Brief Survey of Biometric Identification

Mohsen Hajianfard1, Hossein Emami2, Iman Sepahvand3
1--Department of Electrical Engineering, Islamic Azad University, Majlesi Branch, Esfahan, Iran
Email: mohsen.hajianfard@gmail.com
1--Department of Electrical Engineering, Islamic Azad University, Majlesi Branch, Esfahan, Iran
Email: h.emami@ieee.org
3--Department of Electrical Engineering, Islamic Azad University, Lorestan Branch, Esfahan, Iran
Email: Iman_sepahvand@yahoo.com

Received: July 2013 Revised: August 2013 Accepted: November 2013

ABSTRACT
This paper briefly reviews the presents notions and ideas associated with the biometric techniques for recognition of users of system. The recent advances of information technology and the increasing requirement for security have led to a rapid development of intelligent personal identification systems based on biometrics. As humans, we all use our natural abilities to recognize people through their voices, faces and other characteristics. Technology advances, particularly in biometrics, are helping to close the gap between human perception and machine recognition. A priority goal of the use of biometrics is to provide identity assurance or the capability to accurately recognize individuals with greater reliability. Biometric recognition or, simply, biometrics refers to an automatic recognition of individuals based on their physiological and/or behavioral characteristics. This paper gives a brief overview of biometric, biometric recognition system, and various biometric recognition methods and their advantages, and disadvantages.

KEYWORDS: Biometrics, Working of Biometrics, Types of Biometrics

1. INTRODUCTION
In this paper, we have presented the different types of biometrics, their applications and the biometric recognition systems. The biometric is the study of physical or behavioral characteristics used for the identification of a person [1]. These characteristics of a person include the features like fingerprints, face, hand geometry, voice, and iris biometric features. These biometrics features can be used for authentication purpose in computer based security systems. The identification of a person is becoming highly important as the ID cards, punch, secret password and PIN are used for personal identification [2]. The ID can be stolen; passwords can be forgotten or cracked. The biometrics identification overcomes all the above. Additional security barriers can be provided using any one of the biometrics features [3]. The computers based security systems are used at various places like commercial, civilian and government offices to store information and all processing. It is the primary thing to provide security to the information present on internet. For this purpose the confidential authentication is required by replacing the username and password [4]. The biometric systems offer several advantages over traditional authentication systems. The problem of information security gives the protection of information ensuring only authorized users are able to access the information. They are required the person being authenticated to be present at the point of authentication [5]. Thus biometric-based authentication method is most secure system. For many applications the system uses the password as well as biometrics for authentication. The biometric characteristics have been used in different applications. According to the requirement of the application suitable biometric can be selected.

2. BIOMETRICS
The biometric refers to automated methods of authentication based on physical or behavioral characteristics of an individual. The first known example of biometrics was a form of finger printing being used in China to distinguish the young children from one another by stamping children's palm prints and footprints on paper with ink. This is one of the earliest known cases of biometrics in use and is still being used today. Although biometrics emerged from its extensive use in law enforcement to identify criminals, it is being increasingly used today in to establish person recognition in a large number of civilian applications.
Biometrics is a technology that uniquely identifies a person based on his physiological or behavioral characteristics. Since it relies on “something you are”, it can inherently differentiate between authorized personal and an imposter. Theoretically, any human physiological or behavioral characteristic can be used to make a personal identification as long as it satisfies the following requirements [20]:

1) **Universality**: Every person should have the characteristic
2) **Uniqueness**: No two people should be the same in terms of the characteristic
3) **Permanence**: Characteristic should be invariant with time
4) **Collectability**: Characteristic should be able to be measured quantitatively

<table>
<thead>
<tr>
<th>BIOMETRIC</th>
<th>UNIVERSALITY</th>
<th>UNIQUENESS</th>
<th>PERMANENCE</th>
<th>COLLECTABILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Iris</td>
<td>High</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
</tr>
</tbody>
</table>

For practical purposes, there are some additional requirements:

1) **Performance**: This refers to the achievable identification accuracy, the resource requirements to achieve acceptable accuracy and the working or environmental factors that affect the identification accuracy.
2) **Acceptability**: To what extent people are willing to accept the biometric system
3) **Circumvention**: How easy it is to fool the system

<table>
<thead>
<tr>
<th>BIOMETRIC</th>
<th>PERFORMANCE</th>
<th>ACCEPTABILITY</th>
<th>CIRCUMVENTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Face</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Fingerprint</td>
<td>High</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Hand Geometry</td>
<td>Medium</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Iris</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

Biometric accuracy is measured in two ways; the rate of false acceptance (an impostor is accepted as a match

Type 1 error) and the rate of false rejects (a legitimate match is denied - Type 2 error) [2].

Every biometric technique has a different method of assigning a "score" to the biometric characteristic; a "threshold value" is defined which determines when a match is declared. Scores above the threshold value are designated as a "Hit" and scores below the threshold are designated as "No-Hit." Error occurs if a true match does not generate a score above the threshold. A Type 1 error is made when an imposter generates a match score above the threshold. If the Type 1 and Type 2 error rates are plotted as a function of threshold value, they will form curves which intersect at a given threshold value. The point of intersection (where Type 1 error equals Type 2 error) is called the crossover accuracy or Equal Error rate of the system. In general, as the value of the crossover accuracy becomes higher, the inherent accuracy of the biometric increases.

Biometrics is a rapidly evolving technology that has been widely used in forensics (fingerprints), prison security etc. and has the potential to be widely adopted in a broad range of civilian applications such as physical access control, banking security, information system security, voter and driver registration etc. Currently the world market for biometric systems is estimated to be $112 million and growing.

### 2.1. BIOMETRIC SYSTEM PERFORMANCE

Due to different positioning on the acquiring sensor, imperfect imaging conditions, environmental changes, deformations, noise and bad user's interaction with the sensor, it is impossible that two samples of the same biometric characteristic, acquired in different sessions, exactly coincide. For this reason a biometric matching systems' response is typically a matching score $s$ (normally a single number) that quantifies the similarity between the input and the database template representations. The higher the score, the more certain the system is that the two samples coincide [14]. A similarity score $s$ is compared with an acceptance threshold $t$ and if $s$ is greater than or equal to $t$ compared samples belong to a same person. Pairs of biometric samples generating scores lower than $t$ belong to a different person. The distribution of scores generated from pairs of samples from different persons is called an impostor distribution, and the score distribution generated from pairs of samples of the same person is called a genuine distribution [14].

To assess the performance of a biometric system, we analyze it in a hypothesis testing framework. Let the stored biometric sample or template be pattern $P=S(B')$ and the acquired one be pattern $P=S(B)$. Then, in terms of hypothesis testing, we have null and alternative hypotheses:
H₀: B=B', the claimed identity is correct

H₁: B≠B', the claimed identity is not correct

Often some similarity measure s=Sim(P,P') is defined and H₀ is decided if s≥Td and H₁ is decided if s<Td with Td a decision threshold. (Some systems use a distance or dissimilarity measure. Without loss of generality we assume a similarity measure throughout.)

The measure is also referred to as the match score. When B=B', s is referred to as a matching score and B and B' are called a mated pair or matched pair. When P≠P', s is referred to as a non-matched score and B and B' are called a non-mated pair.

For expression 1, deciding H₀ when H₁ is true gives a false acceptance; deciding H₁ when H₀ is true results in a false rejection. The False Accept Rate (FAR) (proportion of non-mated pairs resulting in false acceptance) and False Reject Rate (FRR) (proportion of mated pairs resulting in false rejection) together characterize the accuracy of a recognition system for a given decision threshold. Varying the threshold trades FAR off against FRR. In Figure 2, the FAR is the area under the H₁ density function to the right of the threshold and the FRR is the area under the H₀ density function to the left of the threshold. In a more general framework, we can express the two errors as False Match Rate (FMR) and False Non-Match Rate (FNMR) [16].

The Equal Error Rate (EER) is the point at some threshold (Tₑₑₑₚ) where FRR = FAR, i.e. where the areas marked under the two curves in Fig. 1 are equal.

The important features of the various biometrics are discussed briefly in this section.

2.2. Iris

Iris recognition is based on the features that exist in the colored tissue surrounding the pupil which has many interesting points that can be used for comparison, including rings, rows and spots [1]. The texture of the iris is very complex and distinctive which is very useful for the recognition system. Even the irises of identical twins are different. Although based on this complexity and this distinctness, the system is more accurately deployed and supports the probability of extensive identification systems [2].
2.3. Face
Facial recognition is usually thought of as the primary way in which people recognize one another. After all, given a search through one's wallet, it becomes clear that identification based on facial recognition is used by many organizations, such as universities, government agencies, and banks, although the recognition is usually carried out by a human. Many of these organizations will, of course, have these photos stored in large databases making many commercial and law-enforcement applications feasible given a reliable facial recognition system. Additionally, facial images of a person can usually be collected without necessarily requiring much co-operation from that person. Thus, it is no surprise that facial recognition is a key part of the DARPA-funded Human ID at a Distance Project aimed at developing the technology to identify terrorists from a distance [3].

Despite the aforementioned advantages of using facial recognition, it may perform very poorly when deployed in the real world, especially for recognition at a distance. A facial recognition system deployed in Logan International Airport to detect terrorists failed in 38 percent of the cases to match the identities of a test group of employees, according to a study by the American Civil Liberties Union [4]. A face-recognition system deployed on the streets of Tampa, Florida to identify criminals was scrapped two years later having not identified, alerted of, or caught any criminals, according to a spokesman for the Tampa Police Department [5].

There are many approaches that exist for tackling face recognition. Some of these approaches use the whole face as raw input, such as engine faces (figure 4) and fisher faces, which are based on principal component analysis. Other approaches depend on extracting and matching certain features from the face, such the mouth and eyes. Lastly, some approaches are a mix of the two using data from the whole face as well as specific features to carry out the recognition [6].

2.4. Fingerprint
A fingerprint is the pattern of ridges and grooves on the surface of a fingertip. The fingerprints are highly stable and unique. The uniqueness of fingerprint is determined by global features like valleys and ridges, and by local features like ridge endings and ridge bifurcations, which are called minutiae. The recent studies reveal that probability of two individuals, having the same fingerprint is less than one in a billion. There are various fingerprint matching algorithms like minutiae based matching correlation based matching, genetic algorithms based. Among these, minutiae based matching is the dominated one. In minutiae based matching the similarity of two fingerprints is determined by computing the total number of matching minutiae from the scanned fingerprints. Extraction of minutiae features before matching needs a series of processes, containing alignment computation, image segmentation, image enhancement, and ridge extraction and shinning, minutiae extraction and filtering. Correlation based matching uses one to one correlation between fingerprints. This method gives poor results in fingerprint recognition because correlation cannot recognize elastic-distorted versions of the same fingerprint. In neural network based approach the print fills are classified by using HAVNET. The number of output nodes of HAVNET was equal to number of enrolled fingerprints. The method was not able to distinguish fingerprints of similar shapes The genetic algorithm based methods try to identify the optimal global alignment between two fingerprints. The process is highly time consuming one.
2.5. Gait

Gait recognition is a particular type of biometric due to its capability to identify a person at distance. Gait is related to the way of the person walking. The gait recognition system uses standard camera in any conditions and develops algorithms to extract the silhouette of the person in case he is moving. Therefore the system can track the person over time. However the algorithm is not very efficient for this trait is affected by many conditions such as the type of cloth’s or shoes the individual’s wearing, the walking surface or the health. All these biometrics are acceptable in different environment and none of them is optimal. However the most accurate ones are iris and fingerprint techniques. Due to the fact iris recognition is expensive and it requires advance requirement, fingerprint is one of the most mature biometrics and suitable for many applications [8]. Fingerprint biometrics is very distinctive, not expensive, unique and permanent and has a very good balance from all the properties.

![Fig. 6. Samples recorded from a gait cycle.](image)

On the other hand, DNA techniques are not able to distinguish between monozygotic twins which are formed when one fertilized egg splits, because they are the only people in the world with identical DNA profile. DNA faces several other challenges as well; several hours are required in order to obtain a fingerprint and the test is quite expensive to perform. Besides, DNA includes sensitive information related to genetic and medical aspects of individuals, and hence any misuse of DNA information can disclose the user’s privacy. This is why people are fairly hostile to DNA usage [10].

2.7. Hand Geometry

While it does not occur to humans, in everyday life, to observe one’s hand geometry to identify who they may be, primitive biometric systems that do just that have been in existence since the 1960s. Use of hand geometry has several advantages as shown by a survey of 129 users of a hand geometry biometric system at Purdue University’s Recreation Centre. Out of the survey participants, 93% liked using the technology, 98% found it easy to use, and no one found the technology invasive of privacy [24]. Similar to other technologies, hand geometry's ease of use and acceptably amongst users does come at a cost. For one thing, hand geometry is not especially distinctive, especially when applied to a large population. Thus, it is most suitable for purposes of verification rather than identification. Additionally, hand geometry may not be an ideal biometric to use if users include children whose hand-geometry template may vary during their growth period [25].

Hand geometry recognition can be done based on the measurement and matching of various features, such as the finger width, finger length, hand size, and hand contour. Most hand-geometry systems determine the different parts of the hand based on pins between fingers, restricting the position in which one can place one’s hand [26]. Figure 6 shows one of such hand geometry recognition systems.

![Fig. 7. DNA double Helix](image)

5
2.8. Voice
Voice recognition systems can discriminate between two very similar voices, including twins. Voice recognition utilizes various audio capture devices (microphones, telephones and PC microphones). Its performance depends on the quality of the audio signal. Unauthorized access via tape recording can be prevented by asking the user to repeat random phrases, the benefit of this way Use existing telephones & can be automated, and coupled with speech recognition systems.

![Voice print](image)

Fig. 9: Voice print

2.9. Retina Scan
Retinal scan captures the pattern of eye’s blood vessels. Retina is very difficult to spoof. Retinal patterns are different for right and left eye, for identical twins, do not change with age. Moreover, the image will not fall on the retina for dead person In it, low-intensity coherent light source is projected onto the retina to illuminate the blood vessels which are then photographed and analyzed. A coupler is used to read the blood vessel patterns. A retinal scan has an error rate of 1 in 10,000,000, compared to fingerprint identification error being sometimes as high as 1 in 500.

2.10. Signature
Signature is the way a person signs his name. Depending on this sign, the individual can be identified. Signature recognition examines the unique way in which the signature is written. In the signature recognition system, the signature is compared by examining how the signature was written or it is verified by estimating how the signature was created. Sometimes, this type of biometric can be changed over time. The same person can sign in different way. In addition, it is affected by physical conditions such as sickness or sentimental condition such as individual’s feeling.

It is obvious that no single biometric is the "ultimate" recognition tool and the choice depends on the application. A brief comparison of the above techniques based on seven factors described in section 2 is provided in Table I [15].

3. BIOMETRIC SYSTEEMS
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. That feature vector is usually stored in a database or recorded on a smart card after being extracted.
Biometric system operates in one of two modes: verification or identification.

**Data Acquisition:** Digital cauterization of the biometric is done here and the results are transferred to the signal processing functions.

**Transmission Channel:** This is the communication path between the primary functional components. For self-contained systems, transmission channels are internal but for distributed systems (remote data acquisition) transmission channel might be LAN, private intranet, or even the internet.

**Signal Processing:** This is where the raw biometric data is processed for matching. Processing consists of segmentation of the sample, then isolate and extracting relevant features from the data, and creating a biometric template i.e. mathematical representation of the original biometric. Segmentation is the process of separating relevant features from the background information.

The result of extraction segmentation is a quality score, reflecting the quality of the input by how successful the feature extraction was. Then the newly created template is then compared to one or more reference templates by the matching algorithm. The result of matching algorithm is a match score, indicating how similar the templates are.

**Decision Policy:** It makes a final determination whether there is a match or not. Normally, empirically determined thresholds are used for the quality score and match score. If both scores are met then a match is produced (yes). If only the quality threshold is met, negative match (no). If the quality threshold is not met, the application might refuse the match because of the poor quality data and request a new sample.

**4- MULTIMODAL BIOMETRICS**

Noisy data, Interclass Variation, Interclass Similarities, Non universality, Spoofing etc problems are imposed by unimodal biometric systems which tend to increase False Acceptance Rate [FAR] and False Rejection Rate [FRR], ultimately reflecting towards poor performance of the system.

Some of the limitations imposed by unimodal biometrics can be overcome by including multiple source of information for establishing identity of person [12]. Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a Verification or Identification system. They address the problem of non-universality, since multiple traits ensure sufficient population coverage [13]. Multimodal biometrics also address the problem of spoofing as it concern with multiple traits or modalities, it would be very difficult for an imposter to spoof or attack multiple traits of genuine user simultaneously.

Multimodal biometric system has the potential to be widely adopted in a very broad range of civilian applications: banking security such as ATM security, check cashing and credit card transactions, information system security like access to databases via login privileges. A decision made by a multimodal biometric system is either a "genuine individual" type of decision or an "imposter" type of decision. In principle, Genuine Acceptance Rate [GAR], False Rejection Rate [FRR], False Acceptance Rate [FAR] and Equal Error Rate [ERR] is used to measure the accuracy of system. Generally multimodal biometrics operates in two phases i.e. Enrollment phase and authentication phase which are described as follows:
• Enrollment phase: - In enrollment phase, biometric traits of a user are captured and these are stored in the system database as a template for that user and which is further used for authentication phase.

• Authentication phase: - In authentication phase, once again traits of a user captured and system uses this to either identify or verify a person. Identification is one to many matching which involves comparing captured data with templates corresponding to all users in database while verification is one to one matching which involves comparing captured data with template of claimed identity only.

6- CONCLUSION
The existing methods of automatic authentication involving knowledge or possessions have a number of limitations, particularly in that they can be transferred from one person to another. Automated biometrics can address that problem while overcoming the other problems such as lost, sharing and forgery of other authentication methods. Automated biometric systems can be modeled as a pattern recognition systems. We have presented popular biometrics and a comparative evaluation of them.

REFERENCES: