www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 2 Issue 5 May, 2013 Page No. 1487-1500

FINGERPRINT, RETINA AND FACIAL RECOGNITION BASED MULTIMODAL SYSTEMS

Sachin Dwivedi, Shrey Sharma, Vishwa Mohan, Khatana Arfan Aziz
UG, DGI Greater Noida
sachindwivedi18@gmail.com, sshreysharma6591@gmail.com, vishwa92.hari@gmail.com, arfan2121@gmail.com

Abstract

Biometrics is automated methods of identity verification or identification based on the principle of measurable physiological or behavioral characteristics. Their characteristics are unique and not duplicable or transferable. This paper mainly focuses on a multimodal that comprises of retinal scan, facial recognition and fingerprint scan. Being a very convenient and user friendly way of authentication it is preferred much these days but at the same time it must be secure and reliable enough to meet various security attacks. A biometric system is a system which recognizes the human characteristics and trails, which is use for identifications and access control.The recognition is done on the bases of physiology and behavior characteristics. A unimodal biometric system is one which has only the limited accuracy. So as to improve the accuracy and security of biometric systems researchers came up with the idea of the multi modal biometric system. A multi modal biometric system integrates the results of two or more biometric trails. This paper deals with the multimodal biometric system.

Keywords: multimodal, soft biometric, automated, feature extraction, furrows, ridges

1.0 Introduction

According to International Standard Organization (ISO), biometric means ―automated recognition of individuals on the basis of their physiological and behavioral characteristic. Today's world is becoming more and more insecure and people demand for a security system which is less vulnerable against burglar attacks. To seek out this problem biometric device is one of the solutions. A biometric is the combination of two Greek words bio (life) metric and metric (to measure). Biometric identifies the distinctive, measurable characteristics used The first known example of biometrics in practice was a form of finger printing being used in China in the 14th century, as reported by explorer Joao de Barros. He wrote that the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the young children from one another. This is one of the earliest known cases of biometrics in use and is still being used today.

In the 1890s, an anthropologist named Alphonse Bertillion sought to fix the problem of identifying convicted criminals and turned biometrics into a distinct field of study. He developed 'Bertillon age', a method of bodily measurement which got named after him. The problem with identifying repeated offenders was that the criminals often gave different aliases each time they were arrested. Bertillon realized that even if names

changed, even if a person cut his hair or put on weight, certain elements of the body remained fixed, such as the size of the skull or the length of their fingers. His system wasto label and describe individuals. Biometric identification is often categorized as physiological versus behavioral characteristics.

A physiological biometric would identify by one's voice, DNA, hand print or behavior. Behavioral biometrics is related to the behavior of a person, including but not limited to: typing rhythm, gait, and voice. The reasons to adopt the biometrics for security are its completeness, disparateness, permanence and collectability. Main issues to be considered when implementing a biometric system is performance, acceptability, and circumvention.

Used by police authorities throughout the world, until it quickly faded when it was discovered that some people shared the same measurements and based on the measurements alone, two people could get treated as one.

After this, the police used finger printing, which was developed by Richard Edward Henry of Scotland Yard, instead. Essentially reverting to the same methods used by the Chinese for years. However the idea of biometrics as a field of study with useful identification applications was there and interest in it has grown.

1.1 Traditional Approach for Authentication

* **What you know:** Something that the user knows (typically a PIN, a password or aPassphrase) based on something that the user knows and sets it as their password or means to identify the correct user

* **What you have:** Something that the user has (e.g., a key, a token, a magnetic or Smart Card, a badge, a passport). It may be any of the mentioned things which a user carry and use during authentication

1.1.1Drawbacks

Traditional methods are widely used in biometrics but they have certain drawbacks too like the biometric key may be based on properties that can be forgotten, disclosed, lost or stolen.

It is easy to understand the need for biometrics if you've ever forgot or left your network password on your computer. Aside from what's known as "logical" use—using a finger scan or another type of technology to determine if a user is allowed to access information—biometrics can also give appropriate people access to some building or area. There is an increasing need to find a way to solve user identification issues and cut costs for password administration. In some institution like defense or government the employees found it difficult to remember passwords, or occasionally they borrow user names and passwords belonging to other employee—and misused them.[11]

Today we have the technology to realize the aims, and to refine the accuracy of biometric identification, and therefore the possibility of making it a viable field. Due to the increased use of biometric to authenticate or identify people, lead to the increase in use of multimodal fusion so as to overcome the limitations of single-modal biometric system. Multi-modal is a way of combining two biometric modalities into one single wrapped biometric to make a unified authentication decision. The information of the multimodal system can be fused at any of the four modules.

a. Fusion at the sensor level: Over here the data from different level are fused together, can either use samples of same biometric trait obtained from multiple compatible. Over here the data is fused, so there is very less work to do.Used in Fingerprint Palm print and Voice Biometrics.Fusion at multiple level and different data is shown as a block diagram in figure 1.

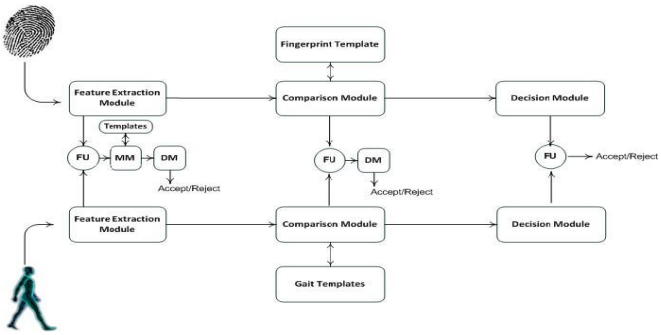


Figure 1: Fusion at sensor level

b. Fusion at the Feature Extraction Level:

Here the data from various sensors are club together. The feature extracted forms the feature vectors are integrated to form a new vector; it can be achieved by single or different algorithm for different modules. It's a challenging task because relationship between features is not known and structurally incompatible features are common and the curse of dimensionality. Refer figure 2.

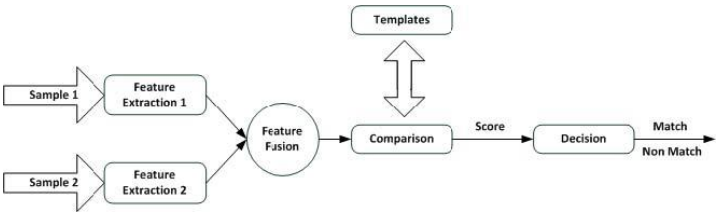


Figure 2 : Fusion at feature extraction level

c. Matcher Score Level:

Here the systems are provided a matching score indicating the proximity of the feature vector with the template vector. The combination of score helps us to identify the clamed identity. These scores contain the richest information about the input. Also it is quite easy to combine the scores of different biometrics so lot of work has been done in this field.See figure 3

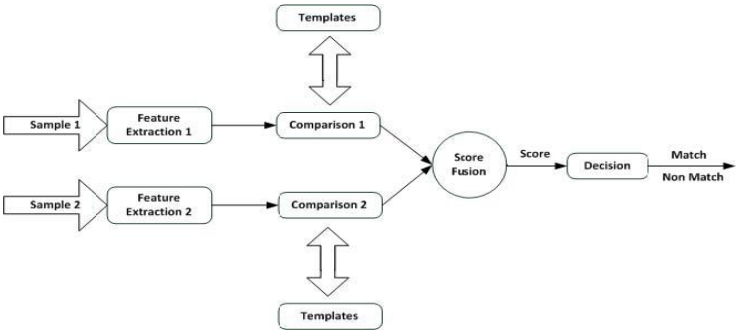


Figure 3: score level matcher

d. Fusion at the Decision Level:

The final outputs of the multiple classifiers are combined. A majority vote scheme can be used to make final decision. Decision level fusion includes very abstract level of information so they are less preferred in designing multimodal biometric systems. Fusion at the matching-score level is the most popular and frequently used method because of its good performance, intuitiveness and simplicity.

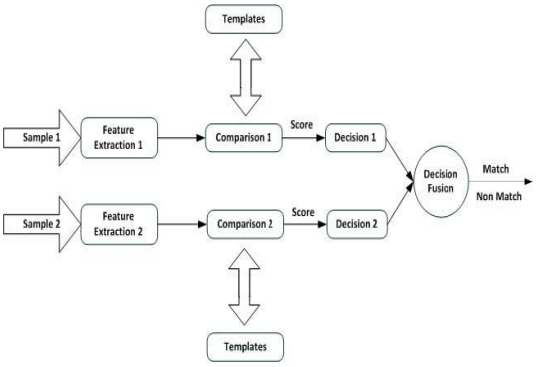


Figure 4: decision level fusion

Sometimes biometric authentication systems replace traditional authentication systems not because of higher security but because of higher comfort and ease of use.

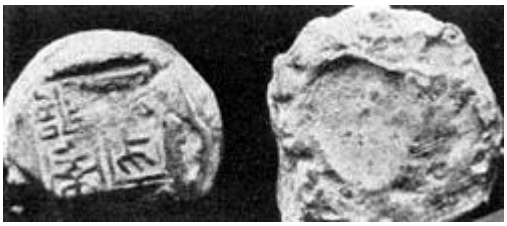
A typical biometric system is comprised of five integrated components: A **sensor** is used to collect the data and convert the information to a digital format. **Signal processing algorithms** perform quality control activities and develop the biometric template. A data storage component

keeps information that new biometric template will be compared to. A **matching algorithm** compares the new biometric template to one or more templates kept in data storage. Finally a decision process uses the result from matching component to make a system level decision.

2.0 History of biometrics

Possibly the first known example of biometrics in practice was a form of finger printing being used in China in the 14th century, as reported by explorer Joao de Barros. He wrote that the Chinese merchants were stamping children's palm prints and footprints on paper with ink to distinguish the young children from one another. This is one of the earliest known cases of biometrics in use and is still being used today.[12]

Picture writing of a hand with ridge patterns was discovered in Nova Scotia. In ancient Babylon, fingerprints were used on clay tablets for business transactions. In ancient China, thumb prints were found on clay seals.



In 14th century Persia, various official government papers had fingerprints (impressions), and one government official, a doctor, observed that no two fingerprints were exactly alike.

1686 - Malpighi

In 1686, Marcello Malpighi, an anatomy professor at the University of Bologna, noted fingerprint ridges, spirals and loops in his treatise. He made no mention of the value of fingerprints for human identification. A layer of skin was named after him; "Malpighi" layer, which is approximately 1.8mm thick.

1858 - Herschel

The English first began using fingerprints in July of 1858, when Sir William James Herschel, Chief Magistrate of the Hooghly district in Jungipoor, India, first used fingerprints on native contracts. On a whim, and without thought toward personal identification, Herschel had RajyadharKonai, a local businessman; impress his hand print on a contract. Figure 5

Figure 5: Local businessman handprint

The idea was merely "... to frighten [him] out of all thought of repudiating his signature." The native was suitably impressed, and Herschel made a habit of requiring palm prints--and later, simply the prints of the right Index and Middle fingers--on every contract made with the locals. Personal contact with the document, they believed, made the contract more binding than if they simply signed it. Thus, the first wide-scale, modern-day use of fingerprints was predicated, not upon scientific evidence, but upon superstitious beliefs.

As his fingerprint collection grew, however, Herschel began to note that the inked impressions could, indeed, prove or disprove identity. While his experience with fingerprinting was admittedly limited, Sir William Herschel's private conviction that all fingerprints were unique to the individual, as well as permanent throughout that individual's life, inspired him to expand their use.[13]

1882 - Thompson

In 1882, Gilbert Thompson of the U.S. Geological Survey in New Mexico used his own thumb print on a document to help prevent forgery. This is the

first known use of fingerprints in the United States. Click the image below to see a larger image of an 1882 receipt issued by Gilbert Thompson to "Lying Bob" in the amount of 75 dollars.

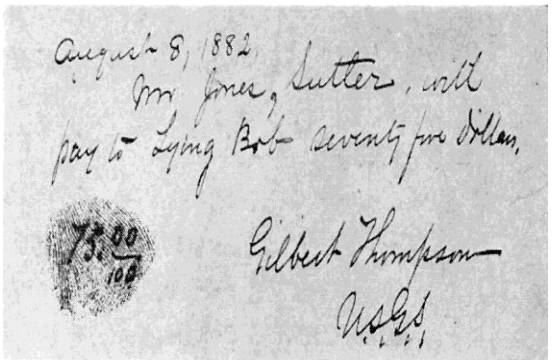


Figure 6: Thumbprint to prevent forgery

1882 Bertillon

Alphonse Bertillon, a Clerk in the Prefecture of Police of at Paris, France, devised a system of classification, known as Anthropometry or the Bertillon System, using measurements of parts of the body. Bertillon's system included measurements such as head length, head width, length of the middle finger, length of the left foot; and length of the forearm from the elbow to the tip of the middle finger.

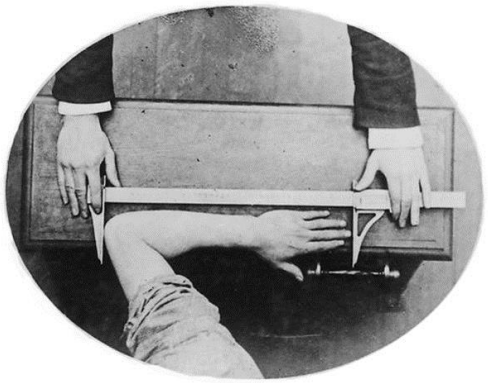


Figure 7: Bertillon's system measurements

3.0Biometric security:

3.1 Stages in biometric security

3.1.1 Measurement (acquisition)

It is the 1st stage of Biometric security. In this stage user contact with the biometric system for the first time. The User's biometric sample is obtained using an input device depending on the type of input system works on. Quality of the First biometric sample is very crucial for further authentications of this user.

3.1.2 Creation of master characteristics:

Measurements are processed as the second step after the acquisition. The number of biometric samples necessary for further processing is based on the nature of given biometric technology. Sometimes a single samples sufficient, but often multiple (usually 3 or 5) biometric samplesare required. The biometric characteristics not so common isneither compared nor stored in the raw format (say as a bitmap).

3.1.3 Storage of master characteristics:

For improved identification in databases with several records, choosing proper discriminating characteristics act as a key for the categorization in improve identification (search). After processing the first biometric sample(s) and extracting the features, it is the time to create a new template on the base of data extracted. This template is stored and maintained
There are basically 4 possibilities where to store the template:

1. A card
2. Central database
3. Workstation
4. Authentication terminal

3.1.4 Authentication:

For judging the originality of the user Current biometric measurements must be obtained. It is then passed to the system so as it can make proper comparison with master template.
In many biometric techniques (e.g., fingerprinting) the further processing trusts the biometric hardware to check the aliveness of the person.

3.1.5 Comparison:

This is the step where actual comparison is made between the currently computed characteristics and the characteristics obtained during enrolment. If the system performs identity verification then only these newly obtained characteristics are compared to the master template.

3.1.6 Decision

The final step in the verification process is the yes/no decision based on a threshold. This decides whether the user is the person who is authorized for the access. If yes he may proceed further else is declined to access the system/data. For an efficient biometric system false reject rate should be low.

3.2 Advantages of biometric authentication:

Following are the advantages of biometric system:

1. These methods use real human physiological or behavioral characteristics to authenticate users.
2. These biometric characteristics are (more or less) permanent and not changeable.
3. Users cannot pass their biometric characteristics to other users as easily as they do with their cards or passwords.
4. Biometric objects cannot be stolen as tokens, keys, cards or other objects used for the traditional user authentication.
5. Most biometric techniques are based on something that cannot be lost or forgotten.
6. Another advantage of biometric authentication systems may be their speed.

3.3 Disadvantages of biometric authentication:

1. Biometric characteristics can be stolen from computer systems and networks.
2. Biometric systems still need to be improved in the terms of accuracy and speed.
3. Biometric systems with the false rejection rate under 1% (together with a reasonably low false acceptance rate) are still rare today.
4. Although few biometric systems are fast and accurate (in terms of low false acceptance rate) enough to allow identification
5. The fail to enroll rate brings up another important problem.
6. Not all users can use any given biometric system. Like People without hands cannot use fingerprint or hand-based systems. Similarly visually impaired people have difficulties using iris or retina based techniques.
7. As not all users are able to use a specific biometric system, the authentication system must be extended to handle users falling into the FTE category.
8. Some biometric sensors (particularly those having contact with users) also have a limited lifetime. While a magnetic card reader may be used for years (or even decades), the optical fingerprint reader (if heavily used) must be regularly cleaned and even then the lifetime need not exceed one year.
9. Biometric systems can potentially be quite troublesome for some users as they find some biometric systems intrusive or personally invasive.
10. Even if no biometric system is really dangerous, users are occasionally afraid of something they do not know much about.
11. In some countries people do not like to touch something that has already been touched many times (e.g., biometric sensor), while in some countries people do not like to be photographed or their faces are completely covered.

4.0 RETINAL SCAN

Retina is a photo-sensitive layer of tissues, lining of the inner surface of the eye. The optics of the eye creates an image of the world on the retina; its function can be considered as analogous to the function of film in a camera. It is made up of neural cells. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. Since infrared energy is absorbed faster by blood vessels in the retina than by surrounding tissue, it is used to illuminate the eye retina. The network of blood vessels in the retina is so complex that even identical twins do not share a similar pattern. Retinal scanning is highly accurate and its error rate is estimated to be only one in a million.

Drawbacks: Although retinal patterns may be altered in cases of diabetes, glaucoma or retinal degenerative disorders.

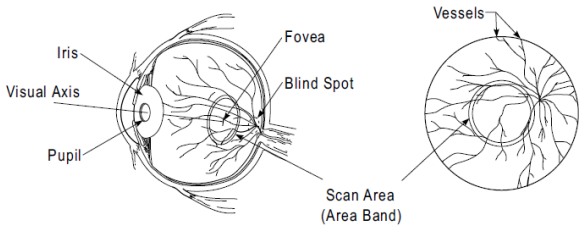


Figure 8: Structure of Human Eye[1]

Dr. Carleton Simon and Dr. Isadora Goldstein, two ophthalmologists for the first time ever gave an idea of retina scanning for identification but it was Robert Buzz Hill, who applied the idea into concept of retina recognition by a device in 1975. He formed a corporation *EyeDentify, Inc.*, which released first ever retina scanner device in 1981. [2][5]

4.1Method of Retinal Scan

Retina recognition is performed by analyzing the unique blood vessels on the retina which differs for every person. These blood vessels are light absorbent. So when a beam of light is passed through the retina, the light is reflected with varied spots. A low intensity light source is utilized in order to scan the vascular pattern at the retina. This involves a 360 degree circular scan of the area taking over 400 readings in order to establish the blood vessel pattern. These varied patterns of light are collected and coded as a template and used for enrollment and verification. Robert Buzz Hill in his article, *Retina Identification* calls this pattern variation as Eye Signature.[1]

Retina-scan technology possesses robust matching capabilities and is usually configured to do one-to-many identification against a database of users, however, this technology requires a high quality image and will not enroll a user unless a good image is acquired. For this reason, there is a moderately high false reject rate due to the inability to provide adequate data to generate a match template.[7]

EyeDentify Inc. introduced its first retina capturing devices were known as 'fundus cameras'.
First, the equipment was considered very expensive and difficult to operate. Second, the light used to illuminate the retina was considered too bright and too discomforting for the user.[6]

4.2Properties of Retinal Scan

- **Acceptability:**Retina recognition has one of the most low acceptability issues among general public. There is a common apprehension that retina scanning may affect the eye.[2]

- **Collectability:**Not so user friendly as compare to other recognition technologies. A user has to wait for a reasonable time to get his eye scanned and he has to move his eye very close to the scanning camera. [5]it has to do be done without eye glasses. [2][5]

- **Uniqueness:**It is one of the best methods, when it comes to the accuracy and uniqueness.[1]

- **Performance:**Highly accurate with almost zero false accepting rate.[1]

4.3Retinal Scanning Process

The overall retinal scanning process may be broken down into three sub-processes:
1. Image/signal acquisition and processing -this sub-process involves capturing an image of the retina and converting it to a digital format.
2. Matching: a computer system is used to verify and identify the user (as is the case with the other biometric technologies reviewed in previous articles).
3. Representation: the unique features of the retina are presented as a template.

The process for enrolling and verifying/identifying a retinal scan is more or less the same as the process applied by any other biometric technologies. This allows up to 400 unique data points to be obtained from the retina. For other biometrics, such as fingerprints, only 30-40 data points (the minutiae) are available.[6]

The strengths and weaknesses of retinal recognition
Just like all other biometric technologies, retinal recognition has its own unique strengths and weaknesses. The strengths may be summed up as follows:
1. The blood vessel pattern of the retina rarely changes during a person's life (unless he or she is afflicted by an eye disease such as glaucoma, cataracts, etc).
2. The size of the actual template is only 96 bytes, which is very small by any standards. In turn, verification and identification processing times are much shorter than they are for larger files.
3. The rich, unique structure of the blood vessel pattern of the retina allows up to 400 data points to be created.
4. As the retina is located inside the eye, it is not exposed to (threats posed by) the external environment. For other biometrics, such as fingerprints, hand geometry, etc., the opposite holds true.

The most relevant weaknesses of retinal recognition are:

1. The public perceives retinal scanning to be a health threat; some people believe that a retinal scan damages the eye.
2. User unease about the need to position the eye in such close proximity of the scanner lens.
3. User motivation: of all biometric technologies, successful retinal scanning demands the highest level of user motivation and patience.
4. Retinal scanning technology cannot accommodate people wearing glasses (which must be removed prior to scanning).
5. At this stage, retinal scanning devices are very expensive to procure and implement.

4.4Pros and cons

- **Pros**

- Almost zero false accepting rates.
- Low (almost 0%) false negative rates.
- Highly reliable as no two people have the same retinal pattern not even identical twins.
- Identification of the person is verified very quickly.

- **Cons**

- Measurement accuracy can be affected by a disease such as cataracts or by by severe astigmatism.
- Scanning procedure is perceived by some as invasive
- Not regarded as very user friendly
- Expensive.

4.5Conclusion

In view of the rich and unique blood vessel patterns in the retina, there is no doubt that retinal recognition is the 'ultimate' biometric. Its high cost and user-related drawbacks have prevented it from making a commercial impact. However, as technology continues to advance, it seems likely that retinal recognition will one day be widely accepted and used.

5.0 Face recognition

Process to identify the face of individual from a digital image or a video frame from a video source is called face recognition. Its use in identification and verification made it popular among the no of projects that may be of private or public sector. In this system the image captured from camera are broadly classified into static and dynamic matching which is known as *probe image*. In this nodal points are measured on the face such as distance between eyes, shape of the cheekbones and other distinguishable features. These nodal points are then matched to database in computer to find the match. This process can be achieved with the help various algorithms. Initially simple

geometric models where use but due to advancement in scientific innovation the face recognition came into spotlight which introduce several algorithm for this.

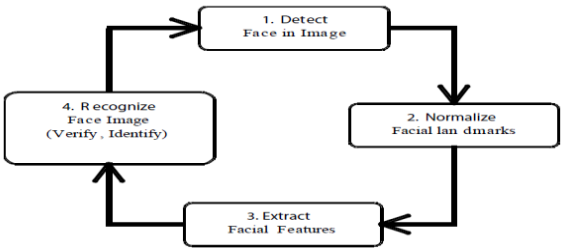


Figure 9: Loop chart for identification [9]

In 1960's first semi automated facial recognition was greeted by woody Bledsoe Helen Chan Wolf, and Charles Bison. The program developed by them require the administrator to locate feature eyes, ears, nose, and mouth on the photograph which calculate distances and ratio to a common reference point which was then compared to reference data. Where as in 1970's Goldstein, Harmon, and Lesk used 21 markers such as hair color and lip thickness, to automate the recognition which required human labor too. With further advancement in 1988 Kirby and Sirovich used principle component analysis, a standard linear algebra technique, to the face recognition problem. Now in 1991 Turk and Pent land discovered Eigen faces techniques discovery that enabled reliable real-time automated face recognition systems.

5.1Process of facial recognition

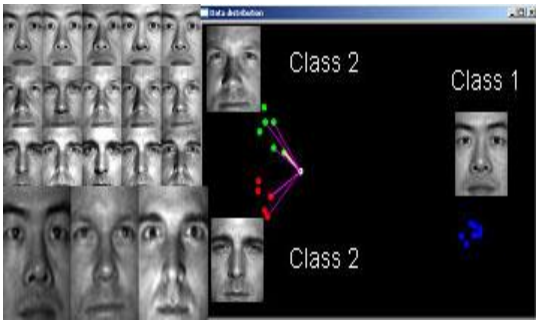
There are two basic technique for face recognition problem ie geometric (feature base) and photometric (view based). With the future studies in this field gave emergence to three basic algorithms they are: Principal Components Analysis (PCA), lineardiscriminant Analysis (LDA), and Elastic Bunch Graph Matching (EBGM). **[10]**

5.1.1 Principal Components Analysis (PCA)

Use Eigen faces technology. Here the probe and gallery image have to be of same size where firstly the target image is normalized to line up eyes and mouth. Then the data compression take place where the most efficient and low dimension record is retrieve, which have only orthogonal values(Eigen faces) and all the unwanted information are removed where the image is represented as weighted sum and stored in the form of 1-D array. The approach require full frontal image for optimal performance. The primary importance of this approach is it reduces the size of data.

5.1.2 Linear Discriminant Analysis (LDA)

It's a static approach which classifies the data into samples of classes based on the training samples with known classes which aim to maximize between-class (across user) variance and minimize within-class(within user) variance as shown in the figure below. as shown there is very little variation with in the class but a high degree of variation between two classes. In high dimensional data it is only applicable for small set of data.



5.1.3 Elastic Bunch Graph Matching (EBGM).

This concept shows the real face concept which has many non linear characteristics such as variation in illumination (outdoor light vs. indoor light), pose (straight vs. Leaning) and expression (smile vs. Brimming with anger) which are non linear in nature. The Gabor jet create a dynamic link architecture which projected the face onto an elastic grid, it's a node on elastic grid which describe the behavior around a given pixel. So it results in convolution of image either a Gabor

filter, use for detecting shape and extra feature using image processing. It's difficult to landmark locations which can be achieved by LDA and PCA.

5.2Pros and Cons of facial recognition

- **Pros**

- Anywhere that you can put a camera, you can potentially use a facial recognition system. Many cameras can be installed throughout a location to maximize security coverage without disrupting traffic flow.
- Face recognition systems can be installed to require a person to explicitly step up to a camera and get their picture taken, or to automatically survey people as they pass by a camera. The later mode allows for scanning of many people at the same time
- Video or pictures can be replayed through a facial recognition system for surveillance or forensics work after an event.
- Face scanning is not noticeable, can be done at a comfortable distance and does not require the user to touch anything.

- **Cons**

- Such systems may be fooled by hats, beards, sunglasses and face masks
- Even changes of lighting and camera angle can have a significant effect on the accuracy of 2D systems
- Some people view mass-scale facial recognition cameras as the ultimate "big brother

5.3Conclusion

Due to increasing in business to replace the expensive man-guard we require a system which has high level of security and can perform the work of verification in a second or less so the face recognition biometric system is one of the solution. It is also helpful to intelligence department to identify the criminals. Using the latest in infrared technology, face recognition systems can enroll and verify operatives in bright sunlight, pitch darkness, or anywhere in between.

6.0 Fingerprint:

Fingerprint recognition is one of the oldest means used for the identification of a person. In ancient times finger marks where taken on clay, finger prints were also used in bonds as it was the best suited proof for a person's willingness.

With the advancements of technology these methods transformed to an automated systems which is widely used these days. The unique pattern of ridges, furrows& minutiae are obtained and a finger print is obtained.[4] These fingerprints obtained are scanned and it form a black (result of ridges) and white (furrows) image. Minutiae points are extracted from the patterns and then applying certain algorithms these are converted in a template and then stored in database. It is very strong, simple and effective biometrics information stored using this technique is encoded with a strong algorithm and in most of the cases no actual image formation of fingerprints is made.

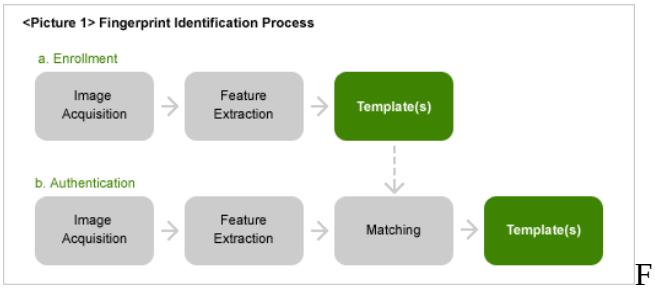


Figure 10: Fingerprint identification process

Since many users fingerprints are used for identification of peoples. Below is a brief chronological history:-[8]

- 1858: A British administrator sir William Herschel in a district in India required fingerprint for civil contracts.
- 1880: NATURE, A scientific journal was published discussing fingerprints for identification purpose obtaining with the help of ink
- 1882: Bertillion gave a formula taking measurements of persons body part and storing it on a card. This system is named after him and called as Bertillion system
- 1883: Mark twain in his book, life on the Mississippi, a murderer was identified with the help of fingerprint
- 1891: Juan vucetich, Argentine police official initiated fingerprints for criminals
- 1892: Sir Francis Galton published 1st book on fingerprints. In the same year Juan Vecitich made the first criminal finger identification of a mother who killed her 2 sons and then cut her own throat. She was identified by her bloody print on a door post.
- 1896: IACP establish national bureau of criminal identification.
- 1901: 1st system of classifying fingerprints was developed by Sir Edward henry, an inspector general of police in Bengal, India.
- 1903: After 1903 many prisoners system began to use fingerprint identification as the primary means to identify peoples. The Illinois supreme court citied the historical research and use of fingerprints as a means of reliable identification in upholding the conviction and thus establishing the use of fingerprints as a reliable means of identification.
- 1905: fingerprints were adopted by U.S military which was later adopted by police agencies too.
- 1908: 1st official fingerprint card was developed.
- 1917: palm print identification was made for the 1st time in Nevada.
- 1924: ID division of FBI was formed
- 1980: Automated fingerprint identification system (AFIS) the 1st computer database pf fingerprints was developed.

6.1Principles of fingerprint recognition

Finger print can be obtained using different techniques which is established on different principles such as optical, ultrasonic and capacitance.[3] They are discussed below:

- **Optical:**Optical methods use the concept of visible light for taking finger prints. Finger is placed on the sensor(usually of glass), beneath this there is a light emitting phosphor layer which illuminates the surface of the finger. The reflected light from the finger is captured as a visual image of the finger print. The quality of finger prints may vary from skin to skin as different people have different types of skin and so the clarity may vary. A dirty or scratched skin gives a bad image.
- **Ultrasonic:**This scanning technique is based on principle of medical ultrasonography. High frequency sound wave is produced with the help of piezoelectric transducers which is expelled on finger and the reflection is captured in the form of image. This overcomes the demerits of optical scanning.
- **Capacitance:** Similar to capacitor the sensors are arranged as parallel plate capacitors in which one plate electrically

conductive is dermal layer and the other one act as dielectric. Image formed in this case is the result of principle of capacitance.

After scanning is performed finger prints obtained are classified into different types. Classification of finger prints is made to collect similar type of prints in a same category. Classes of finger prints are named on the pattern of prints they have. Whorl, right loop, left loop, arch, and tented arch are different types of classes we put them into. These are some examples of different types of finger prints known in figure 11

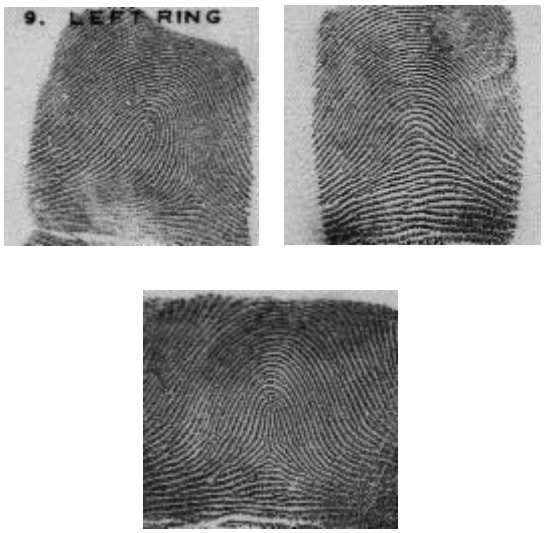


Figure 11: Different types of finger prints

A question may arise that though all the finger prints extracted form a template is formed then why it is needed to classify their classes. These are very much essential for companies which have a large base. FBI approximately has 70 million fingerprints in their database. In this case searching may be slow and will increase the response time for the system. Therefore we classify all of them into certain classes and match the test print among the class in belongs to.

6.2Process of Fingerprint recognition

An image of finger is obtained using machine based any of the above principles. Instead of using a complete picture for reference only some unique features are extracted.
A template is formed and stored in the database. When a finger print is provided for verification it is compared with the template stored in the database. If the features is matched with template user is allowed for access else rejected.

6.3Pros and cons

- **Pros**
- Fast
- Accurate
- Uses Less memory
- Can be easily deployed
- Cheap to install
- Simple
- Unique feature

- **Cons:**
- Old method
- Acceptation rate varies with machine used
- Slight complex dealing with cut skin

6.4Conclusion:

Since it's very cheap and efficient it is one of the most used systems. The main reason for the popularity of fingerprint identification system is its simplicity along with reliability at low cost without compromising with security.

7.0 Soft Biometrics

Soft Biometrics such as weight, gender, colorsetc. are used with Primary Biometrics for improvement in Response Time.
Biometric measurements on the basis of Anthropometric measurement (height and length

of the arm), morphological description (appearance and body shape like eye color and anomalies of the fingers) and peculiar marks (like moles and scars) may be collectively referred to as soft biometrics. This type of biometrics may distinguish people but is not strong enough to rely completely on it. The 1st personal identification was based on these features only for identification of criminals. Inspite of these systems where useful in identifying criminals it had high error rate. These features may be common and may change with time so personal attributes like age, gender, eye color, height and other visible identifications if applied on a system alone it will not be accurate enough and its scope will be limited. Therefore it may be used with traditional biometrics contributing to far more efficient systems. It was noticed that when this features where used with finger print recognizer the efficiency of the system was improved by 5%.

Why do we basically use soft biometrics?? The answer is very simple. The identification or validation time of these type of system is more than that of traditional systems since it s based on geometry which is an easily calculative feature. The identification process is categorized in three levels. Level 1 level 2 and level 3. They run in a sequence and proceeds to next level only if one level is cleared otherwise process is terminated
Level 1- in this level comparing and matching of biometric trait weight is checked. if the weight matches we proceed to level 2
Level2- Geometry is compared and matched
Level3- after geometry is successfully matched at level 3 there is a minute feature matching done to finally identify the user
If any of the level fails the process stops there itself.

7.1 SOFT BIOMETRIC EXTRACTION

Soft biometric systems provide an ease to extracts features. in this test user need not to interact with the system, they are extracted automatically say with the help of infrared beam and therefore feature extraction is very comfortable for a user. The user only needs to interact with primary biometric system. These features help the Primary system to take decisions more accurately and efficiently

7.2FUTURE PROSPECTUS OF SOFTBIOMETRICS

The reason to use such type of biometrics with the primary system is just to advance the effectiveness of the base system. On the one hand the system becomes more calculative but on the other side it alters or shortens the no of matches which is to be made by the system resulting in the overall effective working of the system.
Definitely it increases the cost and the data size but also advances the level of identification which may be more reliable minimizing the response time and False Acceptance Rate (FAR). Therefore thinking with security and accessibility point of view the extra costisbearable.
Utilizing various measures and identifications also increase the scope of the system and strengthens its power to Authenticate. Hence integrating temporary or not so reliable identifying features with a base system is not a bad idea and used widely.

7.3 Key benefits:

Low false acceptance rate
Minimizing time of authentication
Matches needed to be compared are less
Improved response time
Increase in accuracy
Efficiency may be increased to a far extent
Results in more reliable system
Convenience of the user as they may not have to pass any new test it is automated

7.4 Drawbacks:

The system has some drawbacks too like:

- Extra space required
- Increase in complexity
- More computational task for the system
- Cost of the system increases
- May be sometime difficult to deploy in certain area
- Quality of camera effects identification so is dynamic at different places

Multimodal System Using Retinal Scan, Fingerprints Matching, Face Recognition and Soft

Biometrics.To overcome the drawback of aunimodal biometric system researchers came up with the idea of multimodal system. A multimodal system which has fingerprint matching, retinal scan, face recognition using soft biometrics could be highly efficient and user friendly. We purpose face recognition to be the first step of this authenticating process. This is due to the fact that it has some disadvantages such as it does not work well include poor lighting, sunglasses, long hair, or other objects partially covering the subject's face, and low resolution images. Another serious disadvantage is that many systems are less effective if facial expressions vary. Even a big smile can render the system less effective (Wikipedia). It can be considered as weakest process of identification as we compare it with retinal scan technology and fingerprint matching technology. If this process fails to generate correct output for a genuine user the system shifts to next steps of authentication that is fingerprint matching and retinal scan. Both of the latter techniques are fool-proof. Every individual in the world has unique retinal pattern and fingerprints. Even identical twins do not share these features as common.

Now we propose biometric system which comprises of Fingerprint, Retina and Facial Recognition technology. Let us consider individual outputs of these three technologies in every case possible.

FP=0; result of fingerprint scan if fingerprints of user trying to authenticate himself do not matches.
FP=1; result of fingerprint scan if fingerprints of user trying to authenticate himself matches.
RS=0; result of retinal scan if retinal scan of user trying to authenticate himself do not matches.
RS=1; result of retinal scan if retinal scan of user trying to authenticate himself matches.
FR=0; result of face recognition process if system do not recognizes the user trying to authenticate himself.
FR=1; result of face recognition process if system recognizes the user trying to authenticate himself.
As we know output of any biometric authentication process is either 0 or 1, which corresponds to the fact that user is not authenticated and user has not been authenticated respectively. In our system we fuse the outputs of the different stages (that are different unimodal authenticating techniques). In ideal situation (where a genuine user gives his biometric inputs correctly as he has given at the time of enrollment) the "logical and" of all three output should come as 1 i.e. User is authenticated. So here arises a question is it always necessary that the biometric system has to compute output for all three biometric techniques? Multimodal system described in this paper need not to perform calculation for outputs of all three techniques. We start by considering outputs of fingerprint matching and facial recognition. To authenticate a "logical and" of the output should be "1". But what if problems described above with facial recognition occur. In such a case the system would not identify even a genuine use.

Under that condition we take in consideration of output of fingerprint scan and retinal scan and perform "logical or". If the output comes out as true then user is authenticated otherwise not. As any one of the techniques described above could identify a person.

Now question arises what is the need of soft biometrics when we have got such a reliable and efficient system. The basic purpose of soft biometrics is to "partially" identify a person. Partially here means that soft biometrics alone cannot identify a person. It plays a supporting role to the primary biometrics. It filters the database on the basis of certain criteria and output is a pool of lesser number of probable users that can access the system. It leads to increase in efficiency of the system and decrease in response time. In an organization having a large database such technique can be extremely benefit able. Though there are some disadvantages also. Such a high speed and quick response system comes at the cost of expensive hardware support and efficient algorithms to filter the database.

8.0 Conclusion

In this research paper we have discussed the analysis and shortcomings of fingerprints, retina image and facial recognition based multimodal systems with soft biometric support. Unimodal biometric system can identify a person but by

using a multimodal biometric system we simply improves efficiency of it. A multimodal system e.g. fingerprints, retina image and facial recognition give better matching results in comparison to single feature based systems in terms FRR, FAR. Error rate can never be zero as there are always some software and hardware difficulties at some point of time, but a flexible multimodal system gives a better matching score then any multimodal system.

9.0 References:

[1]Biometrics-Evaluation of current Situation Master Thesis performed in Information Coding Group by Salman Zahidi: http://ufdcimages.uflib.ufl.edu/UF/E0/00/26/62/00001/hitchcock_d.pdf

[2]Hill Robert, Retina Identification, http://www.cse.msu.edu/~cse891/Sect601/textbook/6.pdf

[3]http://en.wikipedia.org/wiki/Fingerprint_recognition

[4]http://www.hrsid.com/finger-recognition

[5]Retinal scan, http://en.wikipedia.org/wiki/Retinal_scan.

[6]Biometric technology in practicably Ravi Das http://www.biometricnews.net/Publications/Biometrics_Article_Retinal_Recognition.pdf

[7]SANS Institute InfoSec Reading Room: http://www.sans.org/reading_room/whitepapers/authentication/biometric-scanning-technologies-finger-facial-retinal-scanning_1177Ibid. p. 111.

[8]http://www.crimescene-forensics.com/History_of_Fingerprints.html

.

[9]http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm

[10]Smith, Kelly. "Face Recognition" (PDF). Retrieved 2008-06-04

[11]http://biometrics.pbworks.com/w/page/14811351/Authentication%20technologies#WHYDOWENEEDIT

[12]http://www.biometrics.gov/documents/biohistory.pdf

[13]http://onin.com/fp/fphistory.html