An Overview of Leading Biometrics for Human Identity

S.Sumathi ¹ and R.RaniHema Malini ².
¹Research Scholar,Sathyabama University,Chennai-96
²Professor& Head, Dept of E&I, St.Peter’s University,Chennai-54.
¹sumathi_ba@rediffmail.com and ²ranihema@yahoo.com

ABSTRACT
Biometrics the term covers a wide range of technologies that can be used to identity and verify the person by measuring and analyzing human characteristics. Most of the system requires personal reliable recognition systems to confirm or determine the identity of an individual who require particular service. Main aim is to ensure that service accessed only by legitimate user not others. Most person recognition systems limit themselves to only a single modality. The latest research indicates using a combination of biometric avenues for human identification is more effective, and far more challenging. Since there are number of biometric methods in use, here we discuss some new methods as heart sound, finger knuckle print, dental be used as reliable biometrics.

KEYWORDS
Biometrics, dental, finger knuckle print, heart Sound, Identification, verification.

1. INTRODUCTION
From early days body characteristics are used to recognize the person. By using biometrics it is possible to establish an identity based on “who he is,” rather than by “what he possess” (for example, an ID card) or “what he remember” (for example, a password). Any human physiological or behavioral characteristic that is universal, unique, permanent, and collectable could be used as a biometric Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person. However, in a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a number of other issues that should be considered, including: [1,2]

• Performance, which refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognitions well as the operational and environmental factors that affect the accuracy and speed;
• Acceptability, which indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives;
• Circumvention, which reflects how easily the system can be fooled using fraudulent methods.

A practical biometric system should meet the specified recognition accuracy, speed, and resource requirements, be harmless to the users, be accepted by the intended population, and be sufficiently robust to various fraudulent methods and attacks to the system.

Biometric traits can be split into two main categories:
Physiological Biometrics: It is based on direct measurements of a part of the human body. Fingerprint, face, iris, and hand-scan recognition belong to this group.
Behavioral Biometrics: It is based on measurements and data derived from an action performed by the user, and thus indirectly measures some characteristics of the human body. Signature, gait, gesture, and key stroking recognition belong to this group.

Biometrics can offer greater security and convenience than traditional methods for people recognition. Even if we do not want to replace a classic method (password or handheld token) by a biometric one, for sure, we are potential users of these systems, which will even be mandatory for new passport models. For this reason, it is useful to be familiarized with the possibilities of biometric security technology.

2. BIOMETRIC SYSTEMS
A biometric system is essentially a pattern-recognition system that recognizes a person based on a feature vector derived from a specific physiological or behavioral characteristic that the person possesses. Depending on the application context, a biometric system typically operates in one of two modes: verification or identification. Authentication (or verification) is closely related to recognition (or identification). In identification mode, the system recognizes an individual by searching the entire template database for a match. The system conducts a one-to-many comparison to establish an individual’s identity. In verification mode, the system validates a person’s identity by comparing the captured biometric characteristic with the individual’s biometric template, which is prestored in the system database. The system conducts a one-to-one comparison to confirm an individual’s identity. However, the evaluation criteria for identity recognition are different from those used in authentication systems. The performance of identity recognition systems is quantified in terms of the cumulative match score, i.e., the percentage of correctly identified subjects within the N best matches versus N.

A simple biometric system consists of four basic components:
1) Sensor module which acquires the biometric data;
2) Feature extraction module where the acquired biometric data is processed to extract a set of salient or discriminatory
features. For example, the position and orientation of minutiae points (local ridge and valley singularities) in a fingerprint image are extracted in the feature extraction module of a fingerprint-based biometric system.

3) **Matching module** in which the features extracted during recognition are compared against the stored templates to generate matching scores. For example, in the matching module of a fingerprint-based biometric system, the number of matching minutiae between the input and the template fingerprint images is determined and a matching score is reported. The matcher module also encapsulates a decision making module, in which a user’s claimed identity is confirmed (verification) or a user’s identity is established (identification) based on the matching score.

4) **System database module**, which is used by the biometric system to store the biometric templates of the enrolled users. The enrollment module is responsible for enrolling individuals into the biometric system database. During the enrollment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a digital representation of the characteristic. The data capture during the enrollment process may or may not be supervised by a human depending on the application. A quality check is generally performed to ensure that the acquired sample can be reliably processed by successive stages. In order to facilitate matching, the input digital representation is further processed by a feature extractor to generate a compact but expressive representation, called a template. Depending on the application, the template may be stored in the central database of the biometric system or be recorded on a smart card issued to the individual. Usually, multiple templates of an individual are stored to account for variations observed in the biometric trait and the templates in the database may be updated over time.

3. **OVERVIEW OF COMMONLY USED BIOMETRICS**

Since there are number of biometric methods in use, a brief overview of various biometric characteristics will be given, starting with newer technologies and then progressing to older ones, here we discuss some new methods as heart sound, finger knuckle print, dental be used as reliable biometrics.

**Infrared thermogram (facial, hand or hand vein).** It is possible to capture the pattern of heat radiated by the human body with an infrared camera. That pattern is considered to be unique for each person. It is a noninvasive method, but image acquisition is rather difficult where there are other heat emanating surfaces near the body. The technology could be used for covert recognition. A related technology using near infrared imaging is used to scan the back of a fist to determine hand vein structure, also believed to be unique. Like face recognition, it must deal with the extra issues of three-dimensional space and orientation of the hand. Set-back is the price of infrared sensors.

**Gait.** This is one of the newer technologies and is yet to be researched in more detail. Basically, gait is the peculiar way one walks and it is a complex spatio-temporal biometrics. It is not supposed to be very distinctive but can be used in some low-security applications. Gait is a behavioral biometric and may not remain the same over a long period of time, due to change in body weight or serious brain damage. Acquisition of gait is similar to acquiring a facial picture and may be an acceptable biometric. Since video-sequence is used to measure several different movements this method is computationally expensive.

**Keystroke.** It is believed that each person types on a keyboard in a characteristic way. This is also not very distinctive but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioral biometric; for some individuals, one could expect to observe large variations in typical typing patterns. Advantage of this method is that keystrokes of a person using a system could be monitored unobtrusively as that person is keying information. Another issue to think about here is privacy.

**Odor.** Each object spreads around an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. This would be done with an array of chemical sensors, each sensitive to a certain group of compounds. Deodorants and perfumes could lower the distinctiveness.

**Ear.** It has been suggested that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive. Matching the distance of salient points on the pinna from a landmark location of the ear is the suggested method of recognition in this case. This method is not believed to be very distinctive.

**Hand geometry.** The essence of hand geometry is the comparative dimensions of fingers and the location of joints, shape and size of palm. One of the earliest automated biometric systems was installed during late 60s and it used hand geometry and stayed in production for almost 20 years. The technique is very simple, relatively easy to use and inexpensive. Dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy. Since hand geometry is not very distinctive it cannot be used for identification of an individual from a large population, but rather in a verification mode.

Further, hand geometry information may not be invariant during the growth period of children. Limitations in dexterity (arthritis) or even jewelry may influence extracting the correct hand geometry information. This method can find its commercial use in laptops rather easy. There are even verification systems available that are based on measurements of only a few fingers instead of the entire hand. These devices are smaller than those used for hand geometry.

**Fingerprint.** A fingerprint is a pattern of ridges and furrows located on the tip of each finger. Fingerprints were used for personal identification for many centuries and the matching accuracy was very high. Patterns have been extracted by creating an inked impression of the fingertip on paper. Today, compact sensors provide digital images of these patterns. Fingerprint recognition for identification acquires the initial
image through live scan of the finger by direct contact with a reader device that can also check for validating attributes such as temperature and pulse. Since the finger actually touches the scanning device, the surface can become oily and cloudy after repeated use and reduce the sensitivity and reliability of optical scanners. Solid state sensors overcome this and other technical difficulties because the coated silicon chip itself is the sensor. Solid state devices use electrical capacitance to sense the ridges of the fingerprint and create a compact digital image. In real-time verification systems, images acquired by sensors are used by the feature extraction module to compute the feature values. The feature values typically correspond to the position and orientation of certain critical points known as minutiae points. The matching process involves comparing the two-dimensional minutiae patterns extracted from the user's print with those in the template. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources.

**Face.** Facial images are the most common biometric characteristic used by humans to make a personal recognition, hence the idea to use this biometric in technology. This is a non-intrusive method and is suitable for covert recognition applications. The applications of facial recognition range from static ("mug shots") to dynamic, uncontrolled face identification in a cluttered background (subway, airport). Face verification involves extracting a feature set from a two-dimensional image of the user's face and matching it with the template stored in a database. The most popular approaches to face recognition are based on either: 1) the location and shape of facial attributes such as eyes, eyebrows, nose, lips and chin, and their spatial relationships, or 2) the overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces. Although performance of commercially available systems is reasonable there is still significant room for improvement since false reject rate (FRR) is about 10% and false accept rate (FAR) is 1%. These systems also have difficulties in recognizing a face from images captured from two different angles and under different ambient illumination conditions. It is questionable if a face itself is a sufficient basis for recognizing a person from a large number of identities with an extremely high level of confidence. Facial recognition system should be able to automatically detect a face in an image, extract its features and then recognize it from a general viewpoint (is., from any pose) which is a rather difficult task. Another problem is the fact that the face is a changeable social organ displaying a variety of expressions.

**Retina.** Retinal recognition creates an "eye signature" from the vascular configuration of the retina which is supposed to be a characteristic of each individual and each eye, respectively. Since it is protected in an eye itself, and since it is not easy to change or replicate the retinal vasculature, this is one of the most secure biometric. Image acquisition requires a person to look through a lens at an alignment target, therefore it implies cooperation of the subject. Also retinal scan can reveal some medical conditions and as such public acceptance is questionable.

**Iris.** The iris begins to form in the third month of gestation and the structures creating its pattern are largely complete by the eighth month. Its complex pattern can contain many distinctive features such as arching ligaments, furrows, ridges, crypts, rings, corona, freckles and a zigzag collarette. Iris scanning is less intrusive than retinal because the iris is easily visible from several meters away. Responses of the iris to changes in light can provide an important secondary verification that the iris presented belongs to a live subject. Irises of identical twins are different, which is another advantage. Newer systems have become more user-friendly and cost-effective. A careful balance of light, focus, resolution and contrast is necessary to extract a feature vector from localized image. While the iris seems to be consistent throughout adulthood, it varies somewhat up to adolescence.

**Palmprint.** Like fingerprints, palms of the human hands contain unique pattern of ridges and valleys. Since palm is larger then a finger, palm print is expected to be even more reliable than fingerprint. Palm print scanners need to capture larger area with similar quality as finger print scanners, so they are more expensive. A highly accurate biometric system could be combined by using a high-resolution palm print scanner that would collect all the features of the palm such as hand geometry, ridge and valley features, principal lines, and wrinkles.

**Voice.** The features of an individual's voice are based on physical characteristics such as vocal tracts, mouth, nasal cavities and lips that are used in creating a sound. These characteristics of human speech are invariant for an individual, but the behavioral part changes over time due to age, medical conditions and emotional state. Voice recognition techniques are generally categorized according to two approaches: 1) Automatic Speaker Verification (ASV) and 2) Automatic Speaker Identification (ASI). Speaker verification uses voice as the authenticating attribute in a two-factor scenario. Speaker identification attempts to use voice to identify who an individual actually is. Voice recognition distinguishes an individual by matching particular voice traits against templates stored in a database. Voice systems must be trained to the individual's voice at enrollment time, and more than one enrollment session is often necessary. Feature extraction typically measures formants or sound characteristics unique to each person's vocal tract. The pattern matching algorithms used in voice recognition are similar to those used in face recognition.

**Signature.** Signature is a simple, concrete expression of the unique variations in human hand geometry. The way a person signs his or her name is known to be characteristic of that individual. Collecting samples for this biometric includes subject cooperation and requires the writing instrument. Signatures are a behavioral biometric that change over a period.
of time and are influenced by physical and emotional conditions of a subject. In addition to the general shape of the signed name, a signature recognition system can also measure pressure and velocity of the point of the stylus across the sensor pad.

DNA. Deoxyribonucleic acid (DNA) is probably the most reliable biometrics. It is in fact a one-dimensional code unique for each person. Exception are identical twins. This method, however, has some drawbacks:

1) contamination and sensitivity, since it is easy to steal a piece of DNA from an individual and use it for an ulterior purpose,
2) no real-time application is possible because DNA matching requires complex chemical methods involving expert’s skills,
3) privacy issues since DNA sample taken from an individual is likely to show susceptibility of a person to some diseases. All this limits the use of DNA matching to forensic applications.

Dental. Law enforcement agencies have been exploiting biometric identifiers for decades as key tools in forensic identification. A biometric identifier has to resist the early decay that affects body tissues. Because of their survivability and diversity, the best candidates for post mortem biometric identification are the dental features. ADIS (Automated Dental Identification System) a new fully automated algorithm for identifying people from dental X-ray images as one of ADIS components. The algorithm automatically archives AM (antemortem) dental photographs by extracting teeth shapes and storing them in a database. Given a dental image of a PM (postmortem), the proposed algorithm retrieves the best matches from the database. To generate DIR all reference records are added; high level features NCIC (NCIC,is the national database for dental records that contain textual dental codes) codes are extracted from each reference image and are stored in the DIR and the NCIC respectively. When the user submits a subject record, i.e., an unidentified PM record, high level features are extracted from the subject image. These features are used to select a list of 100-150 candidate matching images from the DIR. Once the list of candidate images are created, they are fed to the image comparison stage that selects a smaller list of candidate images for possible positive matches with the submitted subject image. This smaller list is then given to the forensic expert who makes the final decision. If a positive identification cannot be made for a subject image, then this image is added to the DIR as a new missing or unidentified image.

Heart sound. The possibility of using human heart sounds—an acoustic signal—as a reliable biometric for human identification based on the following requirements.[1]

1) Universal: Each living human being has a heart that keeps on pumping until his death.
(2) Quantifiable: Heart sound can be digitally captured and measured using an electronic stethoscope.
(3) Vulnerability: Unlike other biometric technologies that use fingerprints, pictures or static bio-signals to identify a person, heart sound cannot be copied and reproduced easily as it is based on intrinsic human biometric dynamic signals acquired from the body. When compared with voice, we feel that the heart sound exhibits two significant advantages. First, human voice can be easily obtained using a concealed recorder without the person knowing whereas to acquire a person heart sound, the recording device has to be placed on the person chest surface, with his permission, to capture the vibrations from the heart. Second, to reproduce the same heart sound of an individual, an artificial pumping heart with the same anatomy needs to be reconstructed; the physical attribute surrounding the artificial heart must also match the same individual body structure. Hence, heart sound cannot be easily recorded and simulated accurately.

4) Acceptability: Privacy issue will affect the extent to which people are willing to accept the use of their heart sound as a biometric identifier in their daily lives.

5) Usability: With the advancement in wearable computing, wireless sensors can eventually be placed on human to capture their heart signal when they are moving or performing other activities.

(6) Unique: The physical state of an individual’s health, age, size, weight, height, structure of the heart as well as the genetics factors all contribute to an individual’s unique heart sound. The heart sounds of two persons having the same type of heart diseases also vary.

(7) Variability: In a controlled environment, the human heart sound remains sufficiently invariant over a specific period of time. The goal of feature extraction is to find a transformation that converts the original heart signal into a relatively low dimensional feature space that is able to preserve the information pertinent to the application while enabling meaningful comparisons to be performed using simple measures of similarity. For the biometric application, the physiological property of the heart sound is more important than the heart rate. Hence, be restricting the processing of the heart sound to the frequency domain. Use the cepstral coefficient as the feature. The heart sound is modeled as the outcome of a time-varying linear system where the excitation input carries information on the heart beat rate, and the transfer function is time varying. Since the characteristic of the heart sound signal is very similar to the speech signal, we provide a comparison according to Ref. [2] and summarize the results in Table 1.
An Overview of Leading Biometrics for Human Identity

<table>
<thead>
<tr>
<th>Biometric Identifier</th>
<th>University</th>
<th>Distinctiveness</th>
<th>Permanence</th>
<th>Collectability</th>
<th>Performance</th>
<th>Acceptability</th>
<th>Circumvention</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNA</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Ear</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Face</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Facial Thermogram</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Gait</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Hand Vein</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Iris</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Keystroke</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Odor</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Palmprint</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Retina</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Signature</td>
<td>L</td>
<td>L</td>
<td>L</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>H</td>
</tr>
<tr>
<td>Voice</td>
<td>M</td>
<td>L</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Heart Sound</td>
<td>H</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>M</td>
<td>L</td>
</tr>
</tbody>
</table>

Table I. COMPARISON OF VARIOUS BIOMETRIC TECHNOLOGIES

**Finger-knuckle prints.** A new biometric technique- the finger-knuckle print (FKP), which refers to the image of the outer surface of the finger phalangeal joint.[6] The finger-back surface-the ‘dorsum’ of the hand-can be very useful in user identification, but it has not yet attracted significant attention of researchers. In particular, the image-pattern formation from finger-knuckle bending is highly unique and thus makes this surface a distinctive biometric identifier. The anatomy of our fingers allows them to bend forward and resist backward motion. This asymmetry results in a very limited number of creases and wrinkles on their palm side. Therefore, finger-knuckle patterns are a promising avenue for further developments in touch less personal identification. The advantages of employing finger-knuckle imaging are numerous. First, user acceptance of outer-palm surface imaging is very high since, unlike for fingerprints, there is no stigma of potential criminal investigation associated with this approach.

Second, the finger geometry can be acquired simultaneously from the same image and employed to improve the system's performance. Peg-free imaging of the finger-back surface is also convenient. Such images can be acquired online and used to extract scale, translational and rotational-invariant knuckle features for reliable identification. Texture analysis of the normalized knuckle-image regions can reveal highly discriminative information for identification purposes.

