© UNIVERSAL RESEARCH REPORTS | REFEREED | PEER REVIEWED
ISSN : 2348 - 5612 | Volume : 04 , Issue : 07 | October - December 2017

Multimodal Biometric System : A Review

Bhushan Kumar

Central University of Rajasthan

2016mtcse003@curaj.ac.in

Abstract

Biometric is a method to verify the identity of a person based on psychological characteristics or behavioral characteristics. Examples of biometrics are fingerprints, iris, face, ear, voice-speech, palm print, signature, and handwriting or keystrokes patterns. Biometric systems are classified into two types: (1) Unimodal biometric system (2) Multimodal biometric system. There is a limited accuracy in the unimodal biometric system. Accuracy can be improved by using multimodal biometric system. Two or more biometric traits are used in multimodal biometric system. This paper presents characteristics of biometrics, comparison of biometric modalities, difference between unimodal and multimodal biometrics, limitations of unimodal biometrics, fusion levels in biometrics.

Keywords:- Biometrics, Unimodal biometrics,Multimodal biometrics, Fusion levels.

Introduction

In today's world where technology is growing with a rapid pace, still there are several person authentication- related issues that need to be handled in daily life.

There are three different types of authen-tication for security. They are something you know- it provides a PIN, password, or details of person's information,something you have- it includes a smart card, card key or secure ID card and something you are- which provides biometric information.Among these, biomet-ric systems provide secure and convenient au-thentication tool and it is not able to stolen, barrowed or forgotten and forging biometric information is very impossible.

Biometric comes from the Greek words bios (life) and metron (measure), and hence biologi-cal measurement is termed as biometric.It refers to the person's physiological (e.g., face, speech, fingerprint, iris) or behavioral (e.g., signature, gait or speech too) characteristics. Physiolog-ical biometrics are related to the shape of the body and are generally more stable. Behavioral biometrics are related to the behaviour of the person and are comparably less stable.

To provide confidential financial transactions and personal data privacy, biometrics is used. Biometrics is used in federal, state and local governments, in military and commercial appli-cations. And also in secure electronic banking, government IDs, retail sales, health and social services are using these technologies.

Authen-tication based applications include network, data protection, remote access to resources, workstation, transactions and web security. To provide healthy growth of the global economy, electronic transactions are essential in biomet-rics. Trust in these electronic transactions is essential to the healthy growth of the global economy. Biometrics is integrated with other technologies such as smart cards, encryption keys and digital signatures. Biometrics is used in our daily lives. Biometric systems are more accurate and convenient for authentication and identification of a person.

II. General Biometrics Technology

A. Processing phases of biometrics

There are three different processing phases are available in biometrics: they are (1) Enrollment phase (2) Verification phase and (3) Identifica-tion phase.

- Enrollment phase

In this phase, template of the individual person images is stored in the database to check person's identity. Using image of that person, features are extracted.

- Verification phase

In this phase, the person is verified with his template which is available in the database by comparing person's captured data.

- Identification phase

In the identification phase, the system will store all user's details. So the system iden-tifies an individual by searching the tem-plates of all users in the system. The sys-tem performs one to many comparisons to verify an individual identity, if it is en-rolled in the system record.

B. Working of Biometric system

The block diagram of biometric system as shown in figure 1 and its working as follows:

- Sensor Module: In this module, different sensors are used to capture biometric data of the individual.
- Preprocessing: Here, to remove noise from the image, filters are used. Image is con-verted into requires size that is the cap-tured image is preprocessed.
- Feature Extraction: In this module, once the image is captured and preprocessed from the sensor module and preprocessing module respectively. Then features are extracted from the image using feature extraction module.
- Matching Module: In this module, as we know template of the individual data is

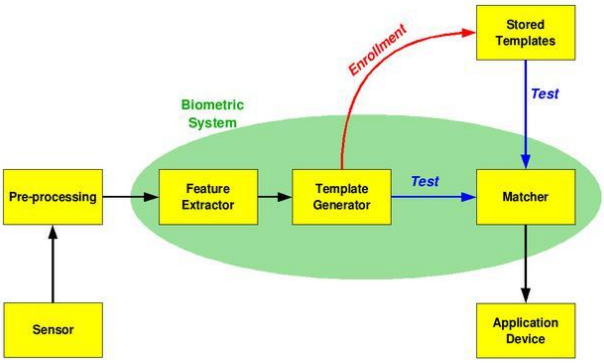


Figure 1: Block diagram of biometric system

stored in the database. So the comparison between the features extracted from the input data and the template stored in the database are performed.

- System Database Module: In this phase, templates of all users are stored in the database.

III. Motivation

Using biometrics, it is easy to recognize an in-dividual based on the recognition methods. To recognize an individual it has some reasons, they include reducing costs and improving scal-ability, reducing error rates, improving accu-racy, improving convenience and increasing physical safety. To verify a person it is required to have passwords, names, social security num-bers, tokens and PINs, so that the person may access its services or benefits. For example ATM card and its corresponding PIN are re-quired to access an automatic teller machine (ATM).

IV. Comparison Of Various Biometrics

A number of biometric characteristics exist and are in use in various applications. Each biomet-ric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is "optimal" The match be-tween a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic. A brief introduc-tion to the commonly used biometrics is given below.

- DNA: Deoxyribonucleic acid (DNA) is the one-dimensional (1-D) ultimate unique code for one's individuality except for the fact that identical twins have identi-cal DNA patterns. It is, however, currently used mostly in the context of forensic ap-plications for person recognition. Three issues limit the utility of this biometrics for other applications: 1) contamination and sensitivity: it is easy to steal a piece of DNA from an unsuspecting subject that can be subsequently abused for an ulterior purpose; 2) automatic real-time recognition issues: the present technology for DNA matching requires cumbersome chemical methods (wet processes) involv-ing an expert's skills and is not geared for on-line noninvasive recognition; and 3) privacy issues: information about sus-ceptibilities of a person to certain diseases could be gained from the DNA pattern and there is a concern that the unintended abuse of genetic code information may re-sult in discrimination, e.g., in hiring prac-tices.

- Ear:It has been suggested that the shape of the ear and the structure of the carti-legenous tissue of the pinna are distinc-tive. The ear recognition approaches are based on matching the distance of salient points on the pinna from a landmark lo-cation on the ear. The features of an ear are not expected to be very distinctive in establishing the identity of an individual.

- Face:Face recognition is a nonintrusive method and facial images are probably the most common biometric character-istic used by humans to make a per-sonal recognition. The applications of fa-cial recognition range from a static, controlled "mug-shot" verification to a dy-namic,uncontrolled face identification in a cluttered background(e.g., airport). The most popular approaches to face recogni-tion are based on either: 1) the location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the over-all (global) analysis of the face image that represents a face as a weighted combina-tion of a number of canonical faces. While the verification performance of the face recognition systems that are commercially available is reasonable. In order for a fa-cial recognition system to work well in practice, it should automatically: 1) detect whether a face is present in the acquired image; 2) locate the face if there is one; and 3) recognize the face from a general viewpoint (i.e., from any pose).

- Facial, hand, and hand vein infrared thermogram:The pattern of heat radiated by human body is a characteristic of an individual and can be captured by an in-frared camera in an unobtrusive way much like a regular (visible spectrum) photo-graph. The technology could be used for covert recognition. A thermogram-based system does not require contact and is noninvasive, but image acquisition is challenging in uncontrolled environments, where heat emanating surfaces (e.g., room heaters and vehicle exhaust pipes) are present in the vicinity of the body. A re-lated technology using near infrared imag-ing is used to scan the back of a clenched fist to determine hand vein structure. In-frared sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermograms.

- Fingerprint:Humans have used finger-prints for personal identification for many centuries and the matching accuracy us-ing fingerprints has been shown to be very high. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is deter-mined during the first seven months of fetal development. Fingerprints of iden-tical twins are different and so are the prints on each finger of the same per-son. Today, a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications.The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small- to medium-scale identification sys-tems involving a few hundred users. Mul-tiple fingerprints of a person provide addi-tional information to allow for large-scale recognition involving millions of identities. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identi-fication mode. Finally, fingerprints of a small fraction of the population may be unsuitable for automatic identification be-cause of genetic factors, aging, environ-mental, or occupational

reasons (e.g., man-ual workers may have a large number of cuts and bruises on their fingerprints that keep changing).

- Gait:Gait is the peculiar way one walks and is a complex spatio-temporal biomet-ric. Gait is not supposed to be very distinc-tive, but is sufficiently discriminatory to allow verification in some low-security ap-plications. Gait is a behavioral biometric and may not remain invariant, especially over a long period of time, due to fluc-tuations in body weight, major injuries involving joints or brain, or due to inebri-ety. Acquisition of gait is similar to ac-quiring a facial picture and, hence, may be an acceptable biometric. Since gait-based systems use the video-sequence footage of a walking person to measure several dif-ferent movements of each articulate joint, it is input intensive and computationally expensive.
- Hand and finger geometry:Hand geom-etry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fin-gers. Commercial hand geometry-based verification systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmen-tal factors such as dry weather or indi-vidual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry infor-mation may not be invariant during the growth period of children. In addition, an individual's jewelry (e.g., rings) or limita-tions in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry information. The physical size of a hand geometry-based system is large, and it cannot be embed-ded in certain devices like laptops. There are verification systems available that are based on measurements of only a few fin-gers (typically,index and middle) instead of the entire hand. These devices are smaller than those used for hand geom-etry, but still much larger than those used in some other biometrics (e.g., fingerprint, face, voice).

- Iris:The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side.The vi-sual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. The accu-racy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris infor-mation. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect arti-ficial irises (e.g., designer contact lenses). Although, the early iris-based recognition systems required considerable user par-ticipation and were expensive, the newer systems have become more user-friendly and cost-effective.
- Keystroke:It is hypothesized that each per-son types on a keyboard in a characteristic way. This behavioral biometric is not ex-pected to be unique to each individual but it offers sufficient discriminatory in-formation to permit identity verification. Keystroke dynamics is a behavioral bio-metric; for some individuals, one may ex-pect to observe large variations in typical typing

patterns. Further,the keystrokes of a person using a system could be moni-tored unobtrusively as that person is key-ing in information.

- Odor:It is known that each object exudes an odor that is characteristic of its chemi-cal composition and this could be used for distinguishing various objects. A whiff of air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of (aromatic) compounds. A component of the odor emitted by a hu-man (or any animal) body is distinctive to a particular individual. It is not clear if the invariance in the body odor could be detected despite deodorant smells, and varying chemical composition of the sur-rounding environment.

- Palmprint:The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the fin-gerprints. Since palmprint scanners need to capture a large area, they are bulkier and more expensive than the fingerprint sensors. Human palms also contain ad-ditional distinctive features such as prin-cipal lines and wrinkles that can be cap-tured even with a lower resolution scanner. Finally, when using a high-resolution palmprint scanner, all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas),principal lines, and wrinkles may be combined to build highly accurate biometric system.
- Retinal scan:The retinal vasculature is rich in structure and is supposed to be a char-acteristic of each individual and each eye. It is claimed to be the most secure bio-metric since it is not easy to change or replicate the retinal vasculature. The im-age acquisition requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a prede-termined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eye piece, and requires a conscious effort on the part of the user. All these factors adversely affect the public accept-ability of retinal biometric. Retinal vasculature can reveal some medical condi-tions, e.g., hypertension, which is another factor deterring the public acceptance of retinal scan-based biometrics.

- Signature:The way a person signs his or her name is known to be a characteristic of that individual. Although signatures require contact with the writing instru-ment and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification. Signatures are a behavioral biometric that change over a period of time and are influenced by phys-ical and emotional conditions of the sig-natories. Signatures of some people vary substantially: even successive impressions of their signature are significantly differ-ent. Further, professional forgers may be able to re-produce signatures that fool the system.
- Voice:Voice is a combination of physiolog-ical and behavioral biometrics. The fea-tures of an individual's voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound. These physiological character-istics of human speech are invariant for an individual, but the behavioral part of the speech of a

person changes over time due to age, medical conditions (such as a com-mon cold), and emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification. A text-dependent voice recognition system is based on the utterance of a fixed pre-determined phrase. A text-independent voice recognition system recognizes the speaker independent of what she speaks. A text-independent system is more diffi-cult to design than a text-dependent sys-tem but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sen-sitive to a number of factors such as back-ground noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel.

V. Biometrics Comparison

There are various numbers of pros and cons for every biometric system. The main aim of biometrics is to change the existing password. Biometrics uses both biological and physiolog-ical features to identify a person. Biometrics has some of the features which include iris patterns, retina design, facial geometry, finger-prints, voice recognition and hand recognition and so on.

The following seven factors are:

- Universality
- Uniqueness
- Permanence
- Measurability
- Performance
- Acceptability
- Circumvention

In Universality, using biometric trait every individual should access the application. In Uniqueness, for every person the given bio-metric trait is different from other person. In permanence, for a given matching algorithm, biometric trait for a person is invariant over time. The biometric trait which changes signifi-cantly is not a good biometric. In measurability, the biometric trait uses suitable devices, these devices should be able to acquire and digitize the trait for every individual and it is inconve-nience to the biometric trait. The biometrics system uses acquired raw data to process and to extract features from the biometric trait. In performance, biometrics system should have the higher accuracy to meet the requirements of the application and to achieve this accu-racy it requires recognition accuracy and the resources are required to achieve the accuracy. In acceptability, every individual should have biometric trait in the system and these indi-viduals will use application to present their biometric trait to the system in the large pop-ulation. In circumvention, using biometrics it is easy to imitate the artifacts using biometric traits for example, mimicry can be used for behavioral characteristics and for physiological characteristics fake fingers are used to imitate the biometric trait of an every person. Secu-rity should be very important, to conform the needs of the application.

VI. Unimodal and Multimodal Biometrics

For identification and verification features, bio-metric uses a single biometric trait of the per-son is referred as unimodal biometrics. Bio-metrics which uses more than two biometric traits of the individual to identify a person is called as multimodal biometrics. The recogni-tion rate can be improved by using multimodal biometrics. Compared to unimodal biometrics, multimodal biometrics is most widely used in the organizations.

VII. Limitation of Unimodal Biometrics

The successful installation of biometric systems in various civilian applications does not imply that biometrics is a fully solved problem. It is clear that there is plenty of scope for im-provement in biometrics. Researchers are not only addressing issues related to reducing er-ror rates, but they are also looking at ways to enhance the usability of biometric systems.

Biometric Systems that operate using any sin-gle biometric characteristic have the following limitations.

- Noise in sensed data. The sensed data might be noisy or distorted. A fingerprint with a scar or a voice altered by cold are exam-ples of noisy data. Noisy data could also be the result of defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavor-able ambient conditions (e.g., poor illumi-nation of a user's face in a face recognition system). Noisy biometric data may be in-correctly matched with templates in the database resulting in a user being incor-rectly rejected.
- Intra-class variations.The biometric data ac-quired from an individual during authenti-cation may be very different from the data that was used to generate the template during enrollment, thereby affecting the matching process. This variation is typi-cally caused by a user who is incorrectly interacting with the sensor or when sen-sor characteristics are modified (e.g., by changing sensors-the sensor interoperabil-ity problem) during the verification phase. As another example, the varying psycho-logical makeup of an individual might re-sult in vastly different behavioral traits at various time instances.
- Distinctiveness.While a biometric trait is expected to vary significantly across in-dividuals, there may be large inter-class similarities in the feature sets used to rep-resent these traits. This limitation restrictsthe discriminability provided by the bio-metric trait. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.
- Nonuniversality.While every user is ex-pected to possess the biometric trait be-ing acquired, in reality it is possible for a subset of the users to not possess a par-ticular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor qual-ity of the ridges. Thus, there is a failure to enroll (FTE) rate associated with using a single biometric trait. It has been empiri-cally estimated that as much as 4% of the population may have poor quality finger-print ridges that are difficult to image with the currently available fingerprint sensors and result in FTE errors.
- Spoof attacks.An impostor may attempt to spoof the biometric trait of a legitimate enrolled user in order to circumvent the system. This type of attack is especially relevant when behavioral traits such as signature and voice are used. However, physical traits are also susceptible to spoof attacks. For example, it has been demon-strated that it is possible (although dif-ficult and cumbersome and requires the help of a legitimate user) to construct arti-ficial fingers/fingerprints in a reasonable amount of time to circumvent a fingerprint verification system.

VIII. Multibiometrics

Multi-biometric combine two or more differ-ent biometric sources of a person and sensed by different sensors. This system relies on the evidence presented by multiple sources of bio-metric information.

Therefore, it can be classified into the following categories:

- Multi-sample: In this system, a single sen-sor can be used to acquire multiple sam-ples of the same biometric sources in order to account for the variations that can occur in the trait. One of the main issues in this system is in determining the number of samples that have to be acquired from a person.
- Multiple algorithms:Multi-algorithm sys-tems combine the output of multiple fea-ture extraction algorithms or multiple matchers or other algorithms operating on the same set of images or traits. Since it uses the same sensor are cost effective.
- Multiple instances system:For this type of system, multiple instances of the same body sources are used which is also known as multi-unit systems. It can be cost effective if single sensor is used.
- Multimodal System:This is the current biometric systems researchers are work-ing which involved two or more biometric traits being used for user identification. It can be expensive because more sensors are used.
- Multi-sensor system:Data from the same biometric recorded from different sensors are linked together. These are then inte-grated at fusion level.
- Hybrid:This is a system which merge more than one of the above multi-biometric systems.
- Study have found that multi-biometrics im-proved better than a unimodal biometric in terms of increasing the security level. This boost the level of confidence for people to use and trust the system. Each biometric traits has its own strengths and weaknesses and the choice typically depends on the application.

IX. Multimodal Biometric System

Multimodal biometric systems are more reli-able because of the many, independent biomet-ric traits. Due to this it has higher accuracy in identifying an individual. The system is uni-versal in nature because it can take other form of biometric traits for identification purpose. It also has liveness detection which protect from spoofing or hackers.

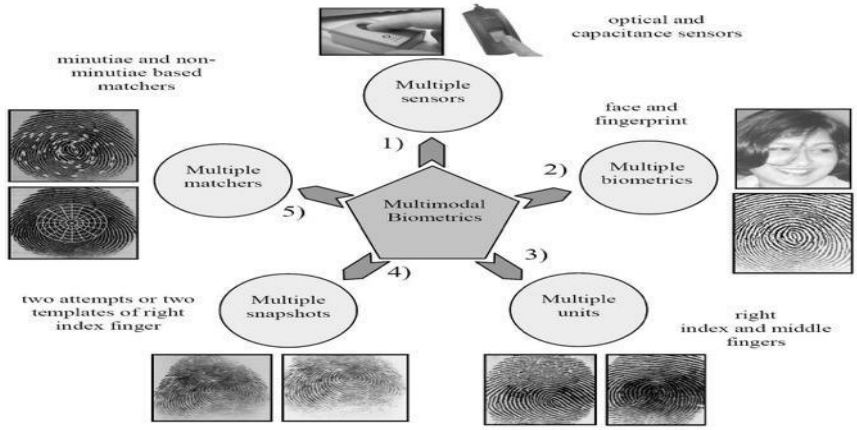


figure 2: Various scenarios in a multimodal biometric system.

Multimodal biometric system can perform in three different ways:

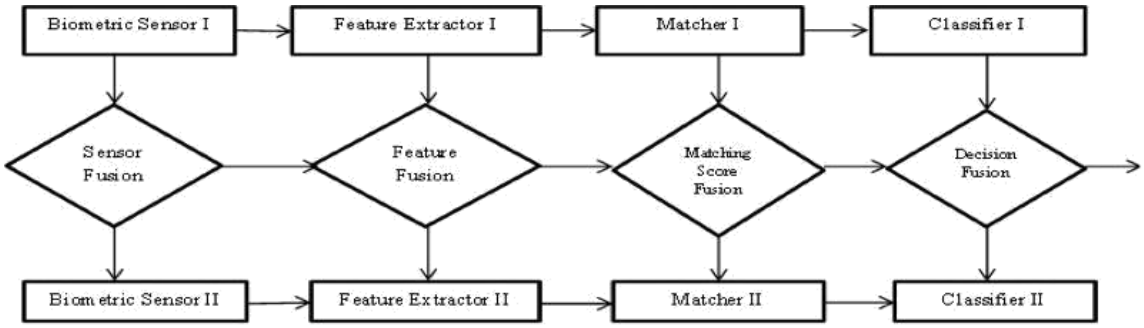
- Serial mode (cascade mode):Each trait is examined before the next trait is investi-gated. The overall recognition duration can be decreased, as the total number of possible identities before using the next trait could be reduced.
- Parallel mode:Sensed or captured image from multiple traits are used in concurrent way to perform recognition. Final decision is taken from the combined results.
- Hierarchical mode:Individual classifiers are joint together in a hierarchy-tree-like-structure. This mode is preferred when a large number of classifiers are expected.

X. Fusion Levels In Biometrics

In multibiometrics, two or more biometric trait is used in biometric systems and also decision channels used more than one. Biometric fu-sion is defined as its aim is to design a proce-dure, which combines classification outcome from each biometric channel. To decrease the weakness of individual measurements and to enhance the strengths using different biometric attributes, biometric fusion is used widely in the industry.

In biometrics system, implementations of multibiometrics can be done by using levels of fusion. To address number of issues in the bio-metrics, fusion is used. Some of the issues are robustness, applicability, accuracy, efficiency and universality. To increase robustness of the multibiometrics, various levels of fusion are used for fusing the biometrics traits. Four types of fusions are available they are as fol-lows: sensor level, feature level, matching score level and decision level. The block diagram of fusion levels in a multibiometrics as shown in figure 3.

- Fusion using sensor level:Merged biometric trait is formed by using different sensors. For example fingerprint scanner, iris scan-ner and video camera etc. Fusing of bio-metrics traits is done by using different sensors. And these biometrics traits are processed.
- Fusion using Feature level:Signals are pro-cessed first which are coming from dif-ferent biometric traits in the feature level. And later from each biometric trait, sep-arately feature vectors are extracted. In feature level fusion, signals coming from different biometric channels are first pro-cessed after which the feature vectors are extracted separately from each biometric trait. The fusion algorithms are used to form composite feature vector by combin-ing feature vectors and later classifications are applied for feature vectors. To select useful features, reduction techniques are used in feature level. Compared to match-ing score method, feature level contains richer information of biometrics and there-fore good recognition results are obtained from feature level fusion. And also when features of different biometric traits are compatible, feature level provides more accuracy.



- Fusion using Matching score level:Instead of combining feature vectors, they are pro-cessed separately in the biometrics. Then matching score for each individual bio-metric trait is obtained and on the basis of accuracy of biometrics trait, composite matching score is found by fusing match-ing level. And later classifications are used. To combine match scores, number of tech-niques is used such as mean fusion, highest rank, logistic regression etc. By using different traits, normalization of scores are acquired which is the important benefit of this fusion. To achieve this normalization of match scores, some of the techniques used are z-score, piecewise linear, min-max etc. Less complexity is obtained from matching score level compared to other fusions and therefore this level of fusion is used widely.

- Fusion using Decision level:Separately pre-classification of each biometric trait is done first in the decision level. In the biometrics, individual biometric trait is captured first and extraction of features is done from the captured trait. Classifica-tion of traits is done as either accepts or re-jects on the basis of extracted features. By combining the outputs of different traits, final classification of biometrics is done.

XI. Previous Work

Anil Jain et al.,[5] introduce a multimodal biometric system in, which integrates face recognition, fingerprint verification, and speaker verification in making a personal iden-tification. This system takes advantages of the capabilities of each individual biometrics.The final decision made by this system is based on the integration of the decisions made by the fingerprint verification module,the face recognition module, and the speaker verifica-tion module.They have used Cryptographic algorithm for Feature extraction method.

S. Liu et al., [8] proposes a user access, e-commerce and other security applications by using secure authentication method. With the help of physically and behavioral characteristics biometrics are used to identify a person, for that reason biometrics is used. For examples fingerprint, hand or palm geometry, and retina, iris, or facial, signature, voice, keystroke, pattern, and gait. Here, signature and voice biometrics traits are used to implement the proposed work.

Figure 3: Multibiometrics Fusion Levels.

S. Ribaric et al.,[11] propose a scanner-based multimodal biometric identification system that integrates palm-print, finger- and hand-geometry features. The system is based on a low-cost desktop scanner, which is used as the biometric acquisition device. As the system has a high user acceptance and high user-identification accuracy, it is attractive for restricting access to web pages that contain confidential information or for authenticating users of e-commerce applications.Fusion at the matching-score level is obtained by means of the total similarity measure. In the decision module, three rules are used to establish identity. The system was tested on a database of 130 persons. The test performance, FAR=0% and FRR =0.2%, suggests that the system can be used in medium and high-security Internet environments.

Teoh et al.,[14] presents a decision fu-sion technique for a bimodal biometric verification system that makes use of facial and speech biometrics.The decision fusion schemes considered have simple Bayesian structures (SBS) that particularize the univariat Gaussian density function, Beta density function or Parzen window density estimation. SBS has advantages in terms of computation speed, storage space and its open framework.From the experiments, it has been found that the best result is obtained by using SBS with the particularized Beta density function as this leads to lower FAR and FRR, compared to other SBS schemes that particularize the univariat Gaussian and estimated density function by using the Parzen window as well as other classical fusion schemes.

Conti V. et al.,[2] proposed a multimodal bio-metric system using two different fingerprints of the same person.The matching module integrates fuzzy logic methods for matching score fusion. Experimental trials using both decision level fusion and matching score level fusion were performed. Experimental results show an improvement of 6.7% using the matching score level fusion rather then a unimodal authentication system.

Shahin et al.,[12] described the design and development of whole hands biometrics prototype system that acquires left and right (L/R) index and ring fingerprints (FP), L/R Near-Infra-Red (NIR) dorsal hand vein (HV) patterns, and L/R NIR dorsal hand geometry (HG) shape. The acquired sample images were found to have good quality for all features and patterns extraction to all modalities. The designed prototype can be considered for authentication and identification purposes. Advantages of this system over few existing multimodal systems are its being very hard to spoof attacks on the sensory level and the NIR HV and NIR HG themal images are good signals for liveness detection.This system has the accuracy of 95.8%.

Monwar et al.,[9] presented an effective fusion scheme that combines information

presented by multiple domain experts based on the rank-level fusion integration method. The developed multimodal biometric system possesses a number of unique qualities, starting from utilizing principal component analysis and Fisher's linear discriminant meth-ods for individual matchers (face, ear, and signature) identity authentication and utilizing the novel rank-level fusion method in order to consolidate the results obtained from different biometric matchers. The ranks of individual matchers are combined using the highest rank, Borda count, and logistic regression approaches. The results indicate that fusion of individual modalities can improve the overall performance of the biometric system, even in the presence of low quality data.This paper present a comparison between various PCA and FLD-based multimodal biometric systems and differences between the results obtained before and after using rank-level fusion.

Tayal et al., [13] proposes a multimodal biometric system that combines iris recogni-tion and speaker identification systems using the energy compaction and time frequency resolution of wavelet analysis,. The uniqueness of iris pattern and the robustness of speaker identification based on pitch period estimation complement each other in the proposed system. The paper also critically analyzes the implementation of Daubechies wavelets (Db3 and Db4) in the analysis of iris and speech samples with an endeavor to have a high success rate with optimal computational complexity.The success rate of the system was evaluated on the basis of registered templates in the database created during enrolment process and newly entered templates for authentication. The success rate was found to be 99.6%.

Ravi J et al.,[10] proposes a multimodal biometric system that combines finger and iris together. They used Fast fourier transform, concatenation and euclidean matching as a feature extraction method.They proposes PCA technique for IRIS and Finger print biometrics. For proposed model, multibiometrics fuses PCA minutia extraction and Weighted LBP feature extraction. The results from these extractions are applied on different biometric traits. To identify a person the IRIS and Fin-gerprint are used in the proposed system. To compare performance and accuracy different recognition methods are used. Examples of classifiers are SVM and ANN. These are used for matching.

Islam, Syed MS, et al.,[4] presented an automatic extraction of local 3D features (L3DF) from ear and face biometrics and their combination at the feature and score levels for robust identification. This paper is the first to present feature level fusion of 3D features extracted from ear and frontal face data. Scores from L3DF based matching are also fused with iterative closest point algorithm based matching using a weighted sum rule. We achieve identification and verification (at 0.001 FAR) rates of 99.0% and 99.4%, respectively, with neutral and 96.8% and 97.1% with non-neutral facial expressions on the largest public databases of 3D ear and face.

Gawande et al.,[3] this paper presents a feature level fusion method for a multimodal biometric system based on fingerprints and irises. The proposed approach for fingerprint and iris feature extraction, fusion, and classi-fication by RBFSVM and PolySVM has been tested for unimodal as well as multimodal identification systems using the real fingerprint database and CASIA iris database. In greater detail, the proposed approach performs fingerprint and iris feature extraction using the Haar wavelet based method. These codified features are the representation of unique template. The improvement in performance of FAR, FRR, and response time is observed as compared to existing researches. From the experimental results it can be concluded that the feature level fusion produces better recognition than individual modalities. The proposed method sounds strong enough to enhance the performance of multimodal biometric. The proposed methodology has the potential for real-time implementation and large population support.

Lathika et al.,[7] proposes a multimodal biometric system consisting of a combination of face, ear (physical traits) and gait biometric (behavioural traits) modalities. The ear has an advantage since it is co-located with the face and hence it can be captured with the same or similar sensor. The Gait recognition has unique advantages over traditional biometric. Advances in sensor technology like miniaturized accelerometers in smart phones and Kinect camera have provided the means to record and analyze gait data from a new point of view. In this work we employ a wavelet transform for feature extraction, which describes the ratio between dark and bright areas. In the recognition stage, we use artificial neural networks to achieve good recognition rate in the presence of wide facial variations. Samples of Face, Ear

and Gait datasets from GAID, CAS IA, US TB, AR, UWA and ORL database were used to evaluate the performance of the system. The samples are normalizedusing z-score method for better fusion results. Further, match score fusion approaches were used for fusing the face, ear and gait.

Aizi et al.,[1] proposed a client-server network architecture for a remote multimodal biometric identification. As a matter of fact, they used two modalities, namely, the human iris and his fingerprint in order to strengthen the security, since the unimodal biometric systems cannot always be used reliably to perform recognition. However, the association of the information presented by the various modalities may allow a precise recognition of the identity. Concerning the fusion of these two modalities, they used a new approach at the scores level based on a classification method by the decision tree and a combination method by the sum. The results obtained confirm that the proposed method helped significantly to optimize the performance of the identification.The application of the biometrics on the internet still raises several problems. Among these problems there are the security issues. One must secure the biometric data by finding the ways to restrict the access to these data.

XII. Conclusion

Multimodal biometrics are gaining its popular-ity in the current technological world. These systems are expected to improve the recogni-tion accuracy of a personal authentication sys-tem by combining the evidence presented by multiple sources of information. There has been evidence that this type of system is bet-ter than applying unimodal biometric systems and can overcome the problems in the previous system.

In this study, current and previous multimodal biometric systems are summarized and pre-sented. The level of fusions that can be ap-plied is also presented. The list is expanding and becoming longer as there are still many combination of biometric traits have not been explored e.g., face and iris, speech and iris, 2D fingerprint and 2D iris.

Multimodal biometric systems is gaining its popularity and becoming reality application in the world of verification and identification for the purpose of integrity, safety and security.

References

[1]. Kamel Aizi, Mohamed Ouslim, and Ahmed Sabri. Remote multimodal bio-metric identification based on the fusion of the iris and the fingerprint. In Electrical Engineering (ICEE), 2015 4th International Conference on, pages 1–6. IEEE, 2015.

[2]. Vincenzo Conti, Giovanni Milici, Patrizia Ribino, Filippo Sorbello, and Salvatore Vitabile. Fuzzy fusion in multimodal bio-metric systems. In International Conference on Knowledge-Based and Intelligent Information and Engineering Systems, pages 108–

[3]. 115. Springer, 2007.

[4]. Ujwalla Gawande, Mukesh Zaveri, and Avichal Kapur. A novel algorithm for fea-ture level fusion using svm classifier for multibiometrics-based person identifica-tion. Applied Computational Intelligence and Soft Computing, 2013:9, 2013.

[5]. Syed MS Islam, Rowan Davies, Mo-hammed Bennamoun, Robyn A Owens, and Ajmal S Mian. Multibiometric human recognition using 3d ear and face features. Pattern Recognition, 46(3):613–627, 2013.

[6]. Anil K Jain, Lin Hong, and Yatin Kulka-rni. A multimodal biometric system using fingerprint, face and speech. In Proceed-ings of 2nd Int'l Conference on Audio-and Video-based Biometric Person Authentication, Washington DC, pages 182–187, 1999.

[7]. Anil K Jain, Arun Ross, and Salil Prab-hakar. An introduction to biometric recog-nition. IEEE Transactions on circuits and sys-tems for video technology, 14(1):4–20, 2004.

[8]. BA Lathika and D Devaraj. Artificial neu-ral network based multimodal biometrics recognition system. In Control, Instrumen-tation, Communication and Computational Technologies (ICCICCT), 2014 International Conference on, pages 973–978. IEEE, 2014.

[9]. Simon Liu and Mark Silverman. A practi-cal guide to biometric security technology. IT Professional, 3(1):27–32, 2001.

[10]. Md Maruf Monwar and Marina L Gavrilova. Multimodal biometric system using rank-level fusion approach. IEEE Transactions on Systems, Man, and Cyber-netics, Part B (Cybernetics), 39(4):867–878, 2009.

[11]. J Ravi, KS Geetha, TN Anitha, and KB Raja. Bimodal biometric system using multiple transformation features of finger-print and iris. ACEEE Int. J. on Information Technology, 1(3):20–25, 2011.

[12]. Slobodan Ribari´c, Damir Ribari´c, and Nikola Paveši´c. Multimodal biometric user-identification system for network-based applications. IEE Proceedings-Vision, Image and Signal Processing, 150(6):409–416, 2003.

[13]. MK Shahin, AM Badawi, and ME Rasmy. A multimodal hand vein, hand geometry, and fingerprint prototype design for high security biometrics. In Biomedical Engi-neering Conference, 2008. CIBEC 2008. Cairo International, pages 1–6. IEEE, 2008.

[14]. Akash Tayal, Ramya Balasubramaniam, Ashwini Kumar, Anwesha Bahattachar-jee, and Monisha Saggi. A multimodal biometric authentication system using de-cision theory, iris and speech recognition. In Nonlinear Dynamics and Synchronization, 2009. INDS'09. 2nd International Workshop on, pages 1–8. IEEE, 2009.

[15]. Andrew BJ Teoh, Salina Abdul Samad, and Aini Hussain. A face and speech bio-metric verification system using a simple bayesian structure. Journal of information science and engineering, 21(6):1121, 2005.