CHAPTER 2

DIGITAL IMAGE PROCESSING AND BIOMETRICS
BASED HUMAN IDENTIFICATION SYSTEMS

2.1 DIGITAL IMAGE PROCESSING

The process of receiving and analyzing visual information by digital computer is called Digital Image Processing and Scene Analysis. Digital Image Processing is a prevalently evolving field with growing applications in Science and Engineering. Image Processing holds the possibility of developing the ultimate machine that could perform the visual functions of all living beings. Many theoretical and technological breakthroughs are required before building such a machine i.e., there is an abundance of Image Processing applications that can serve mankind with the available and anticipated technology in the near future. Imaging began in the 19th century with photography and continued with X-rays, television and electronic scanning in the 20th century. Image Processing as a field of study began in 1950s with pictures of the earth from high-flying spy airplanes and then with pictures of the earth’s surface taken from orbiting satellites.

Processing of an image includes improvement in its appearance and efficient representation. So the field consists of not only feature extraction, analysis and recognition of images, but also coding, filtering, enhancement and restoration. The entire process of Image Processing and analysis starting from the receiving of visual information to the giving out of description of the
scene, may be divided into three major stages which are also considered as major sub-areas and given below:

- **Discretization and Representation**: Converting visual information into a discrete form; suitable for computer processing; approximating visual information to save storage space as well as time requirement in subsequent processing.

- **Processing**: Improving image quality by filtering etc.; compressing data to save storage and channel capacity during transmission.

- **Analysis**: Extracting image features; quantifying shapes, registration and recognition.

### 2.2 BIOMETRIC TECHNOLOGY

The emerging field of biometric technology addresses the automated identification of individuals, based on their physiological and behavioural traits. The broad category of human authentication schemes, denoted as biometrics encompasses many techniques from Computer Vision and Pattern Recognition. The personal attributes used in a biometric identification system can be physiological, such as facial features, fingerprints, iris, retinal scans, hand and finger geometry; or behavioural, the traits idiosyncratic of the individual, such as voice print, gait, signature and key stroking. Depending on the complexity or the security level of the application, one will opt to use one or more of these personal characteristics.

Biometric system has been actively emerging in various industries for the past few years, and it is continuing to roll to provide higher security features for access control system. Many types of unimodel biometric systems
have been developed and deployed, for example fingerprint, face, speaker, palmprint and hand geometry verification systems. However, these systems are only capable of providing low to middle range of security features. Thus, for higher security feature, the combination of two or more single-model biometrics (also known as multimodel biometrics) is required. In addition, the industry is currently exploring the characteristics of multimodel biometric that are reliable, able to provide high security features, non-intrusive and widely accepted by the public.

Hybrid model biometrics has significant functional advantages over single biometrics, for example, elimination of False Acceptance Rate (FAR) (by adjusting FAR=0%) without suffering from increase occurrence of False Rejection Rate (FRR). In practice, it is difficult to obtain both FAR and FRR to be equal to zero in a single-model biometric verification measurement space. The biometrics industry emphasises heavily on security issues relating to choosing the lowest FAR with relaxed FRR requirement. This often causes high FRR and results in the increase of rejection of valid users. Denial of access by failing to identify genuine user would have adverse effects in the usability and public acceptance of the biometrics system. In fact, both aspects are significant obstacles to the wide deployment of the biometric technology.

2.3 BIOLOGICAL MEASUREMENTS

Any human physiological and/or behavioural characteristic can be used as a biometric characteristic as long as it satisfies the following requirements:

- **Universality**: each person should have the characteristic.
- **Distinctiveness**: any two persons should be sufficiently different in terms of the characteristic.
• **Permanence:** the characteristic should be sufficiently invariant (with respect to the matching criterion) over a period of time.

• **Collectability:** the characteristic can be measured quantitatively.

However, in a practical biometric system (i.e., a system that employs biometrics for personal recognition), there are a number of other issues to be considered, including:

• **Performance:** refers to the achievable recognition accuracy and speed, the resources required to achieve the desired recognition accuracy and speed, as well as the operational and environmental factors that affect the accuracy and speed.

• **Acceptability:** indicates the extent to which people are willing to accept the use of a particular biometric identifier (characteristic) in their daily lives.

• **Circumvention:** 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 (Jain, Ross and Prabhakar 2004).

### 2.4 BIOMETRIC SYSTEM

A biometric system is essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature
set from the acquired data, and comparing this feature set against the template set in the database. Depending on the application context, a biometric system may operate either in verification mode or identification mode.

- **In the verification mode**, the system validates a person’s identity by comparing the captured biometric data with his/her own biometric template(s) stored in the system database. In such a system, an individual who desires to be recognized claims an identity, usually via a personal identification number (PIN), a user name, or a smart card, and the system conducts a one-to-one comparison to determine whether the claim is true or not (e.g., “Does this biometric data belong to Bob?”). Identity verification is typically used for positive recognition, where the aim is to prevent multiple people from using the same identity.

- **In the identification mode**, the system recognizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual’s identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity (e.g., “Whose biometric data is this?”). Identification is a critical component in negative recognition applications where the system establishes whether the person is who he/she (implicitly or explicitly) denies to be. The purpose of negative recognition is to prevent a single person from using multiple identities. Identification may also be used in positive recognition for convenience (the user is not required to claim an identity). While traditional methods of personal recognition such as passwords, PINs, keys, and tokens may
work for positive recognition, negative recognition can only be established through biometrics (Jain, Ross and Prabhakar 2004).

2.4.1 Modules in the Biometric System

A biometric system is designed using the following four main modules (Figure 2.1).

(i) **Sensor module**, which captures the biometric data of an individual. An example is a fingerprint sensor that images the ridge and valley structure of a user’s finger.

(ii) **Feature extraction module**, in which 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.

(iii) **Matcher 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.
(iv) **System database module** 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

![Figure 2.1 Modules of a biometric system](image-url)
representation of the characteristic. The data are captured 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.

2.4.2 Comparison of various Biometrics

A number of biometric characteristics exist and are in use in various applications (Figure 2.2). Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. In other words, no biometric is ‘optimal’. The match between a specific biometric and an application is determined depending upon the operational mode of the application and the properties of the biometric characteristic. A brief introduction to the commonly used biometrics is given below:

- **DNA**: Deoxyribonucleic acid (DNA) is the one-dimensional (1-D) ultimate unique code for one’s individuality except for the fact that identical twins have identical DNA patterns. It is, however, currently used mostly in
the context of forensic applications for person recognition. Three issues limit
the utility of this biometrics for other applications:

(1) **Contamination and sensitivity:** it is easy to steal a piece of
DNA from an unsuspecting subject that can be subsequently
abused for an ulterior purpose.

(2) **Automatic real-time recognition issues:** the present
technology for DNA matching requires cumbersome
chemical methods (wet processes) involving an expert’s
skills and is not geared for on-line noninvasive recognition;
and

(3) **Privacy issues:** information about susceptibilities of a
person to certain diseases could be gained from the DNA
pattern and there is a concern that the unintended abuse of
genetic code information may result in discrimination, e.g.,
in hiring practices.

**Ear:** It has been suggested that the shape of the ear and the structure of
the cartilegenous tissue of the pinna are distinctive. The ear recognition
approaches are based on matching the distance of salient points on the pinna
from a landmark location on the ear. The features of an ear are not expected to
be very distinctive in establishing the identity of an individual.
Figure 2.2  Examples of biometric characteristics
• **Face**: Face recognition is a nonintrusive method, and facial images are probably the most common biometric characteristic used by humans to make a personal recognition. The applications of facial recognition range from a static, controlled ‘mug-shot’ verification to a dynamic, uncontrolled face identification in a cluttered background (e.g., airport). The most popular approaches to face recognition are based on either:

1. The location and shape of facial attributes such as the eyes, eyebrows, nose, lips and chin, and their spatial relationships, or
2. The overall (global) analysis of the face image that represents a face as a weighted combination of a number of canonical faces.

While the verification performance of the face recognition systems that are commercially available is reasonable, they impose a number of restrictions on how the facial images are obtained, sometimes requiring a fixed and simple background or special illumination. These systems also have difficulty in recognizing a face from images captured from two drastically different views and under different illumination conditions. It is questionable whether the face itself, without any contextual information, is sufficient for recognizing a person from a large number of identities with an extremely high level of confidence. In order, for a facial recognition system to work well in practice, it should automatically:

1. Detect whether a face is present in the acquired image;
2. Locate the face if there is one; and
3. Recognize the face from a general viewpoint (i.e., from any pose).
- **Facial, hand, and hand vein infra-red thermogram:** The pattern of heat radiated by human body is a characteristic of an individual and can be captured by an infra-red camera in an unobtrusive way much like a regular (visible spectrum) photograph. The technology could be used for covert recognition. A thermogram-based system does not require contact and is noninvasive, but image acquisition is challenging in uncontrolled environments, where heat emanating surfaces (e.g., room heaters and vehicle exhaust pipes) are present in the vicinity of the body. A related technology using near infrared imaging is used to scan the back of a clenched fist to determine hand vein structure. Infra-red sensors are prohibitively expensive which is a factor inhibiting wide spread use of the thermograms.

- **Fingerprint:** Humans have used fingerprints for personal identification for many centuries and the matching accuracy using fingerprints has been shown to be very high. A fingerprint is the pattern of ridges and valleys on the surface of a fingertip, the formation of which is determined during the first seven months of fetal development. Fingerprints of identical twins are different and so are the prints on each finger of the same person. Today, a fingerprint scanner costs about U.S. $20 when ordered in large quantities and the marginal cost of embedding a fingerprint-based biometric in a system (e.g., laptop computer) has become affordable in a large number of applications.

The accuracy of the currently available fingerprint recognition systems is adequate for verification systems and small-to-medium-scale identification systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale recognition involving millions of identities. One problem with the current fingerprint recognition systems is that they require a large amount of computational resources, especially when operating in the identification mode. Finally,
fingerprints of a small fraction of the population may be unsuitable for automatic identification because of genetic factors, aging, environmental, or occupational reasons (e.g., manual workers may have a large number of cuts and bruises on their fingerprints that keep changing).

- **Gait**: Gait is the peculiar way one walks and is a complex spatio-temporal biometric. Gait is not supposed to be very distinctive, but is sufficiently discriminatory to allow verification in some low-security applications. Gait is a behavioural biometric and may not remain invariant, especially over a long period of time, due to fluctuations in body weight, major injuries involving joints or brain, or due to inebriety. Acquisition of gait is similar to acquiring a facial picture and, hence, may be an acceptable biometric. Since gait-based systems use the video-sequence footage of a walking person to measure several different movements of each articulate joint, it is input intensive and computationally expensive.

- **Hand and finger geometry**: Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. Commercial hand geometry-based verification systems have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. The geometry of the hand is not known to be very distinctive and hand geometry-based recognition systems cannot be scaled up for systems requiring identification of an individual from a large population. Further, hand geometry information may not be invariant during the growth period of children. In addition, an individual’s jewelry (e.g., rings) or limitations in dexterity (e.g., from arthritis), may pose further challenges in extracting the correct hand geometry
information. The physical size of a hand geometry-based system is large, and it cannot be embedded in certain devices like laptops. There are verification systems available that are based on measurements of only a few fingers (typically, index and middle) instead of the entire hand. These devices are smaller than those used for hand geometry, but still much larger than those used in some other biometrics (e.g., fingerprint, face, voice).

• **Iris:** The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The visual texture of the iris is formed during fetal development and stabilizes during the first two years of life. The complex iris texture carries very distinctive information useful for personal recognition. The accuracy and speed of currently deployed iris-based recognition systems is promising and point to the feasibility of large-scale identification systems based on iris information. Each iris is distinctive and, like fingerprints, even the irises of identical twins are different. It is extremely difficult to surgically tamper the texture of the iris. Further, it is rather easy to detect artificial irises (e.g., designer contact lenses). Although, the early iris-based recognition systems required considerable user participation and were expensive, the newer systems have become more user-friendly and cost effective.

• **Keystroke:** It is hypothesized that each person types on a keyboard in a characteristic way. This behavioural biometric is not expected to be unique to each individual but it offers sufficient discriminatory information to permit identity verification. Keystroke dynamics is a behavioural biometric; for some individuals, one may expect to observe large variations in typical typing patterns. Further, the keystrokes of a person using a system could be monitored unobtrusively as that person is keying in information.
• **Odor**: It is known that each object exudes an odor that is characteristic of its chemical composition and this could be used for distinguishing various objects. A whiff of air surrounding an object is blown over an array of chemical sensors, each sensitive to a certain group of (aromatic) compounds. A component of the odor emitted by a human (or any animal) body is distinctive to a particular individual. It is not clear if the invariance in the body odor could be detected despite deodorant smells, and varying chemical composition of the surrounding environment.

• **Palmprint**: The palms of the human hands contain pattern of ridges and valleys much like the fingerprints. The area of the palm is much larger than the area of a finger and, as a result, palmprints are expected to be even more distinctive than the 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. Finally, when using a high-resolution palmprint scanner, all the features of the palm such as hand geometry, ridge and valley features (e.g., minutiae and singular points such as deltas), principal lines, and wrinkles may be combined to build a highly accurate biometric system.

• **Retinal scan**: The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometric since it is not easy to change or replicate the retinal vasculature. The image acquisition requires a person to peep into an eye-piece and focus on a specific spot in the visual field so that a predetermined part of the retinal vasculature could be imaged. The image acquisition involves cooperation of the subject, entails contact with the eyepiece, and requires a conscious effort on the part of the user. All these
factors adversely affect the public acceptability of retinal biometric. Retinal vasculature can reveal some medical conditions, e.g., hypertension, which is another factor deterring the public acceptance of retinal scan-based biometrics.

- **Signature**: The way a person signs his or her name is known to be a characteristic of that individual. Although signatures require contact with the writing instrument and an effort on the part of the user, they have been accepted in government, legal, and commercial transactions as a method of verification. Signatures are a behavioural biometric that change over a period of time and are influenced by physical and emotional conditions of the signatories. Signatures of some people vary substantially: even successive impressions of their signature are significantly different. Further, professional forgers may be able to reproduce signatures that fool the system.

- **Voice**: Voice is a combination of physiological and behavioural biometrics. The features of an individual’s voice are based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips) that are used in the synthesis of the sound. These physiological characteristics of human speech are invariant for an individual, but the behavioural part of the speech of a person changes over time due to age, medical conditions (such as a common cold), and emotional state, etc. Voice is also not very distinctive and may not be appropriate for large-scale identification.

A text-dependent voice recognition system is based on the utterance of a fixed predetermined phrase. A text-independent voice recognition system recognizes the speaker independent of what he/she speaks. A text-independent system is more difficult to design than a text-dependent system but offers more protection against fraud. A disadvantage of voice-based recognition is that speech features are sensitive to a number of factors such as background
noise. Speaker recognition is most appropriate in phone-based applications but the voice signal over phone is typically degraded in quality by the microphone and the communication channel.

A brief comparison of the above biometric techniques based on seven factors is provided in Table 2.1. 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.

Table 2.1 Comparison of various biometric technologies

<table>
<thead>
<tr>
<th>Biometric identifier</th>
<th>Universality</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>L</td>
<td>H</td>
<td>L</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>M</td>
<td>H</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>H</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>M</td>
<td>M</td>
<td>H</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>L</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>L</td>
<td>M</td>
<td>M</td>
</tr>
<tr>
<td>Odor</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>L</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>H</td>
<td>L</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>L</td>
<td>H</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>
</tbody>
</table>
For example, it is well known that both the fingerprint-based and iris-based techniques are more accurate than the voice-based technique. However, in a tele-banking application, the voice-based technique may be preferred since it can be integrated seamlessly into the existing telephone system.

2.4.3 Applications of Biometric Systems

The applications of biometrics can be divided into the following three main groups.

- **Commercial** applications such as computer network login, electronic data security, e-commerce, Internet access, ATM, credit card, physical access control, cellular phone, medical records management, and distance learning.

- **Government** applications such as national ID card, correctional facility, driver’s license, social security, welfare disbursement, border control, and passport control.

- **Forensic** applications such as corpse identification, criminal investigation, terrorist identification, parenthood determination, and missing children.

2.4.4 Limitations of (Unimodel) Biometric Systems

The successful installation of biometric systems in various civilian applications does not imply that biometrics is a fully solved problem. Table 2.2 presents the state-of-the-art error rates of three popular biometric traits. It is clear that there is plenty of scope for improvement in biometrics.
Researchers are not only addressing issues related to reducing error rates, but they are also looking at ways to enhance the usability of biometric systems.

Table 2.2  Error rates associated with fingerprint, face, and voice biometric systems

<table>
<thead>
<tr>
<th>Biometric systems</th>
<th>Test</th>
<th>Test Parameter</th>
<th>FNMR</th>
<th>FMR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fingerprint</td>
<td>FVC 2002</td>
<td>Users mostly in the age group 20-39</td>
<td>0.2%</td>
<td>0.2%</td>
</tr>
<tr>
<td>Face</td>
<td>FRVT 2002</td>
<td>Enrollment and test images were collected in indoor environment and could be on different days</td>
<td>10%</td>
<td>1%</td>
</tr>
<tr>
<td>Voice</td>
<td>NIST 2000</td>
<td>Text dependent</td>
<td>10-20%</td>
<td>2-5%</td>
</tr>
</tbody>
</table>

Biometric systems that operate using any single biometric characteristic have the following limitations.

(i) **Noise in sensed data.** The sensed data might be noisy or distorted. Fingerprints with a scar or a voice altered by cold are examples of noisy data. Noisy data could also be the result of defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavorable ambient conditions (e.g., poor illumination of a user’s face in a face recognition system). Noisy biometric data may be incorrectly matched with templates in the database resulting in a user being incorrectly rejected.
(ii) **Intra-class variations.** The biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment, thereby affecting the matching process. This variation is typically caused by a user who is incorrectly interacting with the sensor or when sensor characteristics are modified (e.g., by changing sensors—the sensor interoperability problem) during the verification phase. As another example, the varying psychological make-up of an individual might result in vastly different behavioural traits at various time instances.

(iii) **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. Golfarelli *et al.* have shown that the information content (number of distinguishable patterns) in two of the most commonly used representations of hand geometry and face are only of the order of and, respectively. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.

(iv) **Nonuniversality.** While every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users not to possess a particular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor quality of the ridges. Thus, there is a Failure To Enroll (FTE) rate associated with using a single biometric trait. It has been empirically estimated that as
much as 4% of the population may have poor quality fingerprint ridges that are difficult to image with the currently available fingerprint sensors and result in FTE errors.

(v) **Spoof attacks.** An impostor may attempt to spoof the biometric trait of a legitimate enrolled user in order to circumvent the system. This type of attack is especially relevant when behavioural traits such as signature and voice are used. However, physical traits are also susceptible to spoof attacks. For example, it has been demonstrated that it is possible (although difficult and cumbersome and requires the help of a legitimate user) to construct artificial fingers/fingerprints in a reasonable amount of time to circumvent a fingerprint verification system.

### 2.5 HYBRID MODEL BIOMETRIC SYSTEMS

Some of the limitations imposed by unimodel biometric systems can be overcome by using multiple biometric modalities (such as face and fingerprint of a person or multiple hand fingers of a person). Such systems, known as Hybrid model Biometric 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 stringent performance requirements imposed by various applications.

Hybrid model Biometric Systems address the problem of nonuniversality, since multiple traits ensure sufficient population coverage. Further, hybrid model biometric systems provide antispoofing measures by making it difficult for an intruder to simultaneously spoof the multiple
biometric traits of a legitimate user. By asking the user to present a random subset of biometric traits (e.g., right index and right middle fingers, in that order), the system ensures that a ‘live’ user is indeed present at the point of data acquisition. Thus, a challenge-response type of authentication can be facilitated using hybrid model biometric systems.

2.6 SOCIAL ACCEPTANCE AND PRIVACY ISSUES

Human factors dictate the success of a biometric-based identification system to a large extent. The ease and comfort in interaction with a biometric system contribute to its acceptance. For example, if a biometric system is able to measure the characteristic of an individual without contact, such as those using face, voice, or iris, it may be perceived to be more user-friendly and hygienic. Additionally, biometric technologies requiring very little cooperation or participation from the users (e.g., face and face thermograms) may be perceived as being more convenient to users. On the other hand, biometric characteristics that do not require user participation can be captured without the knowledge of the user, and this is perceived as a threat to privacy by many individuals.

The very process of recognition leaves behind trails of private information. For example, if a person is identified each time he/she makes a purchase, information about where this person shops and what he/she buys can be simply collected and used by telemarketers to invade his/her privacy. The issue of privacy becomes more serious with biometric-based recognition systems because biometric characteristics may provide additional information about the background of an individual. For example, retinal patterns may provide medical information about diabetes or high blood pressure in an individual. A health insurance company may use this information in an unethical way for economic gains by denying benefits to a person determined
to be of high risk. More importantly, people fear that biometric identifiers could be used for linking personal information across different systems or databases.

On the positive side, biometrics can be used as one of the most effective means for protecting individual privacy. In fact, biometrics ensures privacy by safeguarding identity and integrity. Nevertheless, many people are uneasy about the use of their personal biological characteristics in corporate or government recognition systems. To alleviate these fears, companies and agencies that operate biometric systems have to assure the users of these systems that their biometric information remains private and is used only for the expressed purpose for which it was collected. Legislation is necessary to ensure that such information remains private and that its misuse is appropriately punished.

Most of the commercial biometric systems available today do not store the sensed physical characteristics in their original form but, instead, they store a digital representation (a template) in an encrypted format. This serves two purposes. First, the actual physical characteristic cannot be recovered from the digital template thus ensuring privacy. Second, the encryption ensures that only the designated application can use this template.

2.7 AN OVERVIEW OF SEGMENTATION

In computer vision, segmentation refers to the process of partitioning a digital image into multiple regions (sets of pixels). The goal of segmentation is to simplify and/or change the representation of an image into something that is more meaningful and easier to analyze. Image segmentation is typically used to locate objects and boundaries (lines, curves, etc.) in images. The result of image segmentation is a set of regions that collectively
cover the entire image, or a set of contours extracted from the image (see edge detection). Each of the pixels in a region are similar with respect to some characteristic or computed property, such as colour, intensity, or texture. Adjacent regions are significantly different with respect to the same characteristic(s). Some of the practical applications of image segmentation are:

- Medical Imaging
- Locate tumors and other pathologies
- Measure tissue volumes
- Computer-guided surgery
- Diagnosis
- Treatment planning
- Study of anatomical structure
- Locate objects in satellite images (roads, forests, etc.)
- Face recognition
- Automatic traffic controlling systems
- Machine vision

Several general-purpose algorithms and techniques have been developed for image segmentation. Since there is no general solution to the image segmentation problem, these techniques often have to be combined with domain knowledge in order to effectively solve an image segmentation problem for a problem domain.
As far as human beings are concerned, an image is not just a random collection of pixels: it is a meaningful arrangement of regions and objects. In image analysis and computer vision, by segmentation is meant the ‘labeling’ of pixels as belonging to the same region, where the criteria for the pixel to belong to a particular region are

- Common colour or gray scale (or near enough via quantization)
- Membership of common texture region

Image segmentation was, is and will be a major research topic for many image processing researchers. The reasons are obvious and applications endless: most computer vision and image analysis problems require a segmentation stage in order to detect objects or divide the image into regions which can be considered homogeneous according to a given criterion, such as colour, motion, texture, etc.

Clustering is the search for distinct groups in the feature space. It is expected that these groups have different structures and that can be clearly differentiated. The clustering task separates the data into number of partitions, which are volumes in the n-dimensional feature space. These partitions define a hard limit between the different groups and depend on the functions used to model the data distribution. There also exists a variety of images: natural scenes, paintings, etc. Despite the large variations of these images, humans have no problem to interpret them.

Image segmentation is the first step in image analysis and pattern recognition. It is a critical and essential component of image analysis system. It is one of the most difficult tasks in image processing, and determines the
quality of the final result of analysis. Image segmentation is the process of dividing an image into different regions such that each region is homogeneous.

2.7.1 Amplitude Thresholding

This technique is used in segmentation of binary images such as printed documents, line drawings and graphics, multispectral and colour images, X ray images and so on. Threshold selection is an important step in this method. Some commonly used approaches are as follows.

- Histogram of the image is examined for locating peaks and valleys. If it is multimodel, then the valleys are used for selecting thresholds.
- Threshold (t) is selected so that a predetermined fraction (n) of the total number of samples is below t.
- Adaptively threshold by examining local neighborhood histograms.
- Selectively thresholds by examining histograms only of those points that satisfy a chosen criterion.

2.7.2 Component Labeling

A simple and effective method of segmentation of binary images is by examining the connectivity of pixels with their neighbors and labeling the connected sets.
2.7.3 Boundary Based Approaches

Boundary extraction techniques segment objects on the basis of their profiles. Thus contour following, connectivity, edge linking and graph searching, curve fitting are applicable to image segmentation. These methods find it difficult to segment when objects are touching or overlapping or if a break occurs in the boundary due to noise in the image.

2.7.4 Clustering Based Methods

K-means clustering is an iterative technique that is used to partition an image into K clusters. The basic algorithm is:

1. Pick K cluster centers, either randomly or based on some heuristic
2. Assign each pixel in the image to the cluster that minimizes the variance between the pixel and the cluster center
3. Re-compute the cluster centers by averaging all of the pixels in the cluster
4. Repeat steps 2 and 3 until convergence is attained (e.g. no pixels change clusters)

In this case, variance is the squared or absolute difference between a pixel and a cluster center. The difference is typically based on pixel colour, intensity, texture, and location, or a weighted combination of these factors. K can be selected manually, randomly, or by a heuristic.

This algorithm is guaranteed to converge, but it may not return the optimal solution. The quality of the solution depends on the initial set of clusters and the value of K.
2.7.5 **Histogram-Based Methods**

Histogram-based methods are very efficient when compared to other image segmentation methods because they typically require only one pass through the pixels. In this technique, a histogram is computed from all of the pixels in the image, and the peaks and valleys in the histogram are used to locate the clusters in the image. Colour or intensity can be used as the measure.

A refinement of this technique is to recursively apply the histogram-seeking method to clusters in the image in order to divide them into smaller clusters. This is repeated with smaller and smaller clusters until no more clusters are formed.

One disadvantage of the histogram-seeking method is that it may be difficult to identify significant peaks and valleys in the image. This may affect the quality and usefulness of the final solution.

2.7.6 **Region-Growing Methods**

In the region-growing technique, a region is started with a single pixel. Adjacent pixels are recursively examined and added to the region if they are sufficiently similar to the region. If a pixel is too dissimilar to the current region, it is used to start a new region.

One variant of this technique, proposed by Haralick and Shapiro (1985), is based on pixel intensities. The mean and scatter of the region and the intensity of the candidate pixel is used to compute a test statistic. If the test statistic is sufficiently small, the pixel is added to the region, and the
region's mean and scatter are recomputed. Otherwise, the pixel is rejected, and is used to form a new region.

2.7.7 Model based Segmentation

By inner forces and forces which are computed from the image data, which pull the model towards the object boundary.

Statistical Models: if the object to be segmented is known beforehand, a statistical model can be used to serve as a template.

2.7.8 Template Matching

One direct method of segmenting an image is to match it against templates from a given list. The detected objects can then be segmented out and the remaining image can be analyzed by other techniques. This method can be used to segment busy images such as journal pages containing text and graphics. The text can be segmented by template matching techniques and graphics can be analyzed by boundary-based approaches.

2.7.9 Multi-scale Segmentation

Image segmentations are computed at multiple scales in scale-space and sometimes propagated from coarse to fine scales.

Segmentation criteria can be arbitrarily complex and may take into account global as well as local criteria. A common requirement is that each region must be connected in some sense.
2.7.10 **Semi-automatic Segmentation**

In this kind of segmentation, the user outlines the region of interest with the mouse clicks and algorithms are applied so that the path that best fits the edge of the image is shown.

2.7.11 **Neural Networks Segmentation**

That kind of segmentation relies on processing small areas of an image by the neural network or a set of neural networks. After such processing the decision-taking mechanism marks the areas of an image accordingly to the category recognized by the neural network.

2.8 **HAND GEOMETRY BASED HUMAN RECOGNITION**

As the name suggests, hand geometry is concerned with measuring the physical characteristics of the user’s hand and fingers, from a three-dimensional perspective. One of the most established methodologies, hand geometry offers a good balance of performance characteristics and is relatively easy to use. This methodology may be suitable where larger user bases or users who may access the system infrequently and may therefore be less disciplined in their approach to the system. Accuracy can be very high if desired, while flexible performance tuning and configuration can accommodate a wide range of applications. Hand geometry readers are deployed in a wide range of scenarios, including time and attendance recording where they have proved extremely popular. Ease of integration into other systems and processes, coupled to ease of use makes hand geometry an obvious first step for many biometric projects.
2.8.1 Why Hand Geometry?

There is no effective biometric measurement; each biometrics has its strengths and limitations, and accordingly each biometric appeals to a particular identification (authentication) application. Suitability of a particular biometric to a specific application depends upon several factors; among these factors, the user acceptability seems to be the most significant. For many access control applications, like immigration, border control and dormitory meal plan access, very distinctive biometrics, e.g., fingerprint and iris, may not be acceptable for the sake of protecting an individual's privacy. In such situations, it is desirable that the given biometric indicator be only distinctive enough for verification but not for identification. As hand geometry information is not very distinctive, it is one of the biometrics of choice in applications like those mentioned above.

Hand geometry-based authentication is also very effective for various reasons. Almost all of the working populations have hands and exception processing for people with disabilities could be easily engineered. Hand geometry measurements are easily collectible due to both the dexterity of the hand and due to a relatively simple method of sensing which does not impose undue requirements on the imaging optics. Note that good frictional skin is required by fingerprint imaging systems, and a special illumination setup is needed by iris or retina-based identification systems. Further, hand geometry is ideally suited for integration with other biometrics, in particular, fingerprints. For instance, an identification/verification system may use fingerprints for (infrequent) identification and use hand geometry for (frequent) verification. It is easy to conceptualize a sensing system, which can simultaneously capture both fingerprints and hand geometry.
2.8.2 Comparison of Hand Geometry and Fingerprints

Unlike fingerprints, the human hand is not unique. One can use finger length, thickness, and curvature for the purposes of verification but not for identification. For some kinds of access control like immigration and border control, invasive biometrics (e.g., fingerprints) may not be desirable as they infringe on privacy. In such situations it is desirable to have a biometric system that is sufficient for verification. As hand geometry is not distinctive, it is the ideal choice. Furthermore, hand geometry data is easier to collect. With fingerprint collection good frictional skin is required by imaging systems, and with retina-based recognition systems, special lighting is necessary.

2.8.3 Previous works

- A Hand Geometry-Based Verification System

  In this work the use of hand geometry is explored as a measure of a person's identity. The system consists of an acquisition device that captures the top view and side view of a user's right hand as user places it on the flat surface of the device. A snapshot of the user's hand is taken for processing. A set of features have been identified that could be used to represent a person's hand. These features include the lengths and widths of the fingers at various locations.

- Deformable Matching of Hand Shapes for Verification

  This work involves designing a mechanism that would align hand shapes prior to verifying a person's identity. Such an approach would enhance the integrity of the feature set made available during the verification stage.
Web-Access using Biometrics

This work involves securing a website using biometrics. Users are granted access to a set of files in a web-site after their identity has been verified using Biometrics - Hand Geometry in particular. Biometrics based web-access will add a new layer of security over existing web-security systems.

Hence Biometrics is identified as the research area and the literature collected is presented in the next chapter.