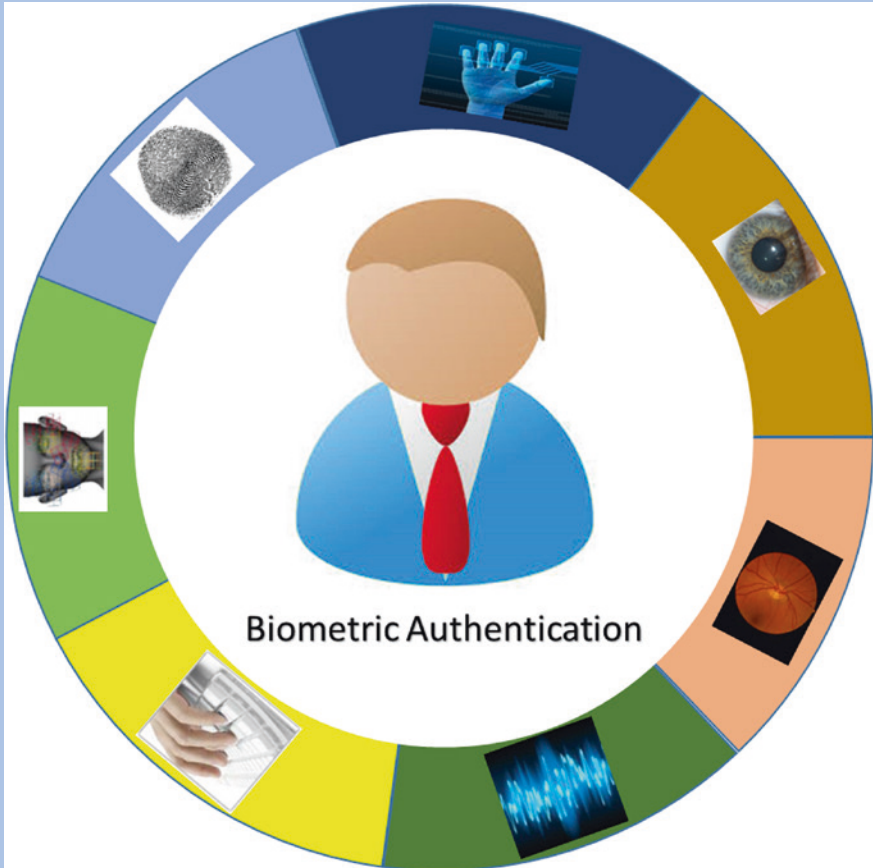


Biometric Authentication

Authentication through human characteristics



This chapter focuses on the biometric authentication process which helps to prevent unauthorized access to computing resources. This chapter focuses on the biometric authentication process which helps to prevent unauthorized access to computing resources. First, biometric authentication steps are discussed, and then the performance of each biometric modality is illustrated. Next sections provide details of physiological and behavioral biometrics along with the available applications where these authentication techniques are in wide used. The last section of the chapter discusses different known attacks of biometric systems along with possible remedies for each of them.

Introduction

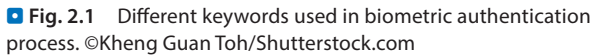
Biometric authentication (sometimes known as biometrics) is a process of recognizing individuals through their physiological and behavioral traits or attributes. The term 'Biometric' is a combination of two Greek words, namely Bio (life) and Metric (to measure), and it refers to a type of authentication «something that you are.» Hence, biometric authentication actually measures as well as analyzes the biological attributes of an individual. In many situations, biometric-based authentications are capable of providing better accuracy in identifying a user than typical password-based systems. ■ Figure 2.1 shows some most common keywords used in biometric-based authentication process.

The main reasons for using biometric authentication are as follows:

1. The risk of identity theft is significantly low compared with other authentication technologies, since it uses human biometric traits.
2. No need to remember any information while authenticating to use a system.
3. Biometric authentication modalities cannot be easily guessed by the hackers.
4. It is not possible to share the biometric information to any other person.

As security breaches have increased, it is now crucial to build a more secure identification and verification system for accessing online resources.

Some of the disadvantages of biometric authentication systems are:



1. Since the biometric features do not change frequently, in the case of compromise of an authentication system and the biometric data getting leaked, this confidential information may become public and abused.
2. Biometric authentication systems mainly depend on biometrics of all registered users. So disabled people and persons with some defects in required biometric cannot be authenticated using the biometric authentication system. For instance, fingerprint-based authentication is one of the widely used biometric today. If a person has an injury in the thumb, he is not able to authenticate at that time. Hence in airports or banks, there should be an alternate way of authentication other than a specific biometric.
3. One of the most concerning disadvantages of biometrics is privacy. As these authentication data are stored in a central database and are sometimes checked against this stored information from different places for identity verification.

fication, there is a risk of losing these personally identifiable information (PII) in the case of compromise of the database. Some people do not want to share their PII and are reluctant to use biometric authentication system.

4. The cost of developing biometric authentication system is relatively high. Also maintaining and updating the authentication database incurs additional cost than other types of authentication systems. For example, an iris scanner is more expensive than a typical keyboard where a user enters his/her password. The size of data that needs to be stored for the biometric authentication is much larger than that of a password database.

The International Biometric society [1] and other groups are continuously exploring new biometric traits which are easy to use, nonintrusive, and provide most accurate results in identification. A paper by Ricanek [2] published in Computer Magazine September 2014 issue titled «Beyond Recognition: The Promise of Biometric Analytics» mentioned that soon biometric analytics will be used as the discovery of potentially interesting information about a person other than verifying identity using biometric signal patterns.

Different Biometric Modalities

Biometric traits can be categorized in different ways based on their features and the way these are used for authentication. In general, those traits are categorized in two types, namely, physiological biometrics and behavioral biometrics [3].

Physiological biometrics are related to human body shape and features. With the change of this body geometry, these biometrics need to be updated to avoid failure of authentication. Some examples of this type are fingerprint, face, hand geometry, iris, retina, etc. In general, the accuracy of physiological biometrics is higher than behavioral biometrics. ■ Figure 2.2 shows fingerprint and hand geometry as examples of physiological biometrics.

Behavioral biometrics are related to certain kind of behavior of an individual. Hence, this authentication system can prevent a person from accessing a cyber-system, if his current behavior pattern is different from the stored behavioral pattern. Examples of this type of biometrics are—voice,



■ **Fig. 2.2** Examples of how physiological biometrics are used for authentication.
 ©Peshkova/Shutterstock.com ©Bruce Rolff/Shutterstock.com

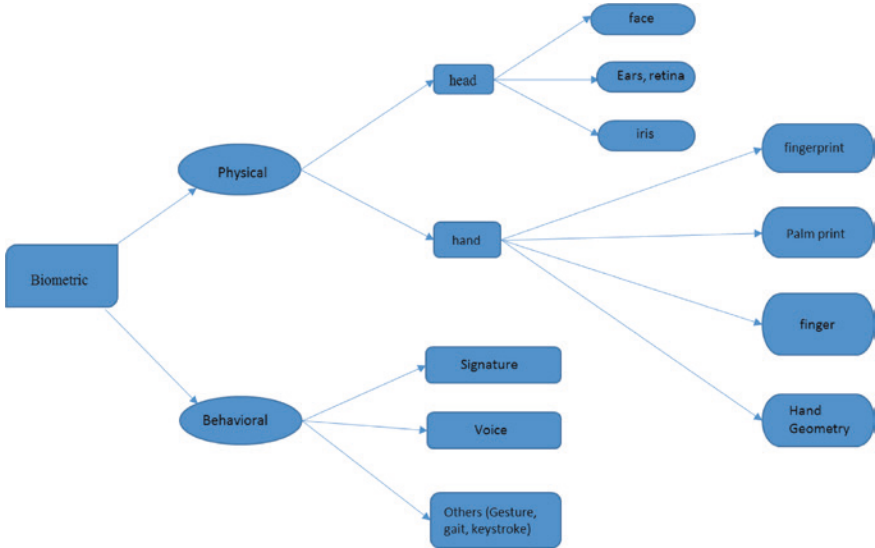


■ **Fig. 2.3** Illustration of behavioral biometrics use for authentication.
 ©Dmitri Mihhailov/Shutterstock.com © Elikes/Shutterstock.com

keystroke analysis, mouse dynamics, signature, gesture, etc.

■ Figure 2.3 shows keystrokes- and voice-based biometrics as examples of behavioral biometrics.

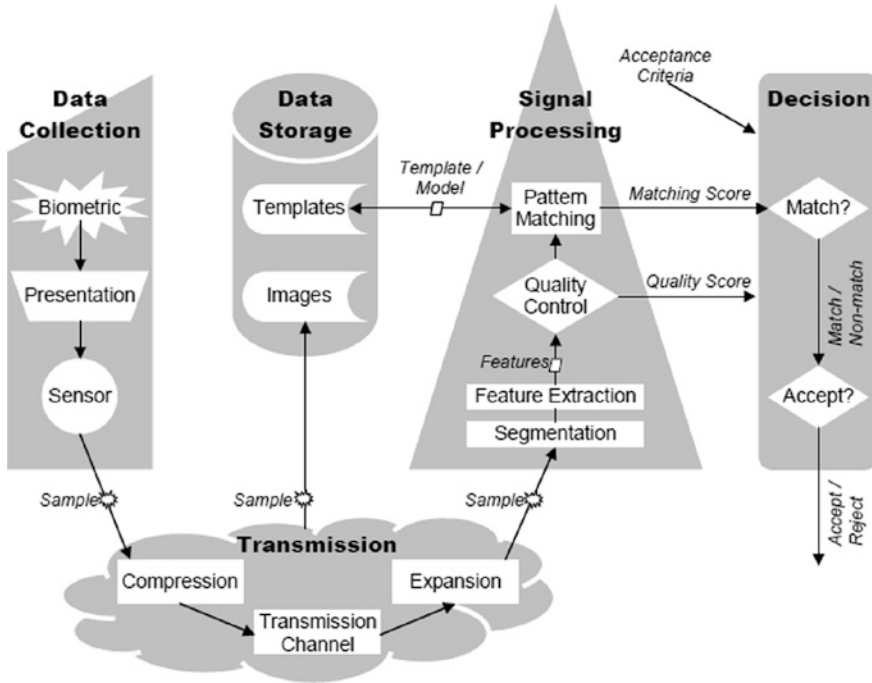
Different subcategories of these two categories [4] are shown in ■ Fig. 2.4. According to the figure, physical biometric is categorized in head and hand biometrics. Head biometrics include face, retina, iris and ear, while hand biometrics include fingerprint, palm print, hand geometry.



■ Fig. 2.4 Physiological and behavioral traits used in different biometric authentication [32]

Biometric Authentication Process

A biometric system is generally composed of four major components, namely, enrollment unit, feature extraction unit, template matching unit, and decision-making unit. Enrollment unit takes biometric inputs from an individual user, creates a template, and stores it in the database. During this process, a biometric reader scans person-specific biometric characteristics and then saves it in the digitized form. Feature extraction module takes the digitized input from the enrollment unit and produces a compact representation of the captured biometric data. This compact data is stored in the identity database for future use. The template matching unit does the comparison of the user's identity against the stored biometric in the database and calculates a score. In the case of biometric identification, the matching is performed on many-to-one basis (captured input with stored templates of multiple users). In case of biometric verification where prior identification was done, the matching of captured information is done as one to one with the stored database. The decision-making unit accepts or rejects a user based on the predefined threshold value of score and the calculated scores in the template matching unit. ■ Figure 2.5 describes the processes involved in biometric-based authentication. The basic steps are:



■ **Fig. 2.5** Basic steps in biometric-based authentication including data collection, data storage, processing of biometric data, and decision-making [33]

Data Collection: This step includes the sample collection procedure of biometric data from the sensor.

Transmission: This step uses compression techniques over the captured samples and transmits the output to the data storage unit. It also sends information to the signal processing unit.

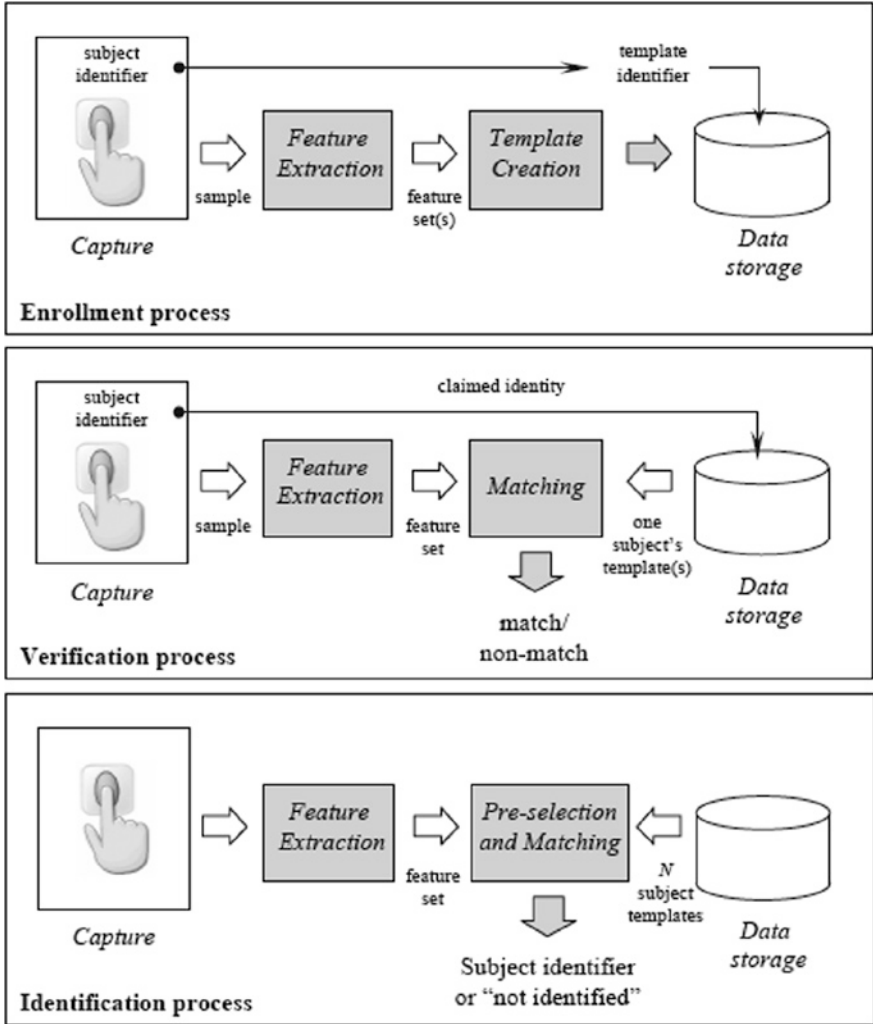
Data Storage: This unit gets the input from the transmission unit and stores the biometric images (sensor captured data) into different templates.

Signal Processing: This unit does segmentation and feature extraction steps to get the required features. Then it passes the features through quality control unit and pattern matching unit.

Decision: This unit computes the matching algorithm and gives accept or reject decision based on the quality score.

The enrollment, identification, and verification processes are shown in the flow diagram in ■ Fig. 2.6.

Enrollment process includes the capture of the biometric signal, extracting of features, the creation of templates, and storing the templates in the database.



■ Fig. 2.6 Enrollment, identification, and verification in a biometric system [5]

The *verification process* includes the capture of the biometric signal and extraction of the features from the captured biometric data. Then these sets of features are compared with the stored subject's template. The template is extracted for the claimed identity while capturing through biometric sensors.

The *identification process* also includes the capture of the biometric signal and extraction of the features from the captured biometric data. These extracted set of features are then compared with all the stored subject templates to identify the subject.

Performance Measures of Biometric Systems

The performance of biometric-based authentication systems is generally represented in terms of decision error rates—false acceptance rate and false rejection rate [5].

False Acceptance Rate (FAR)

In biometrics, the instance of incorrectly identifying an unauthorized person is referred to as a type II error or false acceptance. It is considered as the most serious biometric security error as it gives unauthorized users access to systems. Accordingly, the false acceptance rate (FAR) or false match rate (FMR) is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. FAR is calculated using the following formula:

$$\text{FAR}(\mu) = \frac{\text{Number of false successful attempts made in authenticating users}}{\text{Total number of attempts made in authenticating users}},$$

where ' μ ' is the security level.

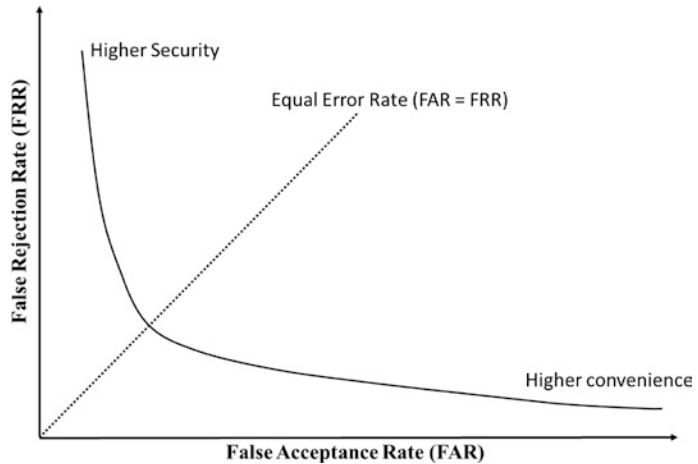
False Rejection Rate (FRR)

False rejection is a condition in biometric-based system, where an authorized person cannot be identified by the authentication process. False rejection rate (FRR) is the measure to calculate the chance of the biometric-based system failing to authenticate a legitimate user and is calculated as the probability of the system to fail in finding a match between an input biometric template and the registered biometric stored in the database. Sometimes it measures a ratio of false rejections and a total number of attempts to do authentication. The term 'rejection' refers to the claim of a user in biometric-based authentication system. It is also known as false non-match rate (FNMR).

$$\text{FRR}(\mu) = \frac{\text{Number of false reject made in authenticating genuine users}}{\text{Total number of attempts made in authenticating users}},$$

where ' μ ' is the security level.

The lower these FAR and FRR values, the better the biometric trait.



■ Fig. 2.7 The representation of FAR, FRR, and EER in receiver operating characteristic (ROC) curve

Equal Error Rate (EER)

This error rate is defined as the value obtained at some threshold level of a biometric system where the False Acceptance Rate (FAR) and False Rejection Rate (FRR) are the same. It is also called a crossover error rate.

In general, lower the equal error rate, the higher the accuracy of that biometric system. All available biometric systems have the capability of adjusting the sensitivity of these error rates. If the false positive is not desired, the system sensitivity can be set to require (nearly) perfect matches of the enrollment data and the input data of users. If FRR is not desired, the sensitivity value can be readjusted to accept the approximate matches of enrollment data and input data. The following ■ Fig. 2.7 (ROC curve) illustrates the threshold level to get the desired ERR value.

Other performance metrics are also used in biometric-based authentication systems such as *Image acquisition errors*. Irrespective of the accuracy of the matching algorithm in a biometric system, the performance of that system gets degraded in case of failing to properly enroll a user. Two examples of this type are failure to enroll rate (FTE) and failure to acquire rate (FTA).

Failure to Enroll Rate (FTE)

This error occurs due to a system's inability to generate the repeatable templates for a particular portion of the population. This can happen if a person does not have that biometric feature, a person cannot produce an image of significant quality during enrollment, or a person cannot reliably match his template in several attempts at the time of verification. FTE also depends on the enrollment policy of the biometric system, and the person can be allowed to enroll at a later date.

Failure to Acquire Rate (FTA)

This error happens for a person when the system is unable to capture or locate the biometric data with a sufficient level of quality. This error rate mainly depends on the threshold level set by the biometric system and can be changed due to the adjustment of the threshold levels of different input biometrics.

Details of Biometric Authentication Modalities

Different physiological biometrics are described in this section. The focus is mainly on the features used to do the authentication and the usability of different biometric traits.

Face Recognition

Facial Recognition is a visual type of recognition that looks at a picture of a face and measures the distance between the eyes, the width of the nose, the distance between the cheekbones, and many other distinctive features as shown in ■ Fig. 2.8.

Different features of the human face are mentioned below along with their error rates and usability as reported in the literature [6]:

Geometrical Features: Seven categories of features are considered as follows:

Lip: Lip center position (x_c and y_c), lip shape (h_1 , h_2 and w), lip orientation (θ). The EER of this feature lies between 5.2 and 6.8%.

Ete: A circle with three parameters (x_0 , y_0 and r) for Iris; two parabolic arcs with six parameters (x_c , y_c , h_1 , h_2 , w , θ) to



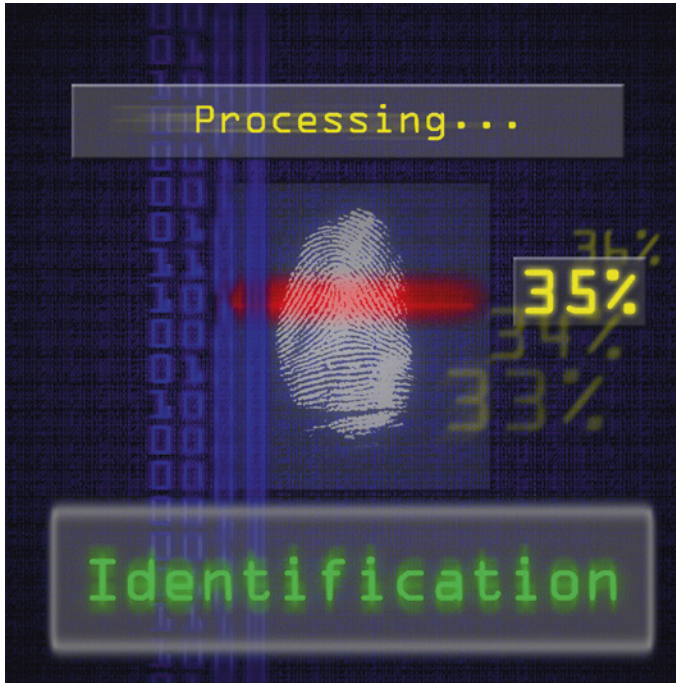
■ **Fig. 2.8** Face recognition process, where the facial points are identified to match with the stored template with the captured image.
©Franck Boston/Shutterstock.com

model boundaries of the eye; last parameter differs in closed and open eye position. The false match probability for the iris recognition is in the range of 1 in 10^{13} and the FNMR is very low. The error rate of retina scan is 1 out of 10,000,000 (almost 0%). Again, its FMR and FNMR are 0 and 1%, respectively. The FAR, FRR, and the crossover rates of the retina scan are 0.31, 0.04, and 0.8% respectively.

Brow and Cheek: Left and right brow: triangular template with three coordinates (x_1, y_1) , (x_2, y_2) , and (x_3, y_3) is used. Cheek also has six parameters (both up and downward triangle template).

Both brow and cheek templates are tracked using Lucas-Kanade algorithm [7]. Here, reported EER is about 15%.

Textural Features: Textural features will be elicited using Local Ternary Pattern (LTP) and Genetic and Evolutionary Feature Extractor (GEFE) [8]. GEFE uses the LTP feature extractors to elicit the distinctive features from the facial images. Its ERR is not much less, about 10%. As reported,



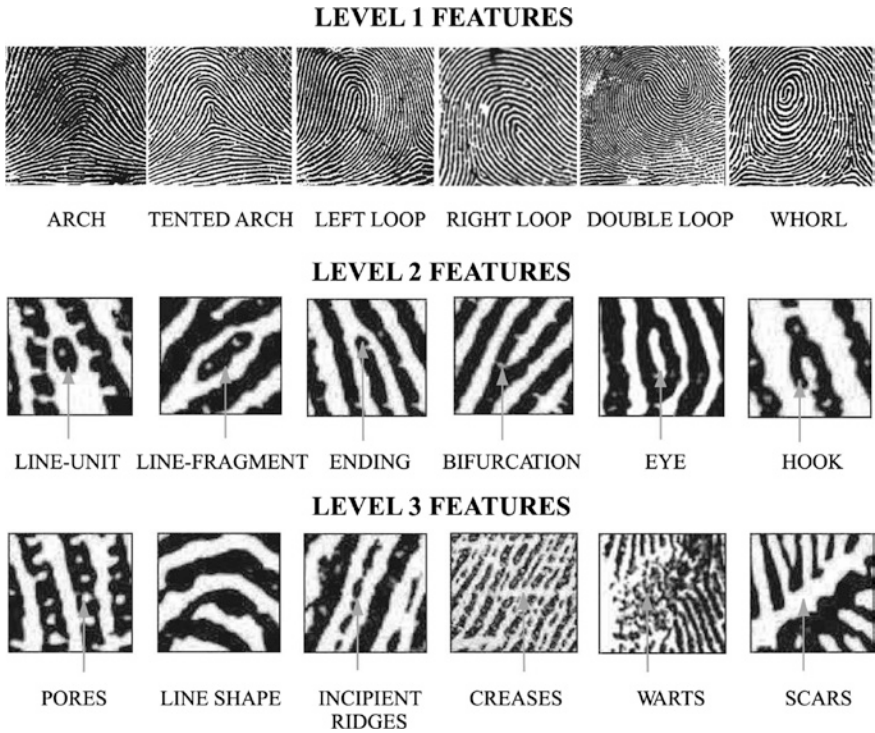
■ Fig. 2.9 The fingerprint recognition of a person is in progress. ©Ford Prefect/Shutterstock.com

overall FAR and FRR for the face recognition modality are 1 and 20% respectively.

Usability: Under normal lighting conditions, geometric features will be used. Under varying lighting conditions, textural features will be utilized. This modality is not reliable if the facial features are altered through plastic surgery [6, 9]. It is also dependent on the motion of the person at the time of taking the picture.

Fingerprint Recognition

Fingerprint Recognition is a visual type of authentication that uses the ridges and valleys found on the surface of fingertips. A picture is taken with the use of a fingerprint scanner that reads the digital image of a fingerprint (shown in ■ Fig. 2.9). The system then finds unique points on the finger and matches the image to one that is stored in the database.



■ **Fig. 2.10** Fingerprint features at level 1 (top row), level 2 (middle row), and level 3 (bottom row) [34–36]

Three levels of fingerprint features are usually considered as mentioned below (■ Fig. 2.10):

Level 1 features: (Global Fingerprint features): This level features include singular points, ridge orientation map, and ridge frequency map.

Level 2 features: (Minutiae-based features): This level features include ridge ending and ridge bifurcation, minutiae location, and orientation. Each of these is a combination of a number of features in order to make a unique identification of a person.

Level 3 features: (Sweat-pore-based features): Sweat pores are considered to be highly distinctive in terms of their number, position, and shape. The best algorithm for fingerprint verification yields EER less than 2.07% and more than 30% of the existing algorithms yield EER less than 5% [6].

According to a study, the overall FAR, FRR, crossover rate and failure to enrollment rates are 2, 2, 2, and 1% respectively. ■ Figure 2.10 shows details of three levels of features:



■ **Fig. 2.11** Iris recognition process of an individual. ©Juergen Faelchle/Shutterstock.com

Usability: Fingerprints can be forged and altered by transplant surgery [6, 10, 11] and in many other ways.

Iris Recognition

Iris Recognition is another type of biometric recognition that uses a camera to capture an image of the iris. This biometric technology acquires an image of the eye, analyzes image data to generate pattern data, and tries to find a match in the stored data. ■ Figure 2.11 shows the image of an iris of an individual.

To calculate the features of an iris, localization features are used. These include iris and pupil boundary localization and pupil center detection. Also, shape, edge, and region information are fused to create a list of features for iris recognition.

Capturing the image of an iris needs a high quality digital camera. Now, commercially available sophisticated cameras

use infrared light to illuminate the iris which is supposed to cause no harm or discomfort to the participants.

Usability: This modality is resistant to false matching and is ideal for high-security applications. The technology is suitable for access control, border control, and large-scale identification and is currently being used by the Immigration Services of the United Kingdom, Canada and many other countries for passport control. Iris recognition technology is used to identify an individual from a crowd and is accurate 90–99% of the time according to the National Institute of Standards & Technology (NIST) [12]. However, the difficulty of operation leads to increased false non-match rates and capture error rates; also user discomfort with eye-based technologies prevent its use than fingerprint.

Retina Recognition

Retina Recognition is a visual type of recognition that shines light into the back of the eye. Because the blood vessels absorb light differently than the surrounding tissue, this process allows the computer to get an accurate picture of the blood vessels. Retina scan requires significantly more effort to use than Iris scan, and it is more challenging as the slightest movement of the eye can cause rejection by the recognition system. It also needs more sophisticated cameras to capture the retina images than Iris scan. ■ Figure 2.12 shows different retinal veins of an individual which are used to identify the person.

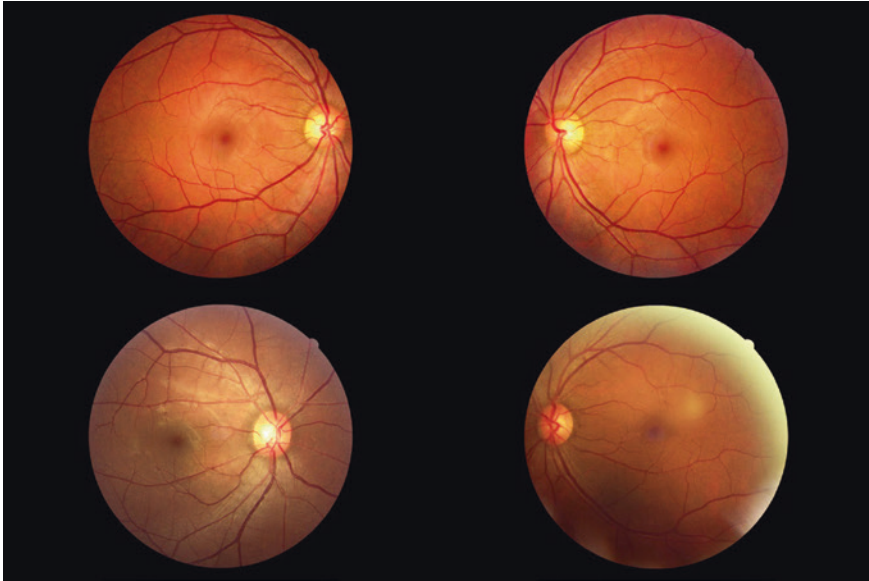
The advantages and disadvantages of retina-based recognition are mentioned below

Advantages:

- Fewer occurrences of false positive rate
- Close to zero in false negative rate
- Very reliable due to the fact that no two persons have the same pattern
- Verification of user's identity is quick.

Disadvantages:

- Accuracy can be affected by some eye diseases
- Scanning process can be considered as invasive
- It is not considered as a user-friendly authentication process
- The higher cost of equipment and the higher cost of deploying this authentication approach.



■ **Fig. 2.12** Pattern of retinal veins to be used to identify an individual in a security system.
©Left-Handed Photography/Shutterstock.com

Usability:

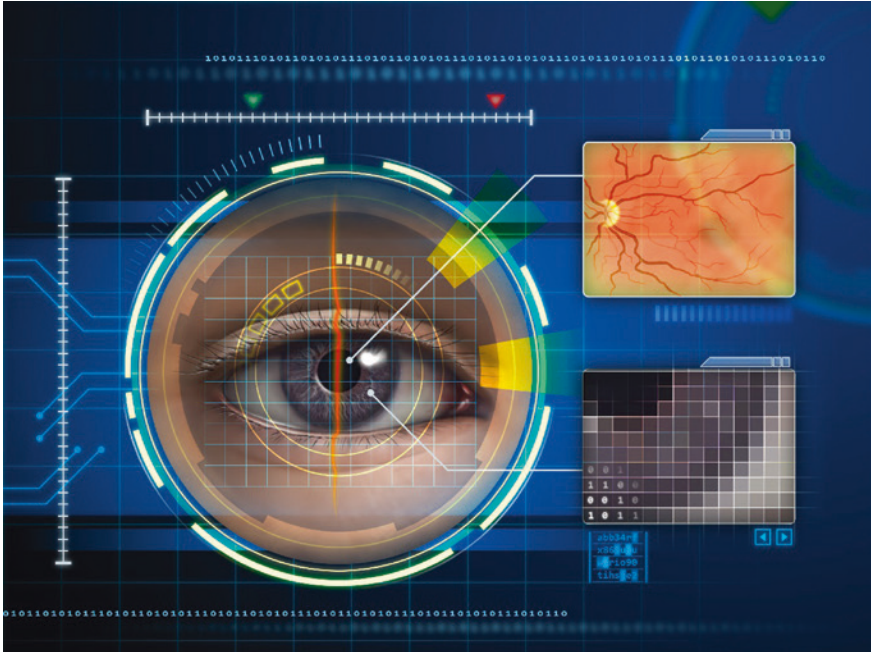
Retina scanning is considered as the most accurate and invulnerable biometric trait to authenticate users in high-security environments. It has been utilized by different government agencies including FBI, CIA, and NASA.

■ Figure 2.13 shows iris recognition and retina recognition which can go together to identify an individual.

Hand Geometry

Biometric hand recognition system measures and evaluates the structure, shape, and proportions of the hand. Different parts of the hand include length, width, and thickness of hand, fingers, and joints. In addition to these features, different characteristics of hand skin surface such as creases and ridges are also considered for hand geometry.

A user puts his palm on a reader's surface and properly aligns his hand to fit the fingers in the appropriate distance. The scanning device then captures hand geometry and extracts the features. These features are then compared with the stored record of the user in the database. This process of



■ **Fig. 2.13** Iris recognition and retina recognition in progress. If both identities match, access is granted to an individual. ©Andrea Danti/Shutterstock.com

authentication generally takes a couple of seconds to verify individuals. Hand-based biometric depends mainly on hand and finger geometry and hence, this biometric trait can also work with dirty hands.

Usability:

Possible applications of hand geometry-based authentication systems are

- Cash vault applications
- Point of Sale applications
- Interactive kiosks
- Parking lot entrance

Figure 2.14 shows the hand geometry scanning is done along with swipe card and face recognition techniques to identify users. Generally, the hand geometry scanner starts scanning from tip of the finger to the end of the palm.

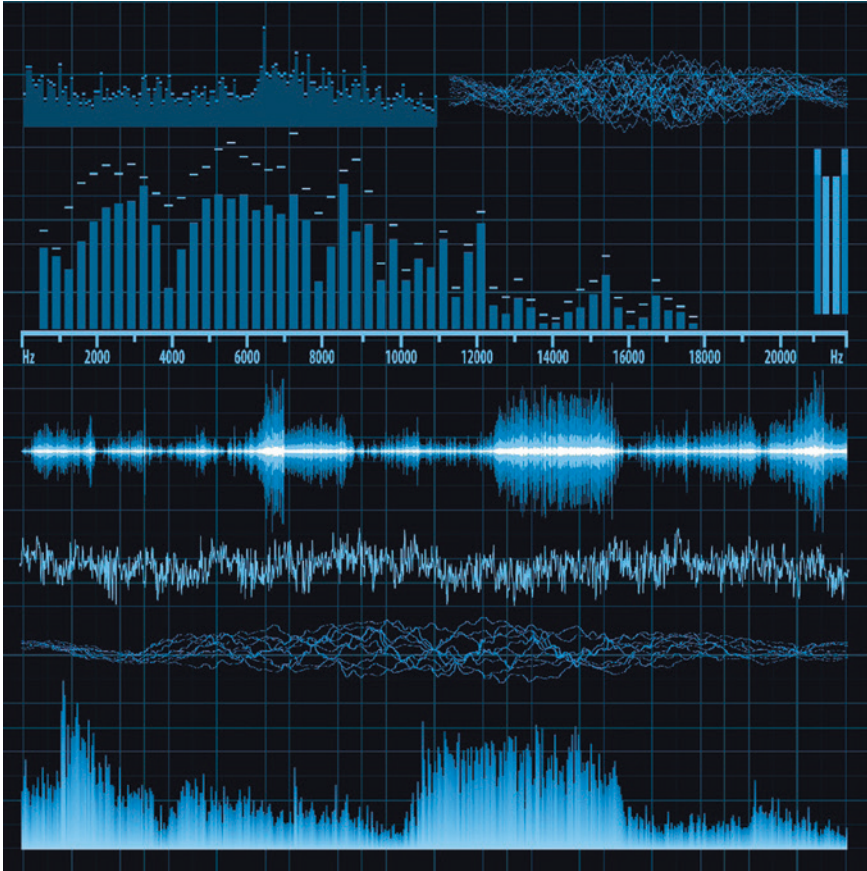
Next, different behavioral biometrics are illustrated with their respective advantages and disadvantages and their usability issues.



■ **Fig. 2.14** Hand geometry is used along with swipe card to identify users. ©Black Jack/Shutterstock.com

Voice (Speaker) Recognition

Voice recognition is an auditory type of authentication that uses the way a person speaks (tone, pitch, speed, etc.) to authenticate a user. This type of recognition measures the sound waves of a person's speech. This is also known as speaker recognition (identify who is speaking) rather than speech recognition (recognize what is being spoken). There are two forms of speaker recognition: text-dependent and text-independent mode. In the first case, the person is given a fixed phrase to say and it records different attempts of the same user to track the variability of his/her voice. A text-independent system is more flexible in terms of presenter's phrasing, and it considers different situational variation of the speech of the user. It is relatively difficult to identify users in text-independent system.



■ **Fig. 2.15** Illustration of voice or speech recognition for identification of users. © Elik/ Shutterstock.com

Voice recognition [6] uses pitch and different formant features. Recent evaluations based on more than 59,000 trials from 291 speakers in identification mode have reported an accuracy in the range of 1% false recognition rate at a 5% miss rate (i.e., a 1% FIR plus a 4% non-identification rate), for the most accurate among the 16 participating systems [6]. The FAR, FRR, and the crossover rates for the voice biometric are 2, 10, and 6%, respectively.

Speech samples are composed of waveforms where time is shown in the horizontal axis and loudness on the vertical axis (■ Fig. 2.15). Speaker recognition process analyzes the frequency of the voice signal and derives characteristics such as quality, duration, intensity, and pitch of the signal [11].

Usability: Some well-known speaker recognition software includes Dragon, Voice Finger, Via Talk, E-speaking, Tazti, etc.

Keystroke Recognition

Keystroke recognition is a behavioral biometric trait which captures the unique way a person types in order to correctly verify the identity of the individual. Typing patterns are generally extracted from computer keyboards, phone's virtual keyboard, etc. In order to extract features for keystroke recognition, it is needed to consider the time taken to move between two keys, how hard the buttons are pressed, and how long a key is pressed before it is released. In general, there are five elements that are captured to do keystroke recognition [13]. These are:

1. Key-down: This event occurs while a person presses a key down. The speed at which this key-down event happens is dependent on the users.
2. Key-up: This event occurs when a currently depressed key is subsequently released by the user.
3. Keystroke: This event is a combination of initial key-down event and corresponding key-up event. These two events together make keystroke event.
4. Hold time: The duration between a key-down event and key-up event happens. It is sometimes known as dwell time. It varies with the users.
5. Delay: The length of time between two successive keystroke events is called delay. The value of this length can be positive or negative (in case of overlapping keystrokes). This term is sometimes called latency.

The features of keystroke recognition are derived from the previously mentioned five elements and first-order statistics are used to calculate the features of keystrokes. Some example of first-order statistics are—minimum, maximum, mean, median, and standard deviation of hold times and latencies [14].

The overall FAR, FRR, and the crossover rates for the keystroke modality are 7, 0.1, and 1.8%, respectively [6].

■ Figure 2.16 shows the keystroke events by a user on a laptop, while ■ Fig. 2.17 shows the finger positions of a person while navigating the keys of a keyboard and mouse.

Usability: Keystroke-based recognition is widely used in continuously authenticating users in different environments.

Gait-Based Recognition

Gait Recognition is a visual type of recognition that authenticates someone based on how they walk. Gait is



■ **Fig. 2.16** A user is typing in a laptop keyboard. This process captures the keystroke patterns of the users. ©Piotr Adamowicz/Shutterstock.com



■ **Fig. 2.17** The finger orientation for navigating keyboards and mouse of a person. ©wrangler/Shutterstock.com

generally considered as a complex locomotion pattern that comprises of synchronized movements of different body parts, joints, and also how they interact with them [15].



■ **Fig. 2.18** Irregular walking patterns can prevent a person from authenticating a system.
©Rawpixel.com/Shutterstock.com

Every person has his/her own walking pattern. Hence, it can be considered as a unique feature for identifying individuals. ■ Figure 2.18 shows the walking pattern of the different individuals that are used to identify them.

The advantages of this biometric trait are [16]:

- Free from background noise
- Does not depend on other person's appearance or camera viewpoint.
- Derive dynamic gait features from the model parameters.

However, this trait requires many parameters to compute from extracted gait features and hence, computational time, data storage, and maintenance costs are relatively higher than other behavioral biometrics.



■ **Fig. 2.19** Walking patterns of individuals that are used to identify them. ©alphaspirit/Shutterstock.com

There are two ways to recognize this biometric trait. One way is to record a video of someone walking, looking at the trajectories of the joints and angles over time to create a mathematical model which is converted into a template. The other way uses radar to record the gait cycle that a person creates when walking and creates a template based on that. Both methods then compare the template created with the templates that are stored in the database for authentication.

Recent work reported [6] an improvement in EER from 8.6 to 7.3% by using Bayesian probability rather than Euclidean distance as a comparison metric. These results were obtained based on relatively large databases, consisting of 1079 video sequences from 115 persons. When this technology is used, irregular walking patterns can prevent a person from authenticating as shown in ■ Fig. 2.19.

Usability:

Gait-based recognition is mostly used in mobile-based authentication systems where users authenticate themselves in their smartphones using accelerometer and gyroscope sensors.

Passthoughts

Recent research focuses on authenticating humans to their computing systems using brainwave signals, which in other terms are called passthoughts [7]. These brainwaves are

captured through consumer-grade wireless headsets and wearable devices having EEG sensors. Passtoughts can be treated as two-factor based authentication approach as they incorporate both knowledge factor and the inherence factor. Knowledge factor consists of a person's mental thought, which only that person knows. Inherence factor consists of EEG signal that comes from a person's brain. In addition, this biometric approach can be treated as one-step two-factor authentication as both factors can be presented at the same time. This provides a great benefit in terms of usability perspective to the participants as they do not need to undergo extra attempt to authenticate themselves.

Brainprint

A biometric Brainprint system [8] is designed to identify individuals with 100% accuracy measuring their EEG signals that represent their brain activities. In general, every individual's brain reacts in a different manner to a same set of images. Hence, the brain activities through EEG signals are able to identify every brainprint (in other words, individuals) with absolute accuracy.

A brainprint of an individual is recorded by having a user look at an image while hooked up to an electroencephalograph that captures his/her brain activity in response to the stimulus. This step is basically the registration phase for the biometric modality. During authentication phase, the user's identity would be verified by exposing her to the stimulus again, recording her current response, and using different pattern recognition algorithms to compare the registered EEG data with authentication EEG data. This biometric-based system has the great potential to be deployed in high-security based system, where 100% accuracy is an absolute need.

Applications of Biometrics

There are many applications of different biometric technologies and their use is being increasingly expanded as new biometrics are becoming available; also more authentication systems are adopting biometrics to authenticate users. ■ Figure 2.20 shows sample application domains of different biometric modalities.

The International Biometric Group (IBG) [1], a technology-neutral, vendor-independent consulting, and inte-



■ Fig. 2.20 Illustrates the application of different biometric modalities. ©Kheng Guan Toh/Shutterstock.com

gration firm founded in 1996, provides objective analysis and independent services on biometrics to public and private sector clients. According to IBG, the following (shown in ■ Fig. 2.21) are some important determining factors for applying different biometrics; while this Zephyr analysis is relatively old, this study provides a guideline in selecting different biometric technologies based on intrusiveness, distinctiveness, cost, and effort required by the users.

In ■ Fig. 2.21, the further away the biometric characteristic is from the center, the better is the biometric technique. So for instance, keystroke scan and signature scan are low cost, require very little effort, and are not intrusive at all; however, they are not distinctive. On the other end of the spectrum, retina scan and iris scan provide very high distinctiveness; however, they are both expensive and intrusive.

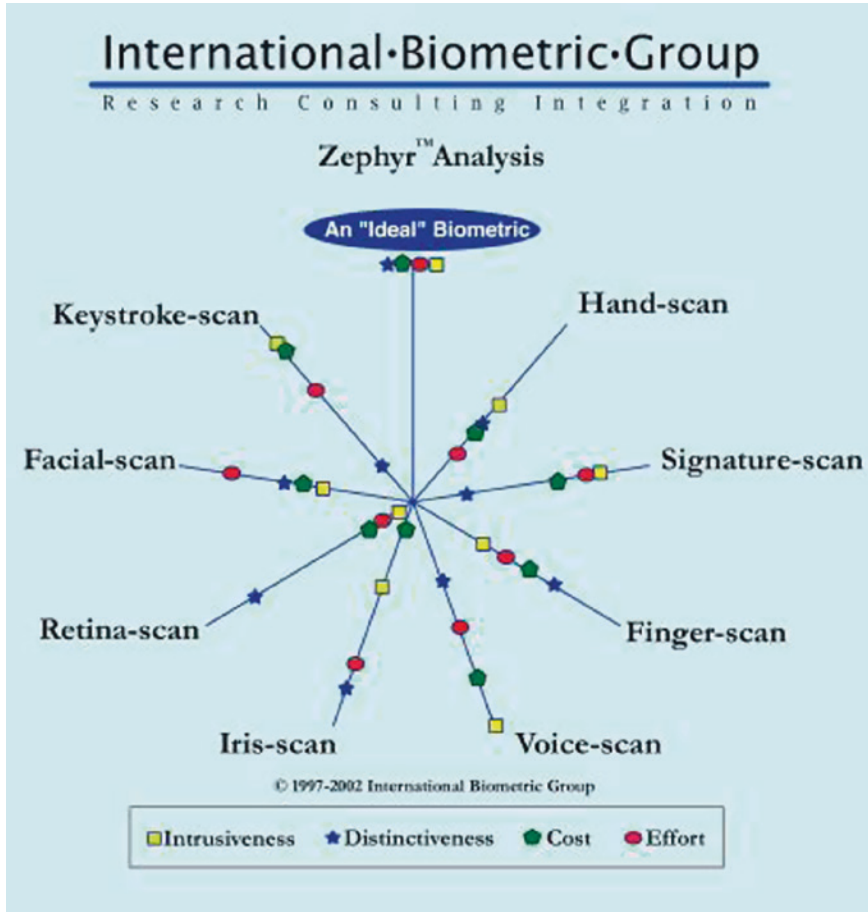
In general, biometric applications fall into three different categories—law enforcement, governments, and commercial.

Law enforcement: Biometric-based authentication is mostly used for law enforcement purposes. Police departments use fingerprint identification systems to identify criminals or fugitives. Forensic applications also use biometric to expedite the investigation process.

Governments: Different branches of the government or federal agencies use biometrics to identify the citizens and foreign nationals. Some of the examples are driving license, national ID card, social security card, border control, passport, US-Visit program, etc.

Business: Commercial sectors increasingly use biometrics to secure their authentication process. ATM booth, credit card, electronic data access, network login are some examples of this type.

Some specific biometric application areas are discussed next:



■ Fig. 2.21 Shows the characteristics of each biometrics and their applicability criteria

Banking

Financial institutions like banks have been using biometrics for many years. Automated teller machines (ATMs) and monetary transaction banks are evaluating a range of biometric technologies for many years. Financial fraud and breaches of security are needed to be controlled for providing better service to the customers. ATMs and transactions at the point of sale (POS) are the most vulnerable to fraud, and they can easily be secured through adopting biometric technologies. Other emerging sectors such as telephone banking and Internet banking require utmost security for bankers and customers to secure their financial transactions.

Computer Access

Fake access to computing systems affects private computer networks and the Internet in a number of ways: lack of confidence and the inability of the network to conduct at full capacity until the breach of security is remediated. Biometric technologies are a great layer of defense to provide security in computer networks. In recent years, financial transaction records, business intelligence, credit card numbers, SSN, confidential medical information, sensitive email contents, and other personal data have become the target of attacks by cyber criminals. This triggers the need to deploy biometric authentication-based sensors on a mass scale, and it eventually escalates the biometric vendors to come across different biometric sensors.

Immigration

Various terrorist threats, drug-running, illegal immigrants, and an increasing number of legitimate travelers are creating a strain on immigration authorities to increase the security checking procedures. It is a crucial need for these authorities to quickly and automatically process law-abiding travelers and identify illegal passengers on the fly. To assist that, biometric-based scanning systems are being deployed in a number of diverse places including all the port of entries of a country. The U.S. Immigration and Naturalization Service (INS) is a major user and evaluator of varieties of biometric technologies. Biometric-based systems are currently in place throughout the U.S. to automate the identification and verification of legitimate travelers and prevent illegal immigrants entering the country. For this purpose, the false acceptance rate (FAR) of the systems should be as low as possible.

National Identity

Biometrics is now widely used to assist government officials to do their everyday jobs. Their tasks include a recording of growth of population, identifying citizens, and preventing fraudulent activities during local and national elections. In order to facilitate that a biometric template is stored on a card, which in turn, acts as a national identity document for a person. Fingerprint scanning is particularly used in these

scenarios to provide higher accuracy rate in person identification. Other than fingerprints, face recognition is also used to identify citizens.

Prisons

Prisons, as opposed to law enforcement, use biometric systems not only to catch criminals, but to make sure that they are securely detained in the given facility. There are many evidences where a good number of prisoners walk out of prison gates before they are officially released by the legitimate authorities. A wide range of biometrics are now being deployed worldwide to provide more secure prison access and police detention areas, enforce home confinement orders, and control the movements of probationers and parolees.

Telecommunications

With the immense growth of global communication systems, cellular networks, dial inward system access (DISA), and a range of telecommunication services are under cyber attacks from cyber criminals and terrorists. Cellular companies are the most vulnerable to cloning (a new phone set is built using information of stolen codes) and new subscription fraud (a phone number is obtained using a false identity of a person). Subsequently, DISA, which allows authorized individuals to communicate with a central exchange unit and to make free calls, is being targeted by phone scammers. To mitigate these threats, biometric-based authentication approaches are being used. Speaker ID in the phone device is a good viable option for the users to verify the numbers and then check the authenticity of the numbers in case of any doubt.

Time and Attendance

Recording and monitoring the movement of employees as they come to the workplace, take breaks for lunch, and leave for the day was traditionally accomplished by 'clocking-in' machