghavendra *et al.* (2017) presented facial modality based biometric system using deep convolutional neural network (D-CNN) for both digital and printed morphoged facial features. The approach is based on the feature level fusion of layers of VGG19 and AlexNet D-CNN and on the newly constructed database that proved improved detection performance. Table 4 describes the major findings with face biometric system.

Table 4. Major Findings and Results of Face Biometric Systems

Author/s	Year	Major Findings	Results
Mamta and Hanmandhu	2014	• Exponential information source • Gaussian information source • Multi quadratic information source • Hanman Classifier	• Worked under Occlusion, less resolution and noise • Proved excellent results.
Jalali *et al.*	2017	• Sensitive CNN • Gradient descent Method • Quality degraded LDHF images	• Algorithm more sensitive to small intensity changes
Nguyen *et al.*	2018	• Affect of super resolution on the biometric system • Based on four traits iris, face, fingerprint and gait • Frequency domain, spatial domain, reconstruction domain	• Comprehensive and Systematic survey
Aneees *et al.*	2017	• Generating the enrollment and cryptography keys • Learning the facial features, Quantization and key generation • Linear Binary Pattern • Statistical test	• Promising results • Generate more secure keys • More computational Complexity
Riera *et al.*	2017	• Histograms of Oriented Gradients (HoG) descriptor • Soft biometric trait e.g. gender, ethnicity and facial marks	• Improve the identification accuracy • Fast Calculations • Extract partial or off-frontal facial patterns. The proposed method based on HoG
Kas *et al.*	2018	• Neighborhood topology and pattern encoding scheme • Mixed Neighborhood Topology Cross Decoded Patterns (MNTCDP) • ORL, YALE, AR datasets	• High performance ability in classifying face images. • Computationally and conceptually and simple yet efficient descriptor
Yaddaden *et al.*	2018	• Convolutional Neural Network • Five benchmark facial expression datasets • Radio frequency identification tags (RFIT)	• Promising results higher than 95% • False positive detection rate reduced by 20%
Yadav *et al.*	2018	• Interval type-II fuzzy membership • kernel based sparse representation	• Classification accuracy to 2-10% higher than the

		• K-Nearest Neighbor	other existing relevant methods
Jun and Kim	2012	• Local gradient patterns • MITCMU and FDDB databases • Face detection 5–27% better than state of the art	• False Positive detection error is reduced
Yua *et al.*	2017	• Discriminative multi-scale sparse coding (DMSC) model • Ultra scale error measurements	• Robust, sparse and highly discriminative coding

4.3. Palm vein

Palm vein pattern recognition is also an exciting concept for the biometric recognition. It is widely accepted and used by many reliable and robust personal identification authentication approaches. It is not easy to discernible the vein structure of the palm asit can vary with the factors such as the age, humidity, temperature, levels of fat and physical activity. Also scars, pigmentation and palm position can also affect the image acquisition. Palm vein structure can be shown in the Fig. 6.

Fig. 6. Palm Vein Biometric Images

Han and Lee (2012) used the palm vein as biometric trait and used texture-based feature extraction technique for the palm vein authentication. A Gabor filter can be used to produce the optimized resolution for the frequency and spatial domains and will be used to extract local features for the palm vein recognition. Here, Vein Code based on the bit string produces template matching and the normalized Hamming distance can be used to detect and measure the similarity of two Vein Code. Dataset consisting of 4140 palm vein images from 207 persons has been developed and that achieved high accuracy rates with enough speed. Su (2009) proposed palm print biometric recognition system in which the characteristic matrix was employed to develop various discriminators for identifying different palm-prints. The image rotation problem can be handled by the ring rotation invariant transformation method. The experiment was implemented by the transformation signals which are fed to the characteristic matrix. Image-shifting complexities weresolved by comparing one pixel in the sample image with the surrounding pixels in unknown image and provide better results as compared with other the state-of-the-art work.

Chevtchenko (2017) presented a new approach for developing biometric system that depends upon the static hand gesture in which they used benchmark dataset including 36 gestures. The dataset contains variations such as illumination, scale and rotation. Gabor features, Fourier, Zernike moments, Hu moments, Pseudo-Zernike moments and complex moments are compared keeping in view the accuracy and speed dimensions. They achieved high accuracy rates with less computational cost. Features extraction algorithms and neural network such as ANN, MLP wasimproved by a multi-objective evolutionary algorithm.

Bingol and Ekinci (2017) proposed a novel method for biometric recognition system based on the palm print. The binocular stereo fusion approach was used to extract the depth information. Firstly, the hand orientation was estimated by building a surface model associated with the eigen vectors of the depth details and based on the relationship, pose correction was done that help in perspective distortion. Next, using segmentation through the Active Appearance Model (AAM), region of interest was calculated. At last the palmprint features were extracted based on the Gabor Kernel Fisher Discriminant Analysis. Dataset of 138 individuals was taken. And they got less EER values from around 14% to 0.75% and the improved recognition results to 97.01%. Su (2009) proposed a framework for the recognition based on the palm extraction in which each user's hand was observed in three distinct ways of photographing. By adjusting different illuminations for each hand image, they still got several problems with respect to the hand images, e.g. by sticking together the middle finger and ring finger and by stretching the thumb and the index fingers, they prevented the task of extracting the thumb, middle, and ring fingers and assist the functioning of the algorithm. Thus, from 40 persons, total 120 photographs were selected and then the experiment proceeds with (1) location of hand-edge (2) fingers truncate (3) geometry description (4) Shift and rotate the image (5) genuine comparisons are conducted. It can be concluded that the error rate was below 3%. Table 5 describes the major findings with palm vein biometric system.

Table 5. Major Findings and Results of Palm Vein Biometric System

Author/s	Year	Major Findings	Results
Han and Lee	2012	• Texture-based features extraction methods • A Gabor filter generates optimized resolution for the spatial and frequency domains • Best parameter values of a single Gabor filter	• High accuracy

		• VeinCodes can be detected and measured by normalized Hamming distance • Dataset contains 4140 palm vein images	
Su	2009	• Characteristic matrix • Ring rotation invariant transform • Worked with discriminators • Pixel to pixel comparison	• Better results as compared to the state of the art work
Chevtchenko	2017	• Static hand gesture • Gabor features, Fourier, Zernike moments, Pseudo-Zernike moments, Hu moments, complex moments • Used ANN and MLP	• High accuracy with less computational cost
Bingol*et al.*	2017	• Binocular stereo fusion approach • Surface model associated with the eigen vectors • Segmentation through the Active Appearance Model (AAM) • Gabor Kernel Fisher Discriminant Analysis. • Dataset of 138 individuals	• Recognition results to 97.01%. • Less EER values from around 14% to 0.75%
Su	2009	• Dataset of 40 person • Location of hand-edge • fingers truncate • Geometry description • Shift and rotate the image • Genuine comparisons are conducted	• Error rate was below 3%.

4.4. Hand Geometry

The hand is considered as a deformable object with large degrees of freedom (DOF) that creates difficulty in the recognition. Hand gestures provide virtual reality environments, content-based image and image/video coding, video retrieval and video games. Good recognition accuracy rates can be achieved with hand geometry and with simplicity, low-cost and speed high user acceptance. Gesture recognition and hand geometry is an interesting and challenging task of seeing the increased human–computer interactions. It is used for the biometric recognition system because during interaction with the devices hand gestures give the patterns as biometric. Hand gesture is helpful for the development and security of the vehicle infotainment systems, smart houses, games, kitchens and operating theaters.

Guo *et al.* (2012) presented a novel framework for the biometric recognition system based on the hand geometrical features by employing the infrared illumination device on which users put their hands without any template in front of the camera. This proposed system detected total 13 points from each palm image and extracted 34 features and worked under dark environmental conditions and complex backgrounds with a database of 6000 images. The experiment generated mean false Acceptance rate (FAR) was 1.85% and the correct identification rate (CIR) of 96.23%. Chevtchenko *et al.* (2017) developed a new method for personal identification based on the static hand gestures by taking benchmark dataset containing gestures and having variations in scale, rotation and illumination. For the feature extraction and classification, the image descriptors such as Pseudo-Zernike moments, Complex moments, Zernike moments, Fourier, Hu moments and Gabor features are compared and used Multilayer Perceptron (MLP). Both, the classifier and the feature vector are adjusted with multi-objective evolutionary algorithm based on NSGA-II and achieved high accuracy rates with less computational cost. Huang *et al.* (2011) developed a novel method for hand gesture based biometric system based on the Gabor filters and support vector machine with high robustness against variations in illumination. They useda skin color model switching method and the insensitiveness to hand-pose flexibilities and gave permission to the users to wear long or shortsleeve shirt. The experiment successfully achieved an accuracy of 96.1%. Pacheco *et al.* (2012) proposed a novel paradigm that employed an agent-based scenario that takes context information for taking decisions. The two agents called primitive agents and combined agents performed syntactic and semantic recognitions. They did not need operation modes; this implies that no button was required to separate geometry and gestures. The experiment successfully achieved an accuracy rate of 96.41% with dataset of 2500 symbols. Tsai and Lee (2011) presented a new biometric system based on hand gesture that combined the back propagation neural network and the VICON. They compared the hidden layer neurons with the other layers to improve the system performance. They stated that very less or very large neurons affect the accuracy rates and showed the importance of the hidden layer. The training epoch size affect in the accuracy of the system with over fitting of the training set and impair of the training set with very large and very small size respectively. Dutta (2009) presented a biometric system based upon the hand shape. Because of its simplicity and high acceptance by the public and non-intrusiveness, the biometric widely accepted its growth. The paper also presented a survey of all the necessary aspects for the development of hand shape recognition systems by reviewing all the modules with the algorithms. They also discussed system taxonomies, performance evaluation methodologies, testing issues and their impact on the accuracy results. Li *et al.* (2017) presented a framework based on the user interaction with mobile phones for the hand gesture recognition. They designed a deep architecture by integrating Bidirectional Long-Short Term Memory (BiLSTM) and Bidirectional Gated Recurrent Unit (BiGRU) with Fisher criterion, termed as F-BiLSTM and F-BiGRU, respectively. By analyzing the acceleration and angular velocity the fisher discriminative models can classify the gestures. For the experiment, they used a large Mobile Gesture Dataset (MGD) consisting of 5547 sequences of 12 gestures and attain superior performance as compared to the literature review. Table 6 shows the summarized findings of the hand geometry based biometric system.

Table 6. Major Findings and Results of HandGeometry Biometric Systems

Author/s	Year	Major Findings	Results
Guo *et al.*	2012	➢ Hand geometrical features ➢ Infrared illumination device ➢ Dark environmental condition and complex backgrounds with database of 6000 images ➢ 13 points from each palm image ➢ Extracted 34 features	➢ Correct identification rate (CIR) to about 96.23% ➢ Mean False Acceptance rate (FAR) was 1.85%.
Chevtchenko *et al.*	2017	➢ Gestures and having variations in scale, rotation and illumination ➢ Multi-objective evolutionary algorithm ➢ Fourier, pseudo-Zernike moments, Zernike moments and complex moments, Hu moments and Gabor features ➢ MLP	➢ Higher accuracy rates with minimum computational cost
Huang *et al.*	2011	➢ Hand gesture identification using Gabor filters ➢ Support Vector Machine ➢ Skin color model and switching method ➢ insensitiveness to hand pose variations	➢ Achieved accuracy of 96.1%.

Pacheco *et al.*	2012	➢ Worked with Primitive agents and Combined Agents ➢ Syntactic and semantic recognitions	➢ Achieved accuracy rate of 96.41% with dataset of 2500 symbols
Tsai and Lee	2011	➢ Hand gesture that uses back propagation neural network ➢ Compared layers with hidden layer neurons ➢ Training epoch size also affects the accuracy of the system	➢ Produced better results
Li *et al.*	2017	➢ Bidirectional Gated Recurrent Unit (BiGRU) ➢ Bidirectional Long-Short Term Memory (BiLSTM) network with F-BiLSTM and F-BiGRU ➢ Mobile Gesture Dataset (MGD) consisting of 5547 sequences of 12 gestures	➢ Superior performance

4.5. Iris

Biometric traits such as Iris is complex, but the patterns have rich, wonderful texture and having complex structure and as compared to fingerprint and face, it is better because iris have been always unique even for twins and it is protected from eyelid, cornea and humor. The structure of iris remains constant and stable throughout the life and serves as a good biometric trait for biometric recognition. The advantage of using iris for biometric recognition involves less margin of errors and fast speed and immune to the contact lenses and aging. These patterns are very rarely affected by the environment and hardly lost and believed that the trait revealed best, efficient and accurate results in the recognition process.

Fig. 7. View of Iris Biometric System

The approach is convenient to use, accepted by millions of the people and very hard to forge. It is widely used for the authentication programs such as national ID and passport less border crossing. For the iris recognition, high resolution pattern identification techniques and distortion free images are required.

Block Diagram of Iris Recognition System: Fig. 8 of iris recognition consists of the processessuch as image acquisition, segmentation, normalization, feature extraction and matching. The iris recognition process can be achieved in three distinct steps:

- Image capture**:** This step involves capturing the image of the iris either manually or automatically. The constraint here is to have a proper clarity and focus of the image.

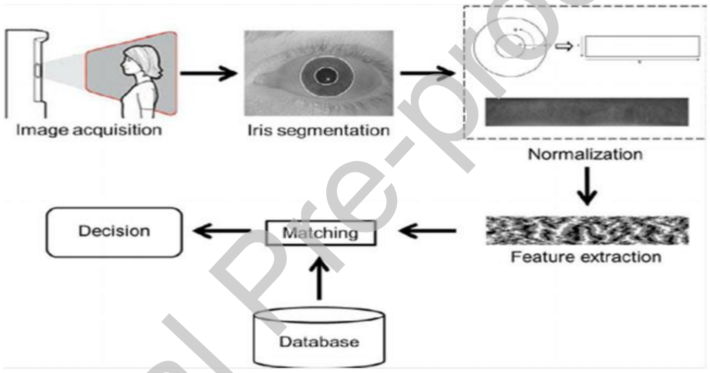


Fig. 8 Iris Recognition Process

- To find the location of the iris and then optimizing the image: After verifying the focus and the clarity, it is necessary to identify the boundary followed by the center of the circular iris. And then to analyze the area suitable for features retrieval and analysis. The next step is to remove deep shadows and the portion which is covered through reflective areas and eyelids. The optimized area is normalized in a rectangular block to have fixed dimensions. Features are then extracted using Dugman’s rubber sheet method.
- Biometric template accumulation and matching: Biometric template and the encoded structural feature are stored in the dataset during the enrollment of a user for the matching process.

4.5.1. Characteristics of Iris pattern

Following are the important charcteristics of the iris that distinguish this biometric modality and prove it to be highly durable and reliable.

- Iris is not same even for the identical twins.
- There are more than 266 degrees of freedom of Iris.
- Protection to the Iris can be given by the eyelid, cornea and humor and is less susceptible to damage and scratches.
- With aging, it does not degenerate.
- There is no effect of the spectacles or contact lenses while reading the iris structure.

4.5.2. Advantages of Iris biometric trait:

- ✓ High scalability
- ✓ Best search speeds
- ✓ Quick in authentication
- ✓ High levels of safety against identity theft.
- ✓ Spoofing is impossible
- ✓ Convenient to use
- ✓ More accurate
- ✓ High Scalability
- ✓ Fast and easy to use
- ✓ Non-institutive
- ✓ Protection and traceability

4.5.3. Disadvantages of Iris Recognition System

- ✓ Expensive to use because of high cost of scanner
- ✓ Distance setting is too important
- ✓ No movement
- ✓ Reflection causes difficulty
- ✓ Harm to iris due to infrared radiations.
- ✓ High memory requirement.
- ✓ Difficult to control
- ✓ Can be deformed

4.5.4. Applications of Iris Recognition System

- ✓ Finance and banking
- ✓ Healthcare and welfare
- ✓ Public safety

4.5.5. State-of-the-art Work

Sibai *et al.* (2011) proposed a novel approach for preprocessing and design and training of feed forward ANN and back propagation algorithm. For pre-processing, they converted the neural network inputs into JPEG format and retrieved the RGB value from the JPEG format. Three data partitioning approaches such as vertical strip, horizontal strip and blocks and two data coding techniques were used. By using this experiment, recognition accuracy achieved was 93.3%. Rai and Yadav (2014) presented a novel method of recognition through IRIs and by using SVM and hamming distance. They selected zig-zag area of the IRIS and selected, trimmed median filter and parabola detection for the eyelash and eyelid detection and removal. The method achieved success with the recognition rate of 99.91% and 99.8% with the CASIA and CHEK image database, respectively. Marsicso *et al.* (2016) presented a comprehensive survey on the iris recognition through machine learning methods with various classifiers. The goal was to use the linear boundary and the kernel functions necessary to reduce mapping of feature vectors in higher dimensional space and emphasized the use of deep learning to boost the performance and the computation needs. Ouabida *et al.* (2016) proposed an active contour approach depends on the optical correlation algorithm. To detect the iris and pupil region, they used the algorithm based on optical correlation and with a simulation of the Vander Lugt correlator, calculated the energy expression. WVU non-ideal, CASIA v4, UBIRIS v2, MMU2 and a motion video were the four iris image dataset used for the experiment. They evaluated, iris and pupil rays' errors, average segmentation error, iris and pupil centers localization errors, average execution time and three performance metrics named dice coefficient, Hausdroff distance and Jaccard coefficient and achieved high accuracy rates with small computation time. Table 7, describes the major findings with Iris modality based biometric system. Jung *et al.* (2017) presented a different concept for the development of Iris recognition system that is suitable for eyeglasses interference in a mobile environment. For the iris pattern generation and eye validation, they used multi scale window masks and for the validation two separate methods are used. Firstly, the algorithm found the true eye position and the secondly method calculates the difference in intensity between the pupil and its surrounding area was calculated and attained improved and reliable results.

Nguyen *et al*. (2017) presented iris recognition system by using CNN features. They explained that off the shelf trained CNN features are best suited for the iris recognition. CNN architectures benefited the iris recognition with the reduced computational complexity, adaptation of domain, fine tuning, architecture evolution and few shot learning and achieved promising recognition results with ND-CrossSensor-2013 and CASIA-Iris-Thousand iris datasets. Nguyen *et al*. (2017b) presented a comprehensive state-of-the-art work on the iris recognition at a distance system (IAAD). They considered both the perspectives called image acquisition and image processing and contributed by providing the significance, applications, review work and a solution to the designing problems and end with the challenges for IAAD to achieve successful recognition rates. Ahmed and Sama (2019) developed a new approach for increasing the recognition accuracy of iris biometric systems. The target was to use the indexing and improving the accuracy when the size of the database was increased. The probable bin location was fixed depending upon the noise level and then a list of candidate dataset was extracted from the probable bin location. While working on the IITD, CASIA-I3 Interval and UBIRIS 2 iris databases, an empirical study for the wavelength and NIR of LED Illuminators generated good quality IRIS Image. The search was to locate the appropriate gazing point for good capture. At 1.1cm distance, two 850 mms LED were selected for IRIS illumination for the size of 7×13.7 phone, they got the accuracy of 99.4%. Arsalan *et al*. (2019) proposed a novel network for semantic segmentation for the Iris region. The network named Fully Residual Encoder Decoder network FRED-NET was designed to get the accurate boundary, less errors, more accuracy and reliability. So, to detect the true and clear iris region and high frequency information FRED-NET i.e. a complete variant network with residual connectivity in encoder and decoder and is based on the convolutional layers came into picture by the team. The proposed model was implemented on five datasets of Iris for VL and NIR light environment and achieved success as compared with other methods.

Sadhya *et al*. (2019) proposed a framework for extracting consistent bits from the Iris codes. They used a criterion called t-criteria for quantifying the stability of iris codes to remove the effects of noise on the extracted bits which was 300 bits from the CASIAv3 Interval and CASIAv4 Thousand databases and got 0.88-consistency and 0.65-consistency of the Iris Codes respectively which was competitive as compared to baseline results. Umer *et al*. (2019) proposed a novel approach for the person identification based on the iris and periocular biometric modality. The proposed system is based on the image preprocessing data augmentation, feature learning and then classification methods. The objective was to resolve the challenges for near-Infrared or visual wavelength lights under constrained and unconstrained environments have been considered here. The datasets selected for the implementation consisted of MMU1, UPOL, CASIA-Iris-distance, and UBIRIS.v2. with the CNN architectures such as ResNet50, VGG16 and Inception-v3 and achieved effective and robust performance. Varkarakis *et al*. (2019) presented deep neural network and data augmentation methodology for off axis iris segmentation. They employed low complexity network design for the off axis iris segmentation and to achieve reduce memory and computational requirements and the evaluation was done on the publicly available Iris datasets and achieved promising results as compared to the state of the art work.

Nguyen *et al*. (2019) proposed a novel model for the Iris network design in an optimal way by considering model size and computation. They also presented a state-of-the-art work and compared them on the basis of computation and memory requirements. The goal was to fully automate the network design process to achieve the best iris network. And also, to check the optimality of the network was the objective of the study.

Table 7. Major Findings and Results of Iris Biometric Systems

Author/s	Year	Major Findings	Results
Sibai *et al.*	2011	➢ Feed forward ANN and back propagation algorithm ➢ Neural network inputs into jpeg format ➢ Retrieve the RGB value from the jpeg format	➢ Achieved recognition accuracy achieved by their experiment was 93.3%.
Rai and Yadav	2014	➢ Novel method of recognition through IRIs and by using SVM and hamming distance. ➢ Zig-zag area of the IRIS and selected, trimmed median filter and parabola detection for the eyelash and eyelid detection and removal.	➢ Achieved recognition rate of 99.91% and 99.8% with the CASIA and CHEK image database, respectively.
Ouabida *et al.*	2016	➢ Active contour approach ➢ Optical correlation algorithm ➢ Vander Lugt correlator ➢ CASIA v4, WVU non-ideal, MMU2, UBIRIS v2, and a motion video are the four iris images dataset used. ➢ Focus on Iris and pupil centers localization errors, iris and pupil ray errors, average segmentation error, and average execution time. ➢ Used performance metrics such as Dice coefficient, Jaccard coefficient, Hausdroff distance	➢ Better accuracy with small computation time achieved small computation time and high accuracy performance.
Marsicso *et al.*	2016	➢ A comprehensive survey on the iris recognition ➢ Machine learning methods with various classifiers. ➢ To use the linear boundary and the kernel functions	➢ Detailed survey

		➢ Reduce mapping of feature vectors in higher dimensional space ➢ Use of deep learning to boost the performance	
Jung *et al.*	2017	➢ Eyeglasses interference in a mobile environment ➢ Multi scale window masks ➢ True eye position ➢ Calculates the difference in intensity between the pupil and its surrounding	➢ Promising result achieved
Nguyen *et al*.	2017	➢ Iris recognition system by using CNN features ➢ off the shelf trained CNN features are best suited for the iris recognition. ➢ CNN architectures benefited the Iris recognition with the reduced computational complexity, adaptation of domain, fine tuning ➢ Worked on architecture evolution and few shot learning	➢ Achieved promising recognition results with ND-CrossSensor-2013 and CASIA-Iris-Thousand Iris datasets.
Nguyen *et al*.	2017b	➢ Comprehensive state-of-the-art work on the Iris recognition at a distance system (IAAD). ➢ Image acquisition and image processing	➢ Provide significance, applications, review work and a solution
Arsalan *et al*.	2019	➢ Fully Residual Encoder Decoder network FRED-NET ➢ semantic segmentation for the Iris region ➢ Residual connectivity in encoder and decoder ➢ Convolutional layers ➢ Five datasets of Iris for VL and NIR light environment	➢ Outperforms as compared with other methods

Ahmed and Sama (2019)	2019	➢ To use the indexing and improving the accuracy when the size of the database was increased. ➢ The probable bin location was fixed depending upon the noise level ➢ While working on the IITD, CASIA-I3 Interval and UBIRIS 2 iris databases, an empirical study for the wavelength and NIR of LED Illuminators generated good quality IRIS Image. ➢ At 1.1cm distance, two 850 mms LED were selected for IRIS illumination for the size of 7×13.7 phone,	➢ Got accuracy rate of 99.4%
Varkarakis *et al.*	2019	➢ Deep neural network and data augmentation methodology ➢ Off axis iris segmentation. ➢ Low complexity network design ➢ Reduce memory and computational requirements ➢ Worked on the publicly available Iris datasets	➢ Promising results as compared with the state of art work
Nguyen *et al.*	2019	➢ Proposed a novel model for the Iris network design in an optimal way ➢ Presented a state-of-the-art work ➢ Computation and memory requirements are the parameters to study	➢ Successfully achieved optimal network in terms of computation and memory requirements.

4 Handwriting

Handwriting is another very strong biometric identifier which has been widely using for the identification. As the handwriting of every individual is unique, so it can be used for biometric identification. The survey on the handwriting as a biometric trait is mentioned in this section. Not only an individual identification, it can also be used for the gender identification, left or right handedness and even nationality identification. Nogueras *et al.* (2012) presented a framework for biometric recognition using handwriting as a biometric modality. They used short sequence of text and strokes for online handwriting recognition. Ahmed *et al.* (2017) proposed a gender classification system using offline handwriting as a biometric trait. The methodology was based on extracting textural features such as LBP, HOG, GLCM, SFTA from males and females handwriting and classifiers such as ANN, SVM, decision tree and random forests and achieved the classification accuracy of 85%. Bertolini *et al.* (2013) used a local binary pattern (LBP), local phase quantization (LPQ) and the dissimilarity-based approach for the framework of writer identification and verification and got improved results as compared to state-of-the-art work. He and Schomaker (2019) proposed a new concept for writer identification process. They used deep adaptive learning method for this approach based on single-word images and multitasking learning model. They transferred the advantages of the convolutional neural network (CNN) from an auxiliary task in the process of writer identification. They proposed a novel adaptive convolutional layer to use the learned deep features. Lexical content, word length and character attributes are the auxiliary tasks that were evaluated. Experimental results on two benchmark datasets showed the improvement in the performance of writer identification. Chahi *et al.* (0219) presented an effective and conceptually simple framework for the feature representation method for the offline text independent writer identification method. They used LBP, LTP, LPQ and used IFN/ENIT (411 writers/Arabic), AHTID/MW (53 writers/Arabic), CVL (309 writers/English), and IAM (657 writers/English) databases. They cropped the set of connected component images and then these texture images are taken for the feature extraction and then the histogram sequence concatenation is used to the feature image after dimensionality reduction and finally KNN was implemented and achieved success with the Arabic and English scripts as compared to the state-of-the art work. Table 8 describes the major findings with handwriting modality based biometric system.

Table 8. Major Findings and Results of handwriting Biometric System

Author/s	Year	Major Findings	Results
Nogueras *et al.*	2012	➢ Short sequence of text and strokes for online handwriting recognition	➢ Received good accuracy for individual identification.
Bertolini *et al.*	2013	➢ Writer identification and verification. ➢ local binary pattern (LBP), local phase quantization (LPQ) and the dissimilarity-based approach.	➢ Got improved results
Ahmed *et al.*	2017	➢ Offline handwriting as a biometric trait ➢ Extracting textural features such as LBP, HOG, GLCM, SFTA from males and females handwriting ➢ ANN, SVM, decision tree and random forests	➢ Achieved the classification accuracy of 85%.

Schomaker	2019	➢ Writer identification process ➢ deep adaptive learning method ➢ single-word images and multitasking learning model. ➢ convolutional neural network (CNN) ➢ Lexical content, word length and character attributes are the auxiliary tasks that were evaluated.	➢ Experimental results on two benchmark datasets showed the improvement in the performance of writer identification.
Chahi *et al.*	2019	➢ framework for the feature representation method for the offline text independent writer identification ➢ LBP, LTP, LPQ and used IFN/ENIT (411 writers/Arabic), AHTID/MW (53 writers/Arabic), CVL (309 writers/English), and IAM (657 writers/English) ➢ Set of connected component images and then these texture images are taken for the feature extraction and then the histogram sequence concatenation is used to the feature image after dimensionality reduction. ➢ KNN classifier was used ➢ Arabic and English script	➢ Improved results

5 Speech

Biometric recognition systems based on the speech are more comfortable for the users because these systems, neither require remembering passwords and carrying identification cards. These systems help recognizing a person based on their speech using computers and can be effectively useful for the suspect identification, door management systems, and vehicle entry system. Heracleous *et al.* (2018) proposed a method for the speech communication and reducing noise factors. They used to conduct sensors in the noisy environments for their experimental study and got improved results. Fusion methods, Hidden Markov model (HMM), decision fusion was used to integrate several sensors. In the noisy environment, by using late fusion an improvement of a 40% was seen and for the clean environment a 24% recognition improvement was observed.

Dehzangi *et al.* (2012) developed a new method based on the coding methods to achieve discriminative feature transformation for the speech recognition. Every dimension of the features holds some specific information. By using the polynomial expansion, the spectral features can be expanded to a high dimensional space, followed using linear sequence kernels. Here, SVM was used for the classification that projects the feature vectors from the high dimensional into lower dimensions. TIMIT corpus was employed in the study that showed 10.5% ASR error rate reduction. Wu and Tsai (2011) presented an identification system based on the speech by using decomposition that depends upon the empirical model for the feature extraction process. Artificial neural network (ANN) was used for the multi tire solution and decomposition for the non-stationary and non-linear data. Estimating the components, energy will help in reduction of the computational dimension and improving the performance of classification. They used BPNN and GRNN for the classification purpose and revealed that GRNN can give better recognition accuracy rates. Sa *et al.* (2018) proposed highly acceptable lip biometric system with image enhancement methods that capture the local features through Scale Invariant Feature Transform (SIFT). The experiment employed spatial steganography algorithm which uses modulation techniques to produce minimum distortion of images and to hide the subject details. Databases that were selected were NITRLipV1 and NITRLipV2 and the goal was to raise the levels of accuracy and improve the security of the template. Radha *et al.* (2017) presented the acoustic and visual cues that were taken by the alternate sensors (TM and Camera) and by using standard microphone (NM) signal, they developed a biometric recognition system with 145 CV units of the Hindi language and was performed by considering the manner of articulation, the vowels and the place of articulation. By merging the standard and alternate signals, multimodal systems gave better results. Huang *et al.* (2017) built the prediction model based on the temporal nature of the patterns and used multiple classifiers for getting good accuracy rates for the automatic speech recognition (ASR). For decoding, they combined *k* multiple maximum-a-posteriori decoders and estimating the score combination at the state level with the k-combination weight that can be learned through Bayesian settings and performed the classification by using Gaussian mixture model (GMM) and feed forward deep neural networks (DNN) with 15.3% error rate was reported.

Das *et al.* (2018) presented a framework for a biometric recognition system based on the lip trait. Scale Invariant Feature Transform (SIFT) were used for the feature extraction. For the minimum distortion, a spatial steganographic algorithm was employed on the lip images to ensure minimum distortion and ensure that the steganographic algorithm improves the recognition rate.

The datasets used for the implementation of the algorithm were NITRLipV1 and NITRLipV2 and it was concluded that by taking identity hiding performance was improved. Table 9 describes the major findings with speech modality based biometric recognition system.

Table 9. Major Findings and Results of Speech Biometric Recognition System

Author/s	Year	Major Findings	Results
Heracleous *et al.*	2018	• Speech communication and reducing noise factors • Fusion methods, Hidden Markov model (HMM), Decision fusion	• Improvement of a 40% • 24% recognition improvement
Dehzangi *et al.*	2012	• Spectral features are scaled to a high dimension space • Linear sequence kernel • Output coding transformation and set of linear SVMs	• TIMIT corpus showed 10.5% • Reduction in ASR error rate
Wu and Tsai		• Decomposition depends upon the empirical mode • Artificial neural network (ANN) • Decomposition for the non-stationary and non-linear data • BPNN and GRNN for the classification	• Reduction of the computati dimension and improving performance of classification. • Better recognition accuracy rat
Sa *et al.*	2018	• Image enhancement method • Scale Invariant Feature Transform (SIFT) • Spatial steganography algorithm • Modulation techniques • NITRLipV1 and NITRLip • V2 database	• Produce minimum distortion
Radha *et al.*	2017	• Acoustic and visual cues taken from alternate sensors • TM Camera and standard microphone (NM) • 145 CV units of the Hindi language • Manner of articulation, vowels and the place of articulation and vowels	• Better results
Huang *et al.*	2017	• Temporal nature of the patterns and used multiple classifiers • Maximum-a-posteriori decoders • score combination at the state level with the k-combination weight that can be learned through Bayesian settings	• 15.3% error rate was reported.

		• Gaussian mixture model (GMM) and feed forward deep neural networks	
Wu and Tsai	2011	• Artificial neural network and empirical mode decomposition. • generalized neural network and back propagation • improve the training time and performance level	• Gaussian regression better than back propagation method.

6 Joint Action and Human Action

Based on the human action and joint action, ne can identify an individual. This means human action is another biometric trait for the personal identification. Wang *et al.* (2018) presented a framework for the action recognition and human identification together. They proposed a new pipeline using RGBD sensors, skeleton transformation and multitask RNN were also used for the development of a new architecture that calculates the probability among the two variables. The results were really promising as compared with the state-of-the-art work. Wang and Wang (2018) proposed joint action based biometric system and based on that the human can be recognized based on their biological motions. They presented end-to-end framework based on the action recognition and person identification and proposed from skeletons using RGBD sensors. Here the skeleton transformation which recorded viewpoint changes and noise and for learning joints and various architectures, they used multi-task RNN with the. For the implementation of the experiment, 3D action recognition benchmark datasets wereused, and the method outperforms the literature work. IIjjina *et al.* (2017) proposed human action related biometric system. They presented a framework for identifying human actions based on the RGB-D video and deep learning. The features extracted were fed as input to the CNN for the discriminative features. The efficiency wasdependent on the MIVIA action SBU Kinect interaction, NTOPS gesture and Weizmann datasets and was affectedby gesture, event, motion, action or activity recognition, single person or interpersonal interaction, interaction with an object and the crowd behavior analysis. The combination of multi-modal information with noise absorption of ConvNet features facilitated with the robustness, adaptability and optimum performance.

Tu *et al.* (2015) presented human action related biometric system based on the feature extracted using CNN. They constructed one motion stream and by integrating traditional streams and human-related streams, they developed a human-related multi-stream CNN (HR MSCNN) framework that study, encode and analyze appearance, motion of the human-related regions. Four major datasets used in the proposed study were HMDB, HMDB, UCF Sports and UCF and provide improved performance as compared to the survey work. Ozkaya *et al.* (2915) presented a framework for a personal identification system based on the meta carp phalangeal joint patterns. For the feature selection, they used a discriminative common vector (DCV), image acquisition, image pre-processing, feature extraction, matching, and performance evaluation. By using cross fold validation approach on two different datasets, the results proved the importance of MJPs for the biometric system and achieved a recognition rate around 95.33%. Table 10 describes the major findings with Joint action modality based biometric system.

Table 10. Major Findings and Results of Joint action Based Biometric System

Author/s	Year	Major Findings	Results
Ozkaya *et al.*	2015	Meta carp phalangeal joint patterns. Discriminative common vector (DCV) Cross Validation	Recognition rate from 95.33% and 100%.
IIjjina *et al.*	2017	RGB-D video and with deep learning CNN for the discriminative features. MIVIA action SBU Kinect interaction, NTOPS gesture and Weizmann datasets	Multi-modal traits with ConvNet features prove robustness, adaptability and optimum performance.
Tu *et al.*	2015	Human action based biometric system Human-related multi-stream CNN (HR MSCNN). Frameworkencodes and analyze appearance and motion Four major datasets used were JHMDB, HMDB, UCF Sports and UCF dataset this framework.	Superior performance
Wang and Wang	2018	Using RGBD sensors Skeleton transformation Multi-task RNN 3D action recognition benchmark datasets	Method outperforms the survey work
Wang	2018	New pipeline using RGBD sensors, Skelton transformation Mul5rtitask RNN are also used Calculates the combined probability among the two variables.	Results were really promising as compared with the state-of-the-art work

7 Retina

Biometric systems based on retinal image analysis are widely used as the retina trait has the capability to generate very high accurate results. Frucci *et al.* (2017) presented a person verification system consisting of co-registration, retina segmentation, feature extraction and matching and depends upon the construction, associated score map and direction map. The work was carried on two publicly available datasets named VARIA and RIDB. The results showed fitness, robustness and the goodness. Kose and Ibas (2011) presented a biometric identification system based on fingerprint, face, hand, retina palm vein and iris. The application of retina includes weapon factories and nuclear research centers. As the retina is unique to every individual and would not change throughout the life, the priority of this method is obvious. They developed a retinal identification system based on retinal vasculatures and gave the most reliable andsecure outputs by using a dataset of four hundred images with a success rate of 95%.

Fabiola *et al.* (2013) proposed a novel pupillary based recognition system. The iris around the pupil is a very effective physiological trait. Eye based biometric systems depend upon the modalities such as iris, retina, sclera vein. A new verification system will be developed based on the papillary and spatio-temporal features extracted from the spontaneous pupillary oscillations because pupillary provides discriminative and authentic information. The goal was to observe the liveliness based on the spontaneous papillary oscillation methods. The method was executed on the own collected database with equal error rate of 0.2338%. Table 11, describes the major findings with retina modality based biometric system.

Table 11. Major findings and Results of Retina Based Biometric System

Author/s	Year	Major Findings	Results
Fabiola *et al.*	2013	• Spatio-temporal features • Spontaneous pupillary oscillations • Own collected database	• Liveness will be observed • Equal error rate of 0.2338%.
Kose and Ibas	2011	• Retinal identification system developed basis of retinal vasculatures in retina • Tolerates translation, scale and rotation • Segment vessel structure • Four hundred images	• Reliable, secure and precise results • Success rate of 95%.
Frucci *et al.*	2017	• Person verification system includes segmentation, co-registration, feature extraction and matching • Two publicly available datasets called VARIA and RIDB	• Best results as compared with the state-of-the-art work

8 Ocular

Ocular biometric is another extensive biometric trait that covers eye movement, periocular, iris and retina. The ocular system consisting of lens, optic nerve, sclera vasculature etc. Here, presenting the state-of-the-art work on the ocular and periocular biometric trait. CrihalMeanu and Ross (2012) put forward a framework for the ocular biometric system that has been achieved growth and popularity due to various reasons with the iris recognition. They investigated the use of the vasculature patterns and sclera texture and observed that vasculature patterns are better discerned in the visible spectrum (RGB) and iris patterns are better discerned in the near infrared spectrum (NIR). The multispectral picture consists of both NIR and RGB channels are used to imagine the iris and the vasculature patterns. They presented an assembly of a multispectral eye database, the development of a novel algorithm for the segmentation and the results of three feature extraction and matching schemes on the database in order to check the potential of the sclera and the vasculature pattern. Experimental results revealed the potential of the biometric in the ocular-based recognition system. Santana *et al.* (2015) proposed the development of the biometric recognition system based on the facial pattern. They showed the importance and validity of the periocular in varying scenarios even when the whole face is not completely visible. The results reported that the combination of the features extracted from the face, periocular, head and shoulder areas when fused with two stage ensembles of classifier yield better results and reveled 92.6% accuracy rate. Fernandez and Bigun (2015) presented a survey on the biometric research with periocular biometric trait. They explained systematically and comprehensively the state-of-the-art work that includes different aspects, existing datasets, the algorithm used, feature extractions, classifiers and concluded that the research in periocular is a challenging and promising topic. Table 12, describes the major findings with Ocular modality based biometric system.

Table 12. Major findings and Results of Ocular Based Biometric System

Author/s	Year	Major Findings	Results
CrihalMeanu and Ross	2012	• Use of the vasculature patterns and sclera texture. • Vasculature patterns are better discerned in the visible spectrum (RGB) and iris patterns are better discerned in the near infrared spectrum (NIR).	• Revealed the potential of the biometric in the ocular-based recognition system

Santana *et al.*	2015	• Importance and validity of the periocular even when the whole face is not completely visible	• Combination of the features extracted from the face, periocular, head and shoulder areas when fused with two stage ensemble of classifier yield better results and reveled 92.6% accuracy rate
Fernandez and Bigun	2015	• Periocular biometric trait • Systematically and comprehensive state-of-the-art.	• Covering different aspects, existing datasets, the algorithm used, feature extractions, classifiers

9 ECG

Sun *et al.* (2019) proposed an Convolutional Long term Short Memory Neural network for the EEG based biometric systems by taking public data set of 109 people, using 16 channels of EEG signals and achieved accuracy rates of 99.58%. They discussed the benefits of taking CNN and LSTM in improving the accuracy rates and use of spatiotemporal features of the signals in lowering the cost of the systems by decreasing the number of LED electrodes. Goshvarpour and Goshvarpour (2019) proposed a hybrid feature set with the help of ECG characteristics of an individual. They used Cauchy–Schwartz divergence (CSD), Euclidean distance (ED), Cauchy–Schwartz quadratic mutual information (CSQMI), Euclidean distance quadratic mutual information (EDQMI), and cross information potential (CIP). They also presented a method for extracting the features and to use KNN with the Information Gain Ratio (IGR). The use of CIP based index with 2NN achieved maximum of 100% accuracy and the highest accuracy rate was 97.62±1.92.

Table 13. Major findings and Results of ECG Based Biometric System

Author/s	Year	Major Findings	Results
Sun *et al.*	2019	• Convolutional Long term Short Memory Neural network for the EEG based biometric systems • Taking public data set of 109 people, using 16 channels of EEG signals	• Achieved accuracy rates of 99.58%.

Goshvarpour	2019	• ECG characteristics of an individual. • Cauchy–Schwartz divergence (CSD), Euclidean distance (ED), Cauchy–Schwartz quadratic mutual information (CSQMI), Euclidean distance quadratic mutual information (EDQMI), and cross information potential (CIP). • Use KNN with the Information Gain Ratio (IGR).	• CIP based index with 2NN achieved maximum of 100% accuracy and the highest accuracy rate was 97.62±1.92.
Deng *et al.* (2018)		Based on the dynamic neural learning mechanism. • RBF was used to extract cardiac dynamics within ECG signal • Construction of a bank of estimators and the discrimination can be measured. • Cardiovascular disease classification • FuWai and PTB ECG datasets .	• Retrieved satisfactory results.
Labati *et al.*	2018	• ECG based biometric system • Used Deep CNN • Closed-set identification, individual verification and periodic re-authentication	• Deep-ECG produced remarkable accuracy

Deng *et al.* (2018) presented a framework for the biometric recognition system based on the dynamic neural learning mechanism. Here, RBF was used to extract cardiac dynamics within ECG signal by using a learning mechanism followed by the construction of a bank of the estimators and the discrimination can be measured. The method can be extended to the cardiovascular disease classification. An experiment was carried out on the FuWai and PTB ECG datasets and retrieved satisfactory results. Labati *et al.* (2018) have presented an ECG based biometric systemthat was based on deep CNN i.e. deep Convolutional Neural Networks and three tasks such as closed-set identification, individual verification and periodic re-authentication. Deep-ECG understood the QRS complexes retrieved from ECG signals and yielded a set of features extracted using a deep CNN. Deep-ECG extracted two types of templates such as real and binary, which were compared using the Euclidean and Hamming distances, respectively, and evaluated with wide sets of samples collected in uncontrolled conditions for closed-set identification, identity verification and periodic re-authentication and concluded that the Deep-ECG produced remarkable accuracy using real as well as binary templates. Table 13 presents the major findings in a summarized way with the ECG based biometric recognition system.

10 Ear

Hassaballah *et al.* (2018) developed a new framework for the ear based biometric recognition system that depends upon the texture operator and local binary pattern variability. The ear identification and verification process were executed on the five benchmark ear datasets that are publicly available. Local binary pattern LBP was used to extract the spatial structure of the image, its strength, computational efficiency properties, high discriminative power and pattern invariance to monotonic grayscale changes. A new pattern called Averaged local binary patterns (ALBP) was presented that represented the texture of ear images and the result proved that the LBP texture descriptors were well performed with the feature extraction process for the ear traitand achieved recognition rates of 99%. Chowdhury *et al.* (2018) presented an identification system for the ear biometric traitand developed an energy feature based on the wavelets. Total nine classifiers were used for source camera classification. The proposed framework was implemented on WPUT, IITD-I, AMI and AWE datasets. By using four ear datasets, a tunable filter bank-based feature methodcan identify the various sources associated with the ear patterns correctly and accurately with an accuracyof 99.25%. Ghoualmi *et al.* (2016) developed a novel approach based on the ear modality that depends upon the artificial bees. The experiment employed scale invariant featureextraction and transformation method with three datasets IIT Delhi, USTB1 and USTB2 and got superiority among the datasets. Table 14 presents the major findings in a summarized way with the Ear based biometric recognition system.

Table 14. Major findings and Results of Ear Based Biometric System

Author/s	Year	Major Findings	Results
Ghoualmi *et al.*	2016	➢ Novel approach based on the ear modality that depends upon the artificial bees. ➢ experiment employed scale invariant feature extraction and transformation method with three	➢ Got superior results with the datasets.

		datasets IIT Delhi, USTB1 and USTB2.	
Chowdhury *et al.*	2018	➢ Presented an identification system for the ear biometric trait ➢ Energy feature based on the wavelets. ➢ Nine classifiers were used. ➢ WPUT, IITD-I, AMI and AWE datasets.	➢ Accuracy of 99.25%
Hassaballah *et al.*	2018	➢ Depends upon the texture operator and local binary patterns variants. ➢ Executed on the five benchmark ear datasets that are publicly available. ➢ Local binary pattern LBP was used to extract the spatial structure of the image. ➢ A new pattern called Averaged local binary patterns (ALBP) was presented	➢ Proved that the LBP texture descriptors were well performed with the feature extraction process for the ear trait and achieved recognition rates of 99.0%
Goshvarpour	2019	➢ ECG characteristics of an individual. ➢ Cauchy–Schwartz divergence (CSD), Euclidean distance (ED), Cauchy–Schwartz quadratic mutual information (CSQMI), Euclidean distance quadratic mutual information (EDQMI), and cross information potential (CIP). ➢ Use KNN with the Information Gain Ratio (IGR).	➢ CIP based index with 2NN achieved maximum of 100% accuracy and the highest accuracy rate was 97.62±1.92.
Deng *et al.*	2018	➢ Based on the dynamic neural learning mechanism. ➢ RBF was used to extract cardiac dynamics within ECG signal ➢ Construction of a bank of estimators and the discrimination can be measured. ➢ Cardiovascular disease classification ➢ FuWai and PTB ECG datasets	• Retrieved satisfactory results.

Labati *et al.*	2018	➢ ECG based biometric system ➢ Used Deep CNN ➢ Closed-set identification, individual verification and periodic re-authentication	• Deep-ECG produced remarkable accuracy

11 Brainprint

Aloui *et al.* (2017) presented a novel and successful concept in the biometric recognition systemon the brain print trait that depends upon the sulcogyral patterns and brain-fold of an individual which was used for the age identification and then the classification of the gender. They developed a new non-invasive technique that explored a brain cortical region of MRI (Medical Resonance Imaging) based on a dataset of 220 persons. Wavelet Gabor Transformation method was used to construct the brain prints and attained a recognition rate of 99.6%.

12 Gaze

Cantoni *et al.* (2018) developed a biometric recognition system that depends upon the gaze and studied that the eye tracking was considered as a powerful tool for the inspection of scientists and engineers. Various applications of eye tracking include military, surveillance, authentication, etc. They discussed the introduction of gaze based biometric recognition, types, approaches, survey of the applications and the bibliography. They also illustrated some case studies using eye tracking. With the enoughavailability of eye tracking hardware, they tried some new experiments for developing a framework for real world applications.

13 Gait

Ben *et al.* (2019) proposed the framework for the biometric system using gait modality which is a high dimensional modality and employed tensor analysis method. It was observed that when the view angles changes, it was complex to recognize cross-view gait even by using learning multi-linear projection matrices. To handle such complexities a general tensor framework for cross-view gait recognition was proposed. To do so, a tensorial couple of mapping, with the coupling of multi-linear locality-preserved criterion (CMLP), multi-linear marginal fisher criterion (CMMF) and multi-linear discriminant analysis criterion (CMDA) was used. For the experiment, CASIA and OU-ISIR gait datasets were selected and the results showed superior performance. Jain *et al.* (2017) presented a novel method for gender classification system based on the gait information that used built-in sensors of a smart phone, Histogram of Gradient (HoG) for the feature extraction and the bootstrap aggregating classifier. Datasets collected consisted of total 654 gait data from 109 subjects and achieved accuracy rates of 91.8%, 94.4% and 88.9% of the first dataset and 90.5%, 91.1% and 88.5% on the second dataset in accordance with the normal, fast and slow walking speeds, respectively.

5. State-of-the-art work based on multiple modalities and the critical survey

5.1 Multimodal systems and its uniqueness as compared to single modal systems

Biometrics measurement deals with themeasurements of the personal traits such as iris, fingerprints, face, retina, hand geometry, voice or signatures which are used for the current security technologies. Multi-biometric systems are different from unimodal in multiple aspects, but the main reason is that the multi biometric systems use multiple biometric traits for the identification and verification of an identity whereas single biometric systems are dependent only on the one identity.

Difference between Unimodal and Multimodal biometric Systems: -

- ✓ Unimodal Systems: Systems usinga single modality are called unimodal systems. The recognition accuracy of these systems is affected and questionable by sample size, low error rate, poor robustness, noisy sensor data and spoofing attacks. Unimodalsystems are less useful because no single biometric must be sufficiently robust and produce accurate results in real-world applications.
- ✓ The multimodal biometric system can generate the problems by fusing two or more biometricmodalities.
- ✓ The multimodal biometrics provides rich information as compared to unimodal biometric recognition systems.
- ✓ Fusion framework and an efficient recognition algorithm are required for multimodal biometric systems.
- ✓ Multimodal biometrics recognition proved reliable, effective, secure approach to identification and authentication and used in, airport, access and visitor control, suspect identification, check in, face surveillance, Jetway surveillance, attendance logging, DVR integration, robotics, hooligan control, and network security.

✓ The benefits of multimodal biometric systems include (a) Reduce false non-match and false match rates (2) Means of verification, enrollment, and identification (3) Attempts to spoof biometric systems.

5.2 Characteristics of multimodal systems

- Higher reliability
- Improved fault tolerance and reduce noise
- Varieties to accept the complex environment
- Strong security measures are available
- Enhances recognition security by combining with multimodal biometric features

5.3 Survey work associated with Multi modal biometric Systems

Moi *et al.* (2014) presented the combination of most promising biometric traits such as iris and face that help in the identification process. Multimodal systems are based on the non-ideal factors such as angles, reflections, expression changes, variations in posing, or blurred images. They used weighted score level fusion technique to fuse the matching scores from these two traits. The dataset used for the experiment was self-generated and named UniversitiTeknologi Malaysia Iris and Face Multimodal Datasets (UTMIFM), UBIRIS version 2.0 (UBIRIS v.2) and ORL face databases, that got high accuracy and high decidability. Chen *et al.* (2016) developed a novel framework for the multimodal system. They used face and fingerprint images that used block based, feature-image matrix. The proposed method retrieved middle layer semantic features of the local features that result in better characterization capabilities, lower dimension and high accuracy rates for multimodal biometrics. They produced results using the Variational Bayesian Extreme Learning Machine (VBELM) that have high stability and generalization. Experimental results showed higher testing accuracy, higher efficiency and better stability in comparison to the traditional methods. Bouchaffra and Amira (2008) presented a study on Structural Hidden Markov Models (SHMM) for biometrics and proved that the novel machine-learning algorithm known as SHMMs extends traditional HMMs and used the local structures for the biometric identification based on both face and finger modalities. The proposed framework showed the benefits of using wavelets with kernels with the SHMMs classifier. Bouchaffra and Amira (2008) proposed a novel face and fingerprint feature modeling using the structural hidden Markov model (SHMM) and using feature extraction techniques such as ridgelet transform and discrete wavelet transform. The proposed algorithm showed that SHMM is more promising as compared to state-of-the-arts classifiers when combine with the discrete wavelet transform. The experiment proved that the with the of ridgelet transform without principal components analysis (PCA) dimension reduction produced better results with the support vector machines (SVMs) classifier. Barrero *et al.* (2017) presented a method for the development of a multi biometric system based on the homomorphic encryption method where all the information either stored in the database is encrypted. Multi-biometric fusion namely feature, score and decision level were used. Experiments were carried out on the on-line signature and fingerprint dataset BiosecurID. The system fulfilled the requirements established in the ISO/IEC 24745.Jing *et al.* (2007) proposed a classifier for the development of recognition system based on the face and palm print images. They executed the Gabor transform on face and palm print images and combine them at the pixel level. The results proved that there was a very small correlation between their normalized Gabor-transformed images. The experiment used a novel classifier, KDCV-RBF to classify the fused biometric images and extracting the image features using a Kernel discriminative common vector (KDCV) approach and performed classification by using the radial base function (RBF) network. As the test data, we take two largest public face databases (AR and FERET) and a large palmprint database. The FERET database consisted of 2200 facial images consisting of 200 individuals with each person contributing 11 images and the AR face database that contains over 4000 color face images of 126 people. The experimental results revealed the proposed biometric fusion recognition approach performs better than the state-of-the-art work. Walia *et al.* (2018) proposed a robust biometric system based on the multi identifiers and on the optimum score level fusion model. The system considered biometric modalities such as Iris, finger vein and fingerprint. They used backtracking search optimization method (BSA) and the proportional conflict redistribution rules (PCR-6) and Fusion of the scores after using multiple traits produced better outputs. Various methods for the fusion are Einstein product, T-norms called Hamanger, Frank and Yagerand used Support Vector Machine for classification and reported accuracy rates of 98.43% with error rates of 1.57%. Table 15 presents the major findings in a summarized way with the multimodal biometric recognition system.

Table 15. Major Findings and Results of Multimodal Biometric Systems

Author/s	Year	Major Findings	Results
Moi *et al.*	2014	• Iris and face biometric traits • Angles, reflections, expression changes, variations in posing, or blurred image angles, reflections, expression changes, variations in posing, or blurred images • Weighted score level fusion technique to fuse the matching scores • UniversitiTeknologi Malaysia Iris and Face Multimodal Datasets (UTMIFM), UBIRIS version 2.0 (UBIRIS v.2) and ORL face databases	• Got high accuracy and high decidability.
Walia *et al.*	2018	• Iris, finger vein and fingerprint • Used backtracking search optimization method (BSA) and the Proportional conflict redistribution rules (PCR-6) • Fusion of the scores after using multiple traits produced better outputs. • Various methods for the fusion are Einstein product, T-norms called Hamanger, Frank and Yager • Support Vector Machine	• The experiment performed the accuracy rates of 98.43% with error rates of 1.57%.
Barrero *et al.*	2017	• Homomorphic encryption method where all the information either stored in the database is encrypted. • Multi-biometric fusion namely feature, score and decision level were used. • Experiments were carried out on the on-line signature and fingerprint dataset BiosecurID. • The system fulfils the requirements established in the ISO/IEC 24745.	•
Jing *et al.*	2007	• (KDCV) approach and performed classification by using the radial base function (RBF) network. • As the test data, we take two largest public face databases (AR and FERET) and a large palmprint database. • The FERET database includes 2200 facial images consisting of 200 individuals with each person contributing 11 images and the AR face database that contains over 4000 color face images of 126 people.	• Gabor transform on face and palm print images • A novel classifier, KDCV-RBF

		• The experimental results revealed the proposed biometric fusion recognition approach performs better than the state-of-the-art work.	
Chen *et al.*	2016	• Used block-based feature image matrix. • The proposed method retrieved middle layer semantic features of the local features with better characterization capabilities, lower dimension and high accuracy rates. • Used Variational Bayesian Extreme Learning Machine (VBELM) with high stability and generalization. • Experimental results showed higher testing accuracy, higher efficiency and better stability.	
Bouchaffra and Amira	2008	• Structural Hidden Markov Models (SHMM) for Biometrics • Fusion of Face and Fingerprint • Novel machine-learning algorithm known as SHMMs extends traditional HMMs • Local structures for the biometric identification based on both face and finger modalities. • Wavelets with kernels with the SHMMs classifier.	
Bouchaffra and Amira	2008	• Proposed a novel face and fingerprint feature model • Used Structural hidden Markov model (SHMM) • Feature extraction techniques such as ridgelet transform and discrete wavelet transform were employed.	• SHMM is more promising as compared to state-of-the-art. • Ridgelet transform without principal components analysis (PCA) dimension reduction. • Produced better results with the support vector machines (SVMs) classifier.

5.4 Design and Implementation of multi biometrics recognition trade-offs

Biometric recognition systems are based on both software and hardware-based techniques. To satisfy all the challenging requirements such as user friendliness, low cost, fast, high performance, less intrusive, high fake detection rates and fraud prevention, the following design issues are to be included such as:

- ✓ Selecting the right biometric modalities.
- ✓ Selecting number of traits.
- ✓ Choosing the required samples for a biometric.
- ✓ Methodology for fusion.
- ✓ Learning weights of biometric traits.
- ✓ Cost-performance and accuracy-reliability trade-offs
- ✓ Verification system for application
- ✓ Features selection difficulties or complexities
- ✓ Privacy issues should be handled

5.5 Factors considered during the development of System with Multi biometric Identifiers:

Following are the important factors that must be taken care of, for the development of multi biometric systems. From the data collection, to the fusion approach, to the feature selection, classifiers and the accuracy achieved, various factors play a vital role.

- There should be no performance loss in the selected protected domain.
- Secure irreversible templates are to be stored in the server's database for achieving irreversibility.
- As no plain information is shared and no biometric information is leaked, thus preventing hill-climbing or inverse biometrics attacks
- The developed system should be used for real-time applications.
- Feature level fusion is most preferred fusion methods for achieving better performance.

6. Synthetic Analysis and Discussions

Biometrics is the science of identifying an individual based on the attributes or traits and is widely used in the civilian, commercial and security systems. Detailed study of biometric systems is not easy as it consists of a vast collection of attributes, datasets, approaches, various layouts of frameworks and so on. Before presenting the critical and synthetic analysis, two steps are necessary which are critical reading and then critical writing. By synthetic analysis, we mean considering various perspectives at own level and on the constituent. By carefully studying, the single and multimodal biometric traits, state-of-the-art work, feature extraction methods, classification methods, dataset collection, online availability, easy approach to pattern collections, comparison of recognition accuracy achieved, following are the discussions which are helpful for the development of biometric systems. So, for the researchers and the readers, the critical and synthesis analysis of biometric system based on the single trait and multiple biometric traits is presented below:

- ✓ Biometric systems have reduced error rates and frauds, improved accuracy, good opportunities for reducing costs, high scalability, increasing physical safety measures, interesting and convenient to use.
- ✓ In password accepting systems, the systems perform well with the right password or token that are used for accessing the sensitive services, but on the other hand, these systems cannot be sure regarding the presence of that correct individual which causes serious problems.
- ✓ Biometric systems confirm an individual regarding the sure identity.
- ✓ It is not to say that the biometric systems are the replacement of authentication tools and technologies, but combining biometric approaches with authentication methods, can increase and improve security aspects of the applications where user cooperation can be inferred.
- ✓ Multimodal biometric systems when compared to the Unimodal systems always prove to be an intelligent agent for giving expert decision in distinguishing genuine subjects as these are based on multiple modalities.
- ✓ It is being assumed after the state-of-the-art work that the facial and Iris recognition systems (Stand-alone) are getting more popular as compared to other traits.
- ✓ Changes in disease, age, stress, training, environment, occupational factors, intentional alterations andsocio-cultural aspects of the situation andchange in human interface with the system affects the recognition rate.
- ✓ Information can be degraded by using data manipulation or transformation and may be corrupted resulting in the inappropriate compression, security breaches, mismanagement causes challenges for the development.
- ✓ Biometric data is generally different from the basic personal information and the templates that are used to access personal information cannot be reverse engineered.

- ✓ Based on the single trait or multiple traits for the development of biometric systems, it is concluded that biometric systems based on the multiple traits are more efficient, reliable and accurate results as multiple traits give more values to the features and hence to the classification.
- ✓ For improving the recognition performance, feature-domain super-resolution and deep-learning super-resolution approaches are in great demand.
- ✓ Multiple modalities used by the multimodal biometric systems overcome the problems faced by the individual classifiers.
- ✓ As many datasets are available, yet there is a need of self-generated datasets with required quantity in terms of sample collections.
- ✓ For the face, speech, iris and fingerprint are most commonly used biometric trait.
- ✓ As seen the popularity and the growth of biometric systems to increase the security, surveillance, discipline and the motivations to do continual work progress with safety measures, their values and needs are increasing day by day.
- ✓ Not only private, even government offices are using biometric systems for the successful operation and the environment.
- ✓ Tables systematically represent the feature extraction methods, classifiers, datasets, accuracy rates, this will pose a challenge to the researchers for an improved version of the development of biometric systems depending upon their choice of the trait.

7. 3D Biometrics: A Future and Challenging perspective

Zhang and Lu (2013) thoroughly explaining the use and advantages of 3D view of biometric modalities for the development of biometric systems. They were listing fingerprint, face, ear and many more modalities in building 3D biometrics systems. For meeting various security needs, more efforts have been put on the development of 3D biometric systems. This section focuses on the today's demand for the person identification with 3D images of biometric modalities. The area is still unexplored in fine capturing of 3D data and if it is possible, then it will be a marvelous shift to meet the real paradigm for the biometric recognition. Biometric modalities are in real sense better represented by using 3D representations and to work with 2D biometric modality will erect a huge difference in terms of accuracy and efficiency as compared with 3d biometric recognition techniques. So, there is a necessitate to use the improved 3D methodological techniques starting from the data collection, preprocessing, feature extraction followed by the classification process which should be highly compatible with 2D and 3D data. To make it practically viable, there is requirement of sensors, scanners, high quality 3D models, biometric authentication techniques with 3D modality images. Fig.10. shows 3D images of various biometric modalities.

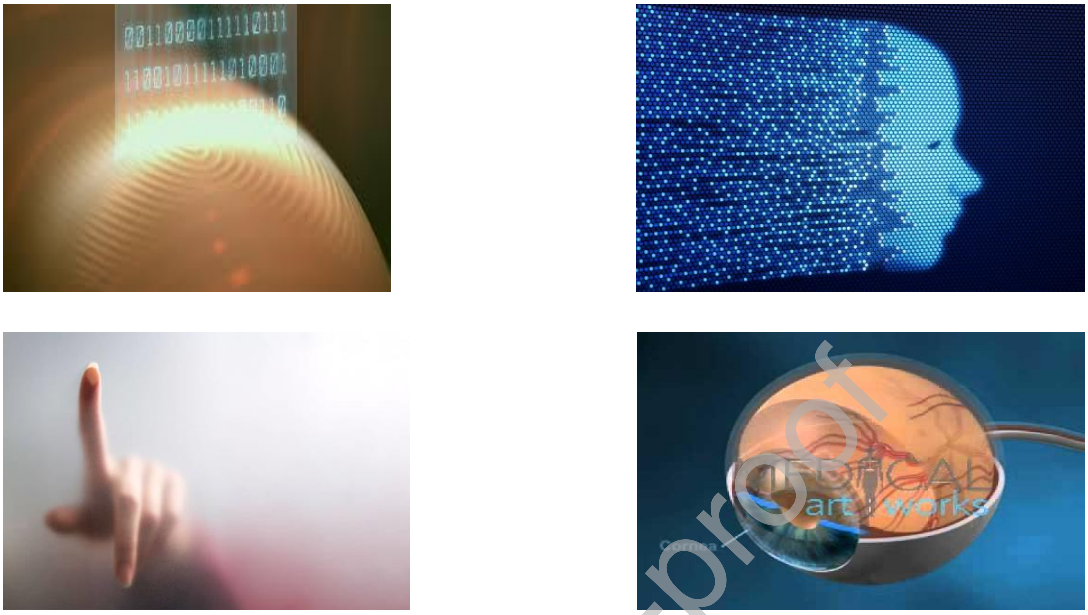


Fig. 10. 3D view of fingerprint, face and eye biometric modality

Most of the biometric recognition methods are based on the 2D images but it's the fact that human characteristics are represented in real way in 3D surface only such as 3D face, 3Dfingerprint, 3D palm vein, 3D ear recognition. An individual identification and verification are worthwhile and productive for many applications such as e-commence, access control, immigration, Internet banking, law enforcement and so on will only produce more accurate results if we shift from 2D to 3D images. 3D biometric technologies are more secured as compared to the 2D methods. These are specially designed to achieve high security requirements, high robustness, more acceptable to variations, providing rich source of information. These 3D approaches can also be fused with the 2D approaches for enhance the accuracy and reliability. Lula (2019) presented a unique and promising method for biometric recognition based on ultrasound which acquires 3D images and providing distinct features with high accurate results.

8. Concluding Remarks

Biometric recognition systems are the systems that have been continuously developed for improving the security levels and comfort in the working environment. The development is made possible only with pattern recognition, machine learning and deep learning methodologies. The wide variety of applications includes Mobile, ATM forensic security, PC, smart cards and networks. The goal of this paper is to make, the researchers aware regarding the development of a framework for biometric systems for novel applications, feature extraction methods, various classifiers, datasets and accuracy rate. The paper presents the comprehensive and systematic survey on the unimodal and multimodal biometric system based on the various traits andtry to cover maximum possible traits. The goal is to compactly summarize the results, other vital research findings in the tabular form for every trait. This will facilitate the naive users with the latest developments, advantages and helps the society by giving measures for the security, surveillanceand investigation levels with reduced cost and increased accuracy. By looking at the popularity and wide acceptance of these recognition systems by the users, it is predicted that the future of the biometric technology is very bright, positive and upbeat especially by inculcating 3D images for the biometric modalities such as fingerprint, ear, face, palm vein, gait and so on. There are still many open directions for the researchers with their novel, exciting and motivating ideas for contributing with the latest developments of the frameworks for unimodal and multimodal biometric systems by integrating 2D and 3D biometric recognition techniques.

References

Aloui K, Nait-Ali A, Naceur MS (2018). Using Brain Prints as New Biometric Feature for Human Recognition Pattern Recognition Letters, *Pattern Recognition Letters*, 113: 38-45. DOI: 10.1016/j.patrec.2017.10.001

Arsalan M, Kim DS, Lee MB, Owais M, Park KR (2019). FRED-Net: Fully Residual Encoder-Decoder Network for Accurate Iris Segmentation. *Expert Systems with Applications,* 122 (2019) 217–241. doi:10.1016/j.eswa.2019.01.010,.

Asaari MSM, Suandi SA, Rosdi BF (2014). Fusion of Band Limited Phase Only Correlation and Width Centroid Contour Distance for finger based biometrics. *Expert Systems with Applications,* 41:3367–3382.

Barrero GM, Maiorana E, Galbally J, Campisi P, Fierrez J (2017). Multi-biometric template protection based on Homomorphic Encryption. *Pattern Recognition*, 67:149–163.

Ben X, Zhang P, Lai Z, Yan R, Zhai X, Meng W (2019). A general tensor representation framework for cross-view gait recognition. *Pattern Recognition*.DOI:10.1016/j.patcog.2019.01.017

Bingol O, Ekinci M (2017). Stereo-Based Palmprint Recognition in Various 3D Postures, *Expert Systems with Applications. Expert Systems with Applications*, 78: 74-88, DOI: 10.1016/j.eswa.2017.01.025

Bouchaffra D, Amira A (2008a). Feature generation and machine learning for robust multimodal biometrics, *Pattern Recognition*, 41: 775–777.

Bouchaffraa D, Amira A(2008b). Structural hidden Markov models for biometrics: Fusion offace and fingerprint, *Pattern Recognition*, 41: 852–867

Cai R, Zhang Z, Hao Z (2013). Causal Gene identification using combinatorial V-structure search. *Neural Networks*, 43:63–71. DOI:10.1016/j.neunet.2013.01.025

Cantoni V, Musci M, Nugrahaningsih N, Porta M (2018) Gaze-based biometrics: An Introduction to forensic applications. *Pattern Recognition Letters,* 113:54-57.

Chen Y, Yang J, Wang C, Liu N (2016). Multimodal biometrics recognition based on local fusion visual features and Variational Bayesian extreme learning machine. *Expert Systems with Applications*. 64:93-103

Chevtchenko SF, Vale RF, Macario V (2017). Multi-Objective Optimization for Hand Posture Recognition. *ExpertSystems With Applications*. 92:170-181

Chowdhury DP, Bakshi S, Sa PK, Majhi B (2018). Wavelet Energy Feature Based Source Camera Identification for Ear Biometric Images, *Pattern Recognition Letters*, DOI: https://doi.org/10.1016/j.patrec.2018.10.009

CrihalMeanu S, Ross A (2012). Multispectral scleral patterns for ocular biometric recognition, *Pattern Recognition Letters*, 33:1860–1869

Das S, Muhammad K, Bakshi S, Mukherjee I, Sa PK, Sangaiah AK, Bruno A (2018). Lip Biometric Template Security Framework Using Spatial Steganography, *Pattern Recognition Letters*. DOI: 10.1016/j.patrec.2018.06.026

Dehzangi O, Mab B, Chng ES, Li H (2012) Discriminative feature extraction for speech recognition using continuous output codes, *Pattern Recognition Letters*, 33(13):1703-1709.

Delac K and Gargic M (2004). A Survey of Biometric Recognition Methods. *In Proceedings of 46th International Symposium on Electronics,* 184-193.

Deng M, Wang C, Tang M, Zheng T (2018). Extracting cardiac dynamics within ECG signal for human identification and cardiovascular diseases classification. *Neural Networks*, 100: 70–83. DOI:10.1016/j.neunet.2018.01.009

Dutta N (2009). A survey of biometric technology based on handshape, *Pattern Recognition.* 42: 2797-2806

Escobar MA M, Hernandez CC, Perez AF, Gutierrez RML (2015). A robust embedded biometric authentication system based on fingerprint and chaotic encryption. *Expert Systems with Applications*. 42(21):8198-8211.

Ezeobiejesi J, Bhanu B (2017). Latent Fingerprint Image Segmentation Using Deep Neural Network. *Chapter in Book Deep Learning for Biometrics*. *Advances in Computer Vision and Pattern Recognition. Springer, Cham*, 83-107.

Fabiola M, Castaldi V, Gomez ES (2013). A new spontaneous pupillary oscillation-based verification system. *Expert Systems with Applications*, 40(13):5352–5362

Fernandez FA, Bigun J (2015). A survey on Periocular Biometrics Research, *Pattern Recognition Letters*, 82(2):92-105.

Frucci M, Riccio D, Baja GS, Serino L (2017). Using direction and scoreinformation for retina based person verification Maria, *Expert Systems With Applications*. DOI: 10.1016/j.eswa.2017.10.044

Galbally J, Bostrom G, Beslay L (2017). Full 3D Touchless Fingerprint Recognition: Sensor, Database and Baseline Performance. *In Proceedings of International Joint Conference on Biometrics*. 225-233. 10.1109/BTAS.2017.8272702

Guo JM, Hsia CH, Liu YF, Yu JC, Chu MH, Le TN (2012). Contact free hand Geometry-based Identification System, *Expert Systems with Applications*, 39:11728–11736.

Han WY, Lee JC (2012). Palm vein recognition using adaptive Gabor filter. *Expert Systems with Applications*. 39: 13225–13234.

Heracleous P, Even J, Sugaya F, Hashimoto M, Yoneyama A (2018). Exploiting Alternative Acoustic Sensors for Improved Noise Robustness in Speech Communication, *Pattern Recognition Letters*, DOI: 10.1016/j.patrec.2018.07.014

Huang DY, Hub WC, Hsiang S (2011). Gabor filter-based hand-pose angle estimation for hand gesture recognition under varying illumination. *Expert Systems with Applications*, 38(5): 6031–6042.

Huang Z, Siniscalchi SM, Lee CH (2017). Hierarchical Bayesian Combination of Plug-inMaximum A Posteriori Decoders in Deep Neural Networks-based Speech Recognition and Speaker Adaptation.*Pattern Recognition Letters*. 98:1-7

Ijjina EP, Mohan CK (2017). Human action recognition in RGBD videosusing motion sequence information and deep learning. *Pattern Recognition.*72:504-516

Jain A, Kanhangad V (2017). Gender classification in smartphones using gait information, *Expert Systems With Applications*, 93”:257-266

Jain AK, Nandakumar K, Ross A (2016). 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognition Letters*, 79:80–105

Jalali A, Mallipeddi R, Lee M (2017). Sensitive deep convolutional neural network for face recognition at large standoffs with small dataset. *Expert Systems With Applications*. 87:304–315.

Jing XY, Yao YF, Zhang D, Yang JY, Li M (2007). Face and palmprint pixel level fusion and Kernel DCV-RBF classifier for small sample biometric recognition, *Pattern Recognition*, 40(11):3209-3224.

Jun B, Kim D (2012). Robust face detection using local gradient patterns and evidence accumulation. *Pattern Recognition*, 45(9):3304–3316

Jung Y, Kim D, Son b, Kim J (2017). An Eye detection method robust to eye glasses for mobile Iris recognition. *Expert Systems with Applications*, 67:178-188

Kas M, Merabet YE, Ruichek Y, Messoussi R (2018). Mixed Neighborhood Topology Cross Decoded Patterns For Image-Based Face Recognition, *Expert Systems With Applications*.114:119-142

Kose C, Ibas CI (2011). A Personal Identification System using retinal vasculature in retinal fundus Images. *Expert Systems with Applications*, 38(11):13670–13681

Labati RD, Munoz E, Piuri V, Sassi R, Scotti F (2018). Deep-ECG: Convolutional Neural Networks for ECG biometric recognition, *Pattern Recognition Letters*.DOI: 10.1016/j.patrec.2018.03.028

Li Ce, Xie C, Zhang B, Chen C, Han J (2018). Deep Fisher Discriminant Learning for Mobile Hand Gesture Recognition. *Pattern Recognition*. 77: 276-288

Lin CH, Chen JL, Tseng CY (2011). Optical Sensor measurement and biometric-based fractal pattern classifier for fingerprint recognition.*Expert Systems with Applications*, 38(5):5081–5089.

Lula A (2019). Ultrasound system for Biometric Recognition. *Sensors (Basel),* 19(10):2317.doi: 10.3390/s19102317

M Hassaballah, Hammam A Alshazly, Abdelmgeid Ali (2018). Ear recognition using local binary patterns: A comparative experimental study.*Expert Systems With Application*s. DOI: https://doi.org/10.1016/jeswa.2018.10.007

Mamta, Hanmandlu M (2014). Robust authentication using the unconstrained infrared face images, *Expert Systems with Applications*, 41(14):6494-6511.

Marsicso MD, Petrosino A, Ricciardi S (2016). Iris Recognition through Machine Learning Techniques: A Survey, *Pattern Recognition Letters*, 82(2):106-115

Moi SH, Asmuni H, Hassan R, Othman RM (2014). Weighted score level fusion based on non-ideal iris and face images. *Expert Systems with Applications*. 41(11):5390-5404.

Muller MK, Tremer M, Bodenstein C, Wurtz RP (2013). Learning invariant face recognition from examples. *Neural Networks*, 41:137–146.

Nguyen K, Fokes C, Ross A, Sridharan S (2017). Iris Recognition With Off-the-Shelf CNN Features: A Deep Learning Perspective, *In the Proceedings of IEEE Conference*, 6: 18848-18855.

Nguyen K, Fookes C, Jillela R, Sridharana S, Ross A (2017b). Long range Iris Recognition: A survey. *Pattern Recognition,* 72:123-143, https://doi.org/10.1016/j.patcog.2017.05.021

Nguyen K, Fokes C, Sridharan S (2019). Constrained Design of Deep Iris Network. *Computer Vision and Pattern Recognition*. https://arxiv.org/abs/1905.09481

Nguyen K, Fookes C, Sridharan S, Tistarelli M, Nixon M (2018). Super-Resolution for Biometrics: A Comprehensive Survey. *Pattern Recognition,* 1-43.

Nogueras SE, Zanuy FM (2012). Biometric recognition using online uppercase handwritten text. *Pattern Recognition*, 45(1):128–144.

Pakutharivu P, Srinath MV (2015). A Comprehensive Survey on Fingerprint Recognition Systems. *Indian Journal of Science and Technology*, 8(35):1-7.

Ouabida E, Essadique A, Bouzid A, Lugt V (2016). Correlator Ouabida based Active Contours for Iris Segmentation and Tracking. *Expert Systems with Applications*, 71(C):383-395.

Ozbulak G, Aytar Y and Ekenel HK (2016) How Transferable Are CNN-Based Features for Age and Gender Classification? *Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG)*, 1-6.

Pascual CV, Hurtado AS, Martinez EM, Gaspar JP (2016). Client Threshold Prediction in Biometric Signature Recognition by Means of Multiple Linear Regression and Its Use for Score Normalization. *Pattern Recognition*, 55:1-13.

Raghavendra R, Raja KB, Venkatesh S and Busch C (2017) Transferable Deep-CNN Features for Detecting Digital and Print-Scanned Morphed Face Images. *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, Honolulu, HI, 1822-1830.

Ramaiah NP, Ijjina CP and Mohan CK (2015) Illumination invariant face recognition using convolutional neural networks. *Proceedings of the IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES)*, Kozhikode, 1-4.

Qin H, Wang P (2019). Finger-Vein Verification Based on LSTM Recurrent Neural Networks. *Applied Sciences*, 9(8):1-18.

Qiu S, Liu Y, Zhou Y, Huang J, NieY (2016). Finger-vein recognition based on Dual-Sliding window localization and pseudo-elliptical transformer. *Expert Systems with Applications*. 64:618–632

Radha N, Shahina A, Prabha P, Preethi Sri BT, Nayeemulla Khan A (2017). An analysis of the effect of combining standard and alternate sensor signals on recognition of syllabic units for multimodal speech recognition. *Pattern Recognition Letters.*115:39-49.

Rai H, Yadav A (2014). Iris recognition using combined support vector machine and Hamming distance approach. *Expert System with Applications*. 41(2):588593.

Riera FB, Gonzalez AM, Vazquez HM (2017). Facial Marks for Improving Face Recognition. *Pattern Recognition Letters*, DOI: 10.1016/j.patrec.2017.05.005

Sadhya D, Kanjar De , Raman B, Roy PP (2020). Efficient extraction of consistent bit locations from binarized Iris features. *Expert Systems with Applications*, 140:1-10, 112884.

Santana MC, Navarro JL, Balmaseda ER (2015). Periocular biometric recognition System on using periocular biometric for gender classification in the wild. *Pattern Recognition Letters*, 1–9.

Sibai FN, Hosai HI, Naqbi RM, DhaniSani S, Shehhi S (2011). Iris recognition using ANN. *Expert System with Applications*, 38(5):5940-5946.

Su CL (2009). Palm-print Recognition by matrix Discriminator. *Expert Systems with Applications,* 36:10259–10265.

Tsai CY, Lee YH (2011). The parameters effect on performance in ANN for hand gesture recognition System. *Expert Systems with Applications*, 38(7): 7980-7983

Umer S, Sardar A, Dhara B C, Raout R K, Pandey H M (2019). Person Identification using fusion of Iris and Periocular Deep Features. *Neural Networks*, 1-18. DOI: https://doi.org/10.1016/j.neunet.2019.11.009, Reference: NN 4317

Varkarakis V, Bazrafkan S, Corcoran P (2019). Deep neural network and data augmentation methodology for off-axis iris segmentation in wearable headsets. *Neural Networks*, 121:101-121, https://doi.org/10.1016/j.neunet.2019.07.020

Wang H, Wang L (2018). Learning content and style: Joint action Recognition and Person Identification from human Skelton.*Pattern Recognition*. 81:23-35

Walia GS, Rishi S, Asthana R, Kumar A, Gupta A (2019). Secure multimodal biometric System based on diffused graphs and optimal score fusion.*IET Digital Library*, 8(4):231–242

Waisy ASA, Qahwaji AR, Ipson S, Fahdawi AS (2017). A multimodal biometric system for personal identification based on deep learning approaches. *In Proceedings of Seventh International Conference on Emerging Security Technologies, 163-168.*

Wang S, Deng G, Hu J (2017). A Partial Hadamard transform approach t the design of cancelable fingerprint template containing binary biometric representation, *Pattern Recognition*, 61:447-458.

XiX, Yang Lu, Yin Y (2016). Learning Discriminative Binary Codes for Finger Vein Recognition, *Pattern Recognition.*66:26-33

Yadav S, Virendra P, Vishwakarma (2018). Extended Interval Type-II and Kernel Based Sparse Representation Method for Face Recognition. *Expert Systems With Applications*. 116:265-274

Yaddaden Y, Adda M, Bouzouane A, Gaboury S, Bouchard B (2018). User Action and Facial Expression Recognition for Error Detection System in an Ambient Assisted Environment.*Expert Systems With Applications.*112:173-189

Yan Y, Wang H, Chen S, Cao X, Zhang D (2016). Quadratic projection based feature extraction with its application to biometric recognition. *Pattern Recognition*, 56:40–49.

Yang W, Wang S, Hu J, Zheng G, Valli C (2018). A Fingerprint and Finger-vein Based Cancelable Multi-biometric System, *Pattern Recognition*. 78:242-251.

Yoo SH, Oh SK, Pedrycz W (2015). Optimized face recognition algorithm using radial basis function neural networks and its practical applications. *Neural Networks*, 69:111–125.

Yua YF, Daia DQ, Rena CX, Huang KK (2017). Discriminative multi-scale sparse coding for single-sample face recognition with occlusion. *Pattern Recognition*, 66:302-312.

Zhang D, Guangming L (2013). 3D Biometrics, Systems and Applications. Springer New York, ISBN: 978-1-4614-7399-2

ZhigangT, Wei X, Qianqing Q, RonaldP, Remco CV, Baoxin L, Junsong Y (2018). Learning representations based on human-relate regions for action recognition. *Pattern Recognition*, 79:32-43

Zhu C, Zheng Y, Luu K, Savvides M (2016) CMS-RCNN: Contextual Multi-Scale Region-based CNN for Unconstrained Face Detection. *Computer Vision and Pattern Recognition*. DOI: arXiv:1606.05413