1. Introduction

1.1 Biometrics

Biometrics comprises methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits. In computer science, in particular, biometrics is used as a form of identity access management and access control. It is also used to identify individuals in groups that are under surveillance [1].

Biometric characteristics can be divided in two main classes:

- **Physiological** are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, palmprint, hand geometry, iris recognition, which has largely replaced retina, and odor/scent.

- **Behavioral** are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term behaviometrics for this class of biometrics [2].

Strictly speaking, voice is also a physiological trait because every person has a different vocal tract, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioral. It is possible to understand if a human characteristic can be used for biometrics in terms of the following parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Universality</strong></td>
<td>Each person should have the characteristic.</td>
</tr>
<tr>
<td><strong>Uniqueness</strong></td>
<td>Indicates how well the biometric separates individuals from another.</td>
</tr>
<tr>
<td><strong>Permanence</strong></td>
<td>Measures how well a biometric resists aging and other variance over time.</td>
</tr>
<tr>
<td><strong>Collectability</strong></td>
<td>Ease of acquisition for measurement</td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td>Accuracy, speed, and robustness of technology used.</td>
</tr>
<tr>
<td><strong>Acceptability</strong></td>
<td>Degree of approval of a technology.</td>
</tr>
<tr>
<td><strong>Circumvention</strong></td>
<td>Ease of use of a substitute.</td>
</tr>
</tbody>
</table>

By using biometrics it is possible to establish an identity based on who you are, rather than by what you possess, such as an ID card, or what you remember, such as a password. In some applications, biometrics may be used to supplement ID cards and passwords thereby imparting an additional level of security. Such an
arrangement is often called a dual-factor authentication scheme [1], [2], [3].

The effectiveness of an authenticator (biometric or non-biometric) is based on its relevance to a particular application as well as its robustness to various types of malicious attacks. O’Gorman [4] lists a number of attacks that can be launched against authentication systems based on passwords and tokens:

- Client attack (e.g., guessing passwords, stealing tokens).
- Host attack (e.g., accessing plain text file containing passwords).
- Eavesdropping (e.g., "shoulder surfing" for passwords).
- Repudiation (e.g., claiming that token was misplaced).
- Trojan horse attack (e.g., installation of bogus log-in screen to steal passwords); and
- Denial of service (e.g., disabling the system by deliberately supplying an incorrect password several times).

While some of attacks can be deflected by incorporating appropriate defense mechanisms, it is not possible to handle all the problems associated with the use of passwords and tokens. Biometrics offers certain advantages such as negative recognition and nonrepudiation that cannot be provided by tokens and passwords. Negative recognition is the process by which a system determines that a certain individual is indeed enrolled in the system although the individual might deny it [1]. This is especially critical in applications such as welfare disbursement where an impostor may attempt to claim multiple benefits (i.e., double dipping) under different names. Non-repudiation is a way to guarantee that an individual who accesses a certain facility cannot later deny using it (e.g., a person accesses a certain computer resource and later claims that an impostor must have used it under falsified credentials). While biometric systems have their own limitations they have an edge over traditional security methods in that they cannot be easily stolen or shared.

1.2 Brief History of Biometrics [5]

Use biometrics date back over a thousand years. In East Asia, potters placed their fingerprints on their wares as an early form of brand identity. In Egypt’s Nile Valley, traders were formally identified based on physical characteristics such as height, eye color, and complexion. This information helped identify trusted
traders whom merchants had successfully transacted business in the past. The Old Testament also provides early (if not perfect) examples of voice recognition and biometric spoofing.

Biometrics as a commercial, modern technology has been around since the early 1970’s, when the first commercially available device was brought to market. One of the first commercial applications was used in 1972 when a Wall Street company, Shearson Hamil, installed Identimat, a finger-measurement device that served as a time keeping and monitoring application. Since this 1972 deployment, biometrics has improved tremendously in ease of use and diversity of applications. The advancement of biometrics has been driven by the increased computing power at lower costs, better algorithms, and cheaper storage mechanisms available today [1].

1.3 Biometric Traits

Biometric traits are actual characteristics or entities which are used to identify human. In the biometric literature, these characteristics are referred to as traits, indicators, identifiers or modalities. As we have discussed earlier there are two classes of biometric traits as Physiological & Behavioral, we discuss them accordingly.

1.3.1 Physiological Biometric Traits

These are based on physical characteristics of human body. Fingerprint, palmprint, hand vein, hand/finger geometry, iris, retina, face, ear, odor or the DNA information of an individual come in this category.

1.3.1.1 Fingerprints

A fingerprint looks at the patterns found on a fingertip. There are a variety of approaches to fingerprint verification. Some emulate the traditional police method of matching minutiae; others use straight pattern-matching devices; and still others are a bit more unique, including things like moiré fringe patterns and ultrasonic. Some verification approaches can detect when a live finger is presented; some cannot [1],[2]. Fig. 1.1 shows location of fingerprints on human hand and a typical fingerprint captured through optical fingerprint scanner.
A greater variety of fingerprint scanning devices are available than for any other biometric, some of them are shown in Fig. 1.2 [6]. As the prices of these devices and processing costs fall, using fingerprints for user verification is gaining acceptance despite the common-criminal stigma. It is not surprising that the workstation access application area seems to be based almost exclusively on fingerprints, due to the relatively low cost, small size, and ease of integration of fingerprint authentication devices.

1.3.1.2 Hand Geometry [6], [8]

Hand geometry involves analyzing and measuring the shape of the hand. This biometric offers a good balance of performance characteristics and is relatively easy to use. It might be suitable where there are more users or where users access the system infrequently and are perhaps less disciplined in their approach to the system. Typical hand geometry scanners are shown in Fig. 1.3. It uses this information to determine the length, width, thickness, and curvature of your hand or fingers. It translates that information.
into a numerical template, which is used for matching. Hand and finger geometry systems have a few strengths and weaknesses. Since hands and fingers are less distinctive than fingerprints or irises, some people are less likely to feel that the system invades their privacy. However, many people's hands change over time due to injury, changes in weight or arthritis. Some systems update the data to reflect minor changes from day to day. Ease of integration into other systems and processes, coupled with ease of use makes hand geometry an obvious first step for many biometric projects.

Fig. 1.3. Example of Typical hand Geometry Scanner and Their use [8]

1.3.1.3 Hand Vein Geometry [8]

As with irises and fingerprints, a person's veins are completely unique. Twins don't have identical veins, and a person's veins differ between their left and right sides. Many veins are not visible through the skin, making them extremely difficult to counterfeit or tamper with. Their shape also changes very little as a person ages.

Fig. 1.4. (a) Finger Vein Scanner by Hitachi (b) Typical Hand Vein Structure

To use a vein recognition system, you simply place your finger, wrist, palm or the back of your hand on or near the scanner. A camera takes a digital picture using near-infrared light. The
hemoglobin in your blood absorbs the light, so veins appear black in
the picture. As with all the other biometric types, the software
creates a reference template based on the shape and location of the
vein structure. This template can be used for matching purpose.

1.3.1.4 Palmprints [1], [3], [8]

The palms of the human hands contain pattern of ridges and
valleys much like the fingerprints. The area of the palm is much
larger than the area of a finger and, as a result, palmprints are
expected to be even more distinctive than the fingerprints. Since
palmprint scanners need to capture a large area, they are bulkier
and more expensive than the fingerprint sensors. Human palms also
contain additional distinctive features such as principal lines and
wrinkles that can be captured even with a lower resolution scanner,
which would be cheaper [3]. Finally, when using a high-resolution
classic print sensor, all the features of the palm such as hand
geometry, ridge and valley features (e.g., minutiae and singular
points such as deltas), principal lines, and wrinkles may be
combined to build a highly accurate biometric system. A palmprint
scanner with a typical palmprint is shown in Fig. 1.5.

![Fujitsu Palmprint Scanner](a) ![Typical Palmprint showing Principle lines, Ridges and wrinkles](b)

Fig. 1.5. (a) Fujitsu Palmprint Scanner (b) Typical Palmprint showing Principle lines, Ridges and wrinkles

1.3.1.5 Finger-knuckle Print [9]

Finger-knuckle print (FKP) refers to the image pattern of the
outer surface around the phalangeal joint of one’s finger, which is
formed by bending slightly the finger-knuckle. FKP contains rich
texture information formed by wrinkles present on fingerprint
surface. A typical finger-knuckle print is shown in Fig. 1.6 (b). This
biometric trait is relatively new and yet to be much explored. The
FKP capture device is developed by Hong Kong Polytechnic University
[9], the proposed system captures the image around the finger knuckle area of a finger directly, which largely simplifies the following preprocessing steps. Meanwhile, with such a design the size of the imaging system can be greatly reduced, which improves much its applicability. Since the finger-knuckle will be slightly bent when being imaged in the proposed system, the inherent finger-knuckle print patterns can be clearly captured and hence the unique features of FKP can be better exploited.

Fig. 1.6. (a) Finger-knuckle Print Scanner (b) Typical Finger-Knuckle Print Image from Hong Kong Polytechnic University FKP Database[9].

1.3.1.6 Face

Face recognition analyzes facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. Because facial scanning needs an extra peripheral not customarily included with basic PCs, it is more of a niche market for network authentication. With security cameras presents in variety of public places facial recognition is a viable option for biometric identification. Face biometrics is relatively less accurate but requires low user co-operation. With advancement in technology variations such as facial thermogram (temperature distribution on a face) and 3D face mapping are also being implemented. Fig. 1.7 (a) & (b) shows these biometrics. Facial thermography refers to the pattern of facial heat caused by the distinctive flow of blood under the skin [5]. IR cameras capture this heat to produce a thermal pattern. Because the vein and tissue structure of an individual’s face is distinctive, the infrared image is also distinctive. The thermal data is analyzed to yield anatomical information, which is converted to a template and used for identification.
1.3.1.7 Iris

An iris-based biometric, on the other hand, involves analyzing features found in the colored ring of tissue that surrounds the pupil (Fig.1.8 (c)).

Iris scanning, undoubtedly the less intrusive of the eye related biometrics, uses a fairly conventional camera element and requires no close contact between the user and the reader. Typical iris
scanners are shown in Fig. 1.8 (a) & (b). In addition, it has the potential for higher than average template matching performance. Iris scanners are becoming more common in high-security applications because people’s eyes are so unique (the chance of mistaking one iris code for another is 1 in $1 \times 10^{78}$ [10]). They also allow more than 200 points of reference for comparison, as opposed to 60 or 70 points in fingerprints. The iris is a visible but protected structure, and it does not usually change over time, making it ideal for biometric identification. Most of the time, people's eyes also remain unchanged after eye surgery, and blind people can use iris scanners as long as their eyes have irises. Eyeglasses and contact lenses typically do not interfere or cause inaccurate readings.

The biometric traits discussed above are studied in this thesis in detail, besides this significant biometrics traits are retinal scan, ear geometry, DNA & Body odor[3], [5], [11].

1.3.2 Behavioral Biometric Traits

The behavioral biometrics deals with the way certain act is performed by human. This includes speaking, writing, walking etc. We discuss here few important behavioral biometric traits.

1.3.2.1 Handwritten Signature

Human handwriting style is unique from person to person. At first glance, using handwriting to identify people might not seem like a good idea. After all, many people can learn to copy other people’s handwriting with a little time and practice. It seems like it would be easy to get a copy of someone's signature or the required password and learn to forge it. But biometric systems don't just look at how you shape each letter; they analyze the act of writing. They examine the pressure you use and the speed and rhythm with which you write. They also record the sequence in which you form letters like whether you add dots and crosses as you go or after you finish the word.

Signature verification analyzes the way a user signs. Signing features such as speed, velocity, and pressure are as important as the finished signature’s static shape. Fig. 1.9 (a) & (b) show such signature scanners. A signature having different pressure levels is shown in Fig. 1.9 (c). Signature verification enjoys a synergy with existing processes that other biometrics do not. People are used to
signatures as a means of transaction-related identity verification, and most would see nothing unusual in extending this to encompass biometrics. Signature verification devices are reasonably accurate in operation and obviously lend themselves to applications where a signature is an accepted identifier. Main application domain of handwritten signature is in banking and e-commerce & document authentication.

![Signature Verification Devices]

(a) (b) (c)

Fig. 1.9. (a) & (b) Dynamic Signature Capturing Devices (c) Dynamic Signature showing Different Pressure Levels by Different Colors

1.3.2.2 Keystroke Dynamics [1]

Unlike signature verification (and most every other biometric) keystroke dynamics are somewhat unique in that they do not require special sensor equipment beyond a regular keyboard. The keystroke dynamics are captured entirely by software, so the technique can be applied to any system that accepts and processes keyboard input events.

Keystroke dynamics can be used for single authentication events or for continuous monitoring. Continuous monitoring is not normally done in commercial biometrics products; however, it has been proposed as a legitimate and reasonable means to help prevent unauthorized use of unattended terminals. Keystroke monitoring is the unsophisticated, yet surprisingly easy way to achieve logging of every key pressed by a user. While many have argued the potential for abuse far outweighs any legitimate use of the process, keystroke monitoring is sometimes used to provide auditing and security information that may be required in certain sensitive environments. Such systems should be marked with banners and notices to inform users that their use is monitored.

The most natural application for keystroke dynamics is to “harden” passwords. The keystroke dynamics of each user is used to augment existing passwords by requiring that the password be
entered in a manner consistent with the intended user. A related use of keystroke dynamics is for human typing detection. That is, keystroke patterns can be used to help determine the difference between man and machine (live human typing vs. scripted programs).

Other biometric traits based on human behavior are Gait, Voice, and Facial Expressions etc. Table 1.1 shows comparison between key biometric traits.

### Table 1.1
Comparison of Key Biometric Technologies

<table>
<thead>
<tr>
<th>Biometric</th>
<th>Fingerprint</th>
<th>Face</th>
<th>Hand Geometry</th>
<th>Iris</th>
<th>Voice</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barriers to Universality</td>
<td>Worn Ridges, Hand or Finger Impairment</td>
<td>None</td>
<td>Hand Impairment</td>
<td>Visual Impairment</td>
<td>Speech Impairment</td>
</tr>
<tr>
<td>Distinctiveness</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Permanence</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Collectability</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>Performance</td>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Acceptability</td>
<td>Medium</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Potential for Circumvention</td>
<td>Low</td>
<td>High</td>
<td>Medium</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

1.4 Biometric System Architecture [2], [3], [6]

A biometric system can operate in the following two modes:

- **Verification (Matching)** – A one to one comparison of a captured biometric with a stored template to verify that the individual is who he claims to be. This can be achieved in conjunction with a smart card, username or ID number.
- **Identification (Recognition)** – A one to many comparisons of the captured biometric against a biometric database in attempt to identify an unknown individual. The identification only succeeds in identifying the individual if the comparison of the biometric sample to a template in the database falls within a previously set threshold.

The first time an individual uses a biometric system is called an enrollment. During the enrollment, biometric information from
an individual is stored. In subsequent uses, biometric information is detected and compared with the information stored at the time of enrollment. Note that it is crucial that storage and retrieval of such systems themselves be secure if the biometric system is to be robust. The first block (sensor) is the interface between the real world and the system; it has to acquire all the necessary data. Most of the times it is an image acquisition system, but it can change according to the characteristics desired. The extraction block performs all the necessary preprocessing; it has to remove artifacts from the sensor, to enhance the input (e.g. removing background noise), to use some kind of normalization, etc. In the third block necessary features are extracted. This step is an important step as the correct features need to be extracted in the optimal way. A vector of numbers or an image with particular properties is used to create a template. A template is a synthesis of the relevant characteristics extracted from the source. Elements of the biometric measurement that are not used in the comparison algorithm are discarded in the template to reduce the file size and to protect the identity of the enrollee.

If enrollment is being performed, the template is simply stored somewhere (on a card or within a database or both) with or without encryption. If a matching phase is being performed, the obtained template is passed to a matcher that compares it with other existing templates, estimating the distance between them using any algorithm (e.g. Hamming distance). The matching program will analyze the template with the input. This will then be output for any specified use or purpose (e.g. entrance in a restricted area).

![Fig. 1.10. Architecture of Typical Biometric System [12].](image-url)
1.5 Performance Metrics

The performance of a biometric system is measured by different parameters or metrics. The following are used as performance metrics for biometric systems [1], [2], [3], [5]:

- **False Accept Rate or False Match Rate (FAR or FMR)** – the probability that the system incorrectly matches the input pattern to a non-matching template in the database. It measures the percent of invalid inputs which are incorrectly accepted.

- **False Reject Rate or False Non-Match Rate (FRR or FNMR)** – the probability that the system fails to detect a match between the input pattern and a matching template in the database. It measures the percent of valid inputs which are incorrectly rejected.

- **Receiver Operating Characteristic or Relative Operating Characteristic (ROC)** – The ROC plot is a visual characterization of the trade-off between the FAR and the FRR. In general, the matching algorithm performs a decision based on a threshold which determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be less false non-matches but more false accepts. Correspondingly, a higher threshold will reduce the FAR but increase the FRR.

- **Equal Error Rate or Crossover Error Rate (EER or CER)** – the rate at which both accept and reject errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is most accurate. Obtained from the ROC plot by taking the point where FAR and FRR have the same value.

Other metrics which are related to the sensor devices are Failure to Enroll Rate (FTE), Failure to Capture Rate (FTC) & Template Capacity. As FAR and FRR are interdependent, it is more meaningful to plot them against each other, as shown in Fig.1.11 Each point on the plot represents a hypothetical system’s performance at various sensitivity settings. With such a plot, you can compare these rates to determine the crossover error rate (Equal Error Rate). Lower the
CER (EER), more accurate the system. Generally physiological biometric traits are more accurate than behavioral biometrics [1], [6].

1.6 Uses for Biometrics

Security systems use biometrics for two basic purposes: to verify or to identify users. Identification tends to be the more difficult of the two uses because a system must search a database of enrolled users to find a match (a one-to-many search). The biometric that a security system employs depends in part on what the system is protecting and what it is trying to protect against. Main application domains are as follows.

1.6.1 Physical Access [3], [6], [13], [14]

For decades, many highly secure environments have used biometric technology for entry access. Today, the primary application of biometrics is in physical security: to control access to secure locations (rooms or buildings). Unlike photo identification cards, which a security guard must verify, biometrics permit manned access control.

1.6.2 Virtual Access [1], [15]

For a long time, biometric-based network and computer access were areas often discussed but rarely implemented. Recently, however, the unit price of biometric devices has fallen dramatically, and several designs aimed squarely at this application are on the market. Analysts see virtual access as the application that will
provide the critical mass to move biometrics for network and computer access from the realm of science-fiction devices to regular system components. At the same time, user demands for virtual access will raise public awareness of the security risks and lower resistance to the use of biometrics.

1.6.3 E-commerce Applications [1], [15], [16], [17],[18]

E-commerce developers are exploring the use of biometrics and smart cards to more accurately verify a trading party’s identity. For example, many banks are interested in this combination to better authenticate customers and ensure nonrepudiation of online banking, trading, and purchasing transactions. Point-of-sales (POS) system vendors are working on the cardholder verification method [19], which would enlist smart cards and biometrics to replace signature verification. MasterCard estimates that adding smart-card-based biometric authentication to a POS credit card payment will decrease fraud by 80 percent [20].

1.6.4 Covert Surveillance [1], [2]

One of the more challenging research areas involves using biometrics for covert surveillance. Using facial and body recognition technologies, researchers hope to use biometrics to automatically identify known suspects entering buildings or traversing crowded security areas such as airports. The use of biometrics for covert identification as opposed to authentication must overcome technical challenges such as simultaneously identifying multiple subjects in a crowd and working with uncooperative subjects. In these situations, devices cannot count on consistency in pose, viewing angle, or distance from the detector.

1.7 Multimodal Biometrics

We have discussed biometric systems based on only one biometric trait or methodology of identification i.e., they rely on the evidence of a single source of information for authentication; such systems are called as unimodal biometric systems.

1.7.1 Need for Multimodal Biometrics [21],[22],[23]

For any unimodal system 100% accuracy is not possible and besides this they suffer from problems such as noise in sensed data, intra-class variations, inter-class similarities, non-universality & spoof attacks. Another thing is that as the enrolled population increases the feature vector space becomes crowded and it
becomes difficult to classify these vectors correctly. Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity [22]. Such systems, known as multimodal biometric systems, are expected to be more reliable due to the presence of multiple & (fairly) independent pieces of evidence [23]. Their decisions are combined through fusion techniques implementing “AND” or “OR” rule, allowing user to be verified using either any one or both the modalities.

1.7.2 Definition of Multimodal Biometrics

Multimodal biometrics refers to the use of a combination of two or more biometric modalities in a verification / identification system. Identification based on multiple biometrics represents an emerging trend. The most compelling reason to combine different modalities is to improve the recognition rate. This can be done when biometric features of different biometrics are statistically independent.

The International Committee for Information Technology Standards (INCITS) Technical Committee M1, Biometrics, and researchers have described methods for performing multi-biometric fusion [24], [25]. In general, the use of the terms multimodal or multi-biometric indicates the presence and use of more than one biometric aspect (modality, sensor, instance and/or algorithm) in some form of combined use for making a specific biometric verification/identification decision [24].

A multimodal system can combine any number of independent biometrics and overcome some of the limitations presented by using just one biometric as your verification tool. For instance, it is estimated that 5% of the population does not have legible fingerprints, a voice could be altered by a cold and face recognition systems are susceptible to changes in ambient light and the pose of the subject. A multimodal system, which combines the conclusions made by a number of unrelated biometrics indicators, can overcome many of these restrictions. Multimodal systems are generally much more vital to fraudulent technologies, because it is more difficult to forge multiple biometric characteristics than to forge a single biometric characteristic [21], [24].
1.7.3 Categories of Multimodal Biometric Systems

To further the understanding of the distinction among the multi-biometric categories [21], [26] they are briefly summarized in the following:

- **Multimodal** biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. For example, a system combining face and iris characteristics for biometric recognition would be considered a “multimodal” system regardless of whether face and iris images were captured by different or same imaging devices. It is not required that the various measures be mathematically combined in anyway. For example, a system with fingerprint and face recognition would be considered “multimodal” even if the “OR” rule was being applied, allowing users to be verified using either of the modalities.

- **Multi-algorithmic** biometric systems take a single sample from a single sensor and process that sample with two or more different algorithms. The technique could be applied to any modality. Algorithms can be designed to optimize performance under different circumstances.

- **Multi-instance** biometric systems use one sensor (or possibly multiple sensors) to capture samples of two or more different instances of the same biometric characteristics. For example, systems capturing images from multiple fingers are considered to be multi-instance rather than multimodal.

- **Multi-sensorial** biometric systems sample the same instance of a biometric trait with two or more distinctly different sensors. Processing of the multiple samples can be done with one algorithm or some combination of multiple algorithms. For example, a face recognition application could use both a visible light camera and an infrared camera coupled with specific frequency (or several frequencies) of infrared illumination.

Multimodal Biometric systems have following advantage over unimodal biometric systems

1. Systems are resistant to intra class similarity of data like facial feature. They combine more than one modality causing reduced intra-class similarity.
2. Noise resistance- Multimodal systems are more resistant to noise as compared to unimodal biometric systems, as they
have more than one modality more data is available for matching.

3. Less vulnerable to spoofing, as it is difficult to spoof more than one modality simultaneously.

As these are clear advantage we have to fight with following issues when it comes for implementation of multimodal biometric security system,

1. Interpretability – various systems using multimodal features must follow uniform rules for classification, these rules are not yet standardized.
2. Implementation Cost – Systems use more hardware and computational resources causing increased setup cost.
3. Reduced matching levels – Better decision fusion algorithms are required to attain higher matching levels in combination of biometric traits than the individual matching level.

All the above issues are being addressed by various researchers worldwide and this can lead to design of better Multimodal Biometric Systems in future.

1.7.4 Fusion in Multimodal Biometric Systems [22]

In multimodal biometrics we use more than one biometric modality hence we have more than one decision channels. We need to design a mechanism that can combine the classification results from each biometric channel; this is called as biometric fusion. Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths and diminish the weaknesses of the individual measurements. Fusion at matching score, rank and decision levels have been extensively studied in the literature [22], [27], [28]. Multimodal Biometrics with various levels of fusion such as sensor level, feature level, matching score level and decision level are possible. Multimodal biometric system can implement any of these fusion strategies or combination of them to improve the performance of the system. In this thesis we have mainly implemented feature level & score level fusion.

1.8 Problem Statement

In this thesis various biometric traits are studied in detail. The topic for research is ‘Biometric Authentication Systems’, it consists of unimodal as well as multimodal biometric systems. First unimodal biometrics implementations are focused and then the multimodal
systems using fusion techniques are implemented. Biometrics such as fingerprints, palmprints, finger-knuckle print, face, iris, online signatures, keystroke dynamics & their multimodal implementations are explored.

Main focus of research is to use image processing techniques for biometric identification, as many biometric traits like fingerprints, palmprints, face, iris etc. are represented by images. We have developed algorithms based on image and signal processing for pre-processing, feature extraction and matching of various biometric traits. Image processing techniques based on spatial as well as frequency domain image enhancement, wavelets, transforms & vector quantization are used.

Improvement in the results by fusion of unimodal biometrics is discussed. The biometric traits tend to vary with ageing; technique to improve performance of biometric system using multimodal approach is presented in this work.