Chapter 1

Introduction
Chapter 1

Introduction

1.1 Biometrics

A wide variety of systems require reliable personal authentication schemes to either confirm or determine the identity of individuals requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed by a legitimate user, and not anyone else. Examples of these systems include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust authentication schemes, these systems are vulnerable to the wiles of an impostor.

Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to systems. However, security can be easily breached in these systems when a password is divulged to an unauthorized user or a card is stolen by an impostor; further, simple passwords are easy to guess (by an impostor) and difficult passwords may be hard to recall (by a legitimate user). The emergence of biometrics has addressed the problems that plague traditional verification methods. Biometrics refers to the automatic identification (or verification) of an individual (or a claimed identity) by using certain physiological or behavioral traits associated with the person. By using biometrics it is possible to establish an identity based on ‘who you are’, rather than by ‘what
you possess’ (e.g., an ID card) or ‘what you remember’ (e.g., a password). Biometric systems make use of fingerprints, hand geometry, iris, retina, face, hand vein, facial thermograms, signature, voiceprint, gait, palmprint, etc. (Figure 1.1) to establish a person’s identity [1, 2]. While biometric systems have their limitations [3], they have an edge over traditional security methods in that it is significantly difficult to lose, steal or forge biometric traits; further, they facilitate human recognition at a distance (e.g., face and gait).

(a) Fingerprint  (b)Face  (c)Hand Geometry
(d)Signature  (e)Iris  (f)Voice

Figure 1.1: Examples of some of the biometric traits used for authenticating an individual.
Biometric systems also introduce an aspect of user convenience that may not be possible using traditional security techniques. For example, users maintaining different passwords for different applications may find it challenging to recollect the password associated with a specific application. In some instances, the user might even forget the password, requiring the system administrator to intervene and reset the password for that user. A Meta Group study reports that a password-related help desk call may cost as much as $30 in terms of support staff time and money [4]. Maintaining, recollecting, and remembering passwords can, therefore, be a tedious and expensive task. Biometrics, on the other hand, addresses this problem effectively, thereby enhancing user convenience: a user can use different ‘passwords’ (biometric traits) for different applications, with ‘password’ recollection not being an issue at all.

A typical biometric system operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set against the template feature set in the database. In an identification scheme the comparison is done against templates corresponding to all the enrolled users in order to recognize the individual (a one-to-many matching); in a verification scheme, the comparison is done against only those templates corresponding to the claimed identity in order to verify the claim (a one-to-one matching). Thus, identification (“Whose biometric data is this?”) and verification (“Does this biometric data belong to DSK?”) are two different problems with different inherent complexities [5]. The templates are typically created at the time of enrollment, and depending on the application may or
may not require human personnel intervention. Figure 1.2 illustrates the enrollment and verification modules of a typical biometric system.

The verification problem may be formally posed as follows: given an input feature vector $X_Q$ and a claimed identity $I$, determine if $(I,X_Q)$ belongs to $\omega_1$ or $\omega_2$, where $\omega_1$ indicates that the claim is true (a genuine user) and $\omega_2$ indicates that the claim is false (an impostor). Typically, $X_Q$ is matched against $X_I$, the biometric template corresponding to user $I$, to determine its category. Thus,

$$
(I, X_Q) \in \begin{cases} 
  w_1 & \text{if } S(X_Q, X_I) \geq \eta, \\
  w_2 & \text{otherwise,}
\end{cases}
$$

(1.1)

where $S$ is the function that measures the similarity between $X_Q$ and $X_I$, and $\eta$ is a predefined threshold. Therefore, every claimed identity is classified as $w_1$ or $w_2$ based on the variables $X_Q$, $I$, $X_I$ and $\eta$, and the function $S$.

The identification problem, on the other hand, may be stated as follows: given an input feature vector $X_Q$, determine the identity $I_k$, $k \in \{1,2,...,N,N+1\}$. Here $I_1,I_2,...,I_N$ are the identities enrolled in the system, and $I_{N+1}$ indicates the reject case where no suitable identity can be determined. Hence,
where $X_{I_k}$ is the biometric template corresponding to identity $I_k$, $X_Q \in \left\{ I_k \text{ if } \max_k \{S(X_Q, X_{I_k})\} > \eta, k=1,2,\ldots,N, \right\}$ and $\eta$ is a predefined threshold.

Biometric systems are being increasingly deployed in large scale civilian applications (Figure 1.3). The Schiphol Privium scheme at the Amsterdam airport, for example, employs iris scan cards to speed up the passport and visa control procedures [6]. Passengers enrolled in this scheme insert their card at the gate and look into a camera; the camera acquires the eye image of the traveller and processes it to locate the iris, and compute the Iriscode [7]; the computed Iriscode is compared with the data residing in the card to complete user verification. A similar scheme is also being used to verify the identity of Schiphol airport employees working in high-security areas. Thus, biometric systems can be used to enhance user convenience while improving security.
Figure 1.2: The enrollment module and the verification module of a biometric system.
A simple biometric system has four important modules:

1. Sensor Module which captures the biometric data of an individual. An example is a fingerprint sensor that captures fingerprint impressions of a user.

2. Feature Extraction Module in which the acquired data is processed to extract feature values. For example, the position and orientation of minutiae points in a fingerprint image would be computed in the feature extraction module of a fingerprint system.

3. Matching Module in which the feature values are compared against those in the template by generating a matching score. For example, in this module, the number of matching minutiae between the query and the template can be computed and treated as a matching score.

4. Decision-making Module in which the user’s claimed identity is either accepted or rejected based on the matching score generated in the matching module (verification). Alternately, the system may identify a user based on the matching scores (identification).
Figure 1.3: Biometric systems in civilian applications. (a) A border passage system using iris recognition at London’s Heathrow airport (news.bbc.co.uk). (b) The INS Passenger Accelerated Service System (INSPASS) at JFK international airport (New York) uses hand geometry to authenticate travellers and significantly reduce their immigration inspection processing time (www.panynj.gov). (c) Ben Gurion airport in Tel Aviv (Israel) uses Express Card entry kiosks fitted with hand geometry systems for security and immigration (www.airportnet.org). (d) The FacePass system from Viisage is used in point-of-sale verification applications like ATMs, therefore, obviating the need for PINs (www.viisage.com). (e) Indivos’ “Pay by Touch” service uses fingerprints to help customers speed up payments in restaurants and cafeterias. When an enrolled customer places her finger on the sensor, the system retrieves her financial account and updates it (www.kioskbusiness.com). (f) The Identix TouchClock fingerprint system is used in time and attendance applications (www.cardsolutions.com).
1.2 Fingerprint as a Biometric

Among all biometric traits, fingerprints have one of the highest levels of reliability [8] and have been extensively used by forensic experts in criminal investigations. A fingerprint refers to the flow of ridge patterns in the tip of the finger. The ridge flow exhibits anomalies in local regions of the fingertip (Figure 1.4), and it is the position and orientation of these anomalies that are used to represent and match fingerprints. Although not scientifically established, fingerprints are believed to be unique across individuals, and across fingers of the same individual [9]. Even identical twins having similar DNA, are believed to have different fingerprints [10]. Traditionally, fingerprint patterns have been extracted by creating an inked impression of the fingertip on paper. The electronic era has ushered in a range of compact sensors that provide digital images of these patterns. These sensors can be easily incorporated into existing computer peripherals like the mouse or the keyboard (Figure 1.5), thereby making this mode of identification a very attractive proposition. This has led to the increased use of automatic fingerprint-based authentication systems in both civilian and law-enforcement applications.
Figure 1.4: A fingerprint image with the core and four minutiae points marked on it. The ridge pattern along with the core and delta points define the global configuration, while the minutiae points define the local structure.
Figure 1.5: Fingerprint sensors installed on (a) a keyboard (the Cherry Biometric Keyboard has a smart card reader and a fingerprint sensor attached to it); (b) a mouse (the ID Mouse manufactured by Siemens has a capacitance-based fingerprint sensor placed on a USB mouse).
1.2.1 Fingerprint Representation

The uniqueness of a fingerprint is determined by the topographic relief of its ridge structure and the presence of certain ridge anomalies termed as minutiae points. Typically, the global configuration defined by the ridge structure is used to determine the class [11, 12] of the fingerprint, while the distribution of minutiae points is used to match and establish the similarity between two fingerprints [13, 14]. Automatic fingerprint identification systems, that match a query print against a large database of prints (which can consist of millions of prints), rely on the pattern of ridges in the query image to narrow their search in the database (fingerprint indexing), and on the minutiae points to determine an exact match (fingerprint matching). The ridge flow pattern itself is seldom used for matching fingerprints.

1.2.2 Fingerprint Matching

Fingerprint matching techniques can be broadly classified as being minutiae-based or correlation-based. Minutiae-based techniques attempt to align two sets of minutiae points and determine the total number of matched minutiae [13,15, 16]. Correlation-based techniques, on the other hand, compare the global pattern of ridges and furrows to see if the ridges in the two fingerprints align [17, 18, 19]. The performance of minutiae-based techniques rely on the accurate detection of minutiae points and the use of sophisticated matching techniques to compare two minutiae sets which
undergo non-rigid transformations. The performance of correlation-based techniques is affected by non-linear distortions and noise present in the image. In general, it has been observed that minutiae-based techniques perform better than correlation-based ones. Correlation-based techniques suffer from the following problems [20]: (a) A fingerprint image may have non-linear warping due to the effect of pressing a convex elastic surface (the finger) on a flat surface (the sensor). Moreover, various sub-regions in the sensed image are distorted differently due to the non-uniform pressure applied by the user. It is difficult to compare two such distorted prints, even if translation and rotation effects are considered. (b) Based on the moisture content of the skin, the acquired images may have either thin or thick ridges. Further, the quality of the images acquired using the sensor may vary with time, thereby complicating the correlation process.

1.2.3 Difficulties and Challenges in Fingerprint Matching

Although the problem of automatic fingerprint matching has been extensively studied, it is nevertheless, not a fully solved problem. There are a variety of unresolved issues that need to be addressed effectively in this rather popular biometric technique. Some of the challenges are described below:

1. The new generation solid-state sensors are being increasingly used to acquire fingerprint images. These sensors when embedded in
compact systems like laptops, mouse, and cellular phones provide a small contact area (e.g., 0.6” x 0.6” in a Veridicom sensor) for the fingertip and, therefore, sense only a limited portion of the fingerprint. This complicates the problem of matching impressions due to the lack of sufficient minutiae information. It is, therefore, essential to augment minutiae information with alternate information available in fingerprints in order to deal with the issues introduced by partial fingerprint images.

2. Due to advancements in sensor technology, a variety of fingerprint sensors with different specifications are now available (Figure 1.6). However, a fingerprint matching system developed for a particular sensor is very often not compatible with images acquired using other sensors. This lack of inter-operability limits the utility of a matcher.

Figure 1.6: A variety of fingerprint sensors with different specifications (e.g., sensing technology, image size, image resolution, image quality, etc.) are now available.
3. The fingerprint matching performance is affected by the non-linear distortions present in the fingerprint image. These distortions are a consequence of the imaging process which requires the finger to be pressed against the sensor surface. To facilitate good matching performance, these distortions have to be accounted for prior to the matching stage.

4. While it is acknowledged that the fingerprints of a person do not change over time, it is possible for minor cuts and bruises to alter the ridge structure of fingerprints (Figure 1.7). Moreover, the moisture content of the fingertip may change over time affecting the quality of the fingerprint image being acquired from a user. The template fingerprint data obtained during enrollment time may not capture these variations. A protocol to update template data is necessary to maintain system performance.

5. Some users consistently provide poor quality fingerprints due to the dry nature of their skin (Figure 1.8). It is difficult to extract features from such poor quality images. Users providing such noisy fingerprint data might find it difficult to enroll in and interact with a biometric system that uses only fingerprints. To address this issue, a multibiometric system, that uses other biometric traits in addition to fingerprints, has to be considered.
Figure 1.7: Effect of noisy images on a fingerprint authentication system. 
(a) Fingerprint obtained from a user during enrollment. (b) Fingerprint obtained from the same user during verification. The development of scars or cuts can result in erroneous fingerprint matching results.
Figure 1.8: Non universality of fingerprints: Four different impressions of a subject’s finger exhibiting poor quality ridges. A fingerprint system might not be able to enroll this subject since minutiae information cannot be reliably extracted.