A brief comparison of the above biometric techniques based on seven factors is provided in Table I. The applicability of a specific biometric technique depends heavily on the requirements of the application domain. No single technique can outperform all the others in all operational environments. In this sense, each biometric technique is admissible and there is no optimal biometric characteristic.

4. ADVANTAGES AND APPLICATIONS OF BIOMETRIC SYSTEMS

1. Advantages
   - Most convenient and secure identification technology, it does not need to remember complex passwords, nor do they need to carry keys, smart cards and the like.
   - Difficult to counterfeit and fake, so the use of biometrics for identity finds a safe, reliable and accurate form.
   - A centralized data base of biometric data is one of the ways there checking whether the same person has registered with a system more than once using different credentials.
   - Biometrics has the potentials to enhance the privacy. It could also be used to encrypt digital information.
   - There are no known health hazards from the use of common biometric technologies and no significant health information is revealed from biometric data.
   - With the help of modern computer technology, it is easy with the computer and security, monitoring, management, systems integration, automated management

2. Applications of biometric systems

Biometric applications fall into three main groups:
- commercial applications, such as computer network logins, electronic data security, e-commerce, Internet access, ATMs, credit cards, physical access control, cellular phones, PDAs, medical records management, and distance learning;
- government applications such as national ID cards, correctional facilities, driver’s licenses, social security, border control, passport control, and welfare-disbursement; and
- forensic applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

5. LIMITATIONS OF BIOMETRIC SYSTEMS USING SINGLE BIOMETRICS
1) **Noise in sensed data**: Example is a fingerprint with a scar. Noisy data can also result from accumulation of dirt on a sensor or from ambient conditions.[3]

2) **Intra-class variations**: Biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment. This variation is typically caused by a user who is incorrectly interacting with the sensor.

3) **Distinctiveness**: While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discriminability provided by the biometric trait.

4) **Non-universality**: While every user is expected to possess the biometric trait being acquired, in reality it is possible that a group of users do not possess that particular biometric characteristic.

5) **Spoof attacks**: An individual may attempt to forge the biometric trait. This is particularly easy when signature and voice are used as an identifier.

### 6. MULTIMODAL BIOMETRIC SYSTEMS

Limitations of unimodal biometric systems can be overcome by using multimodal biometric systems. A multimodal biometric system uses multiple applications to capture different types of biometrics. This allows the integration of two or more types of biometric recognition and verification systems in order to meet stringent performance requirements. Such systems are expected to be more reliable due to the presence of multiple, independent pieces of evidence. These systems are also able to meet the strict performance requirements imposed by various applications.

1) **Multiple sensors**: the information obtained from different sensors for the same biometric are combined. For example, optical, solid-state, and ultrasound based sensors are available to capture fingerprints.

2) **Multiple biometrics**: multiple biometric characteristics such as fingerprint and face are combined. These systems will necessarily contain more than one sensor with each sensor sensing a different biometric characteristic. In a verification system, the multiple biometrics are typically used to improve system accuracy, while in an identification system the matching speed can also be improved with a proper combination scheme (e.g., face matching which is typically fast but not very accurate can be used for retrieving the top matches and then fingerprint matching which is slower but more accurate can be used for making the final identification decision).

3) **Multiple units of the same biometric**: fingerprints from two or more fingers of a person may be combined, or one image each of the two irises of a person may be combined.

4) **Multiple snapshots of the same biometric**: more than one instance of the same biometric is used for the enrollment and/or recognition. For example, multiple impressions of the same finger, multiple samples of the voice, or multiple images of the face may be combined.

5) **Multiple representations and matching algorithms for the same biometric**: this involves combining different approaches to feature extraction and matching of the biometric characteristic. This could be used in two cases. First, verification or an identification system can use such a combination scheme to make a recognition decision. Second, an identification system may use such a combination scheme for indexing.

### CONCLUSION

This century information technology, network technology, fundamentally change our traditional way of life. The biometric authentication technology began to flourish in high-tech, will occupy in social life more and more important position. It is typically confronted with unrealistic performance expectations and not fairly compared with existing alternatives. At the same time, ensure the security of personal information as possible to prevent all types of criminal and economic crimes. Biometrics promises better security to the existing systems. Implementers should decide wisely what Biometric method best suits their needs. They also would have to consider the cost-benefit ratio of biometric technology. The greatest reason for industry skepticism about Biometrics is the reliability of the system. In near future we use biometrics based recognition system in our day to day life.

### REFERENCES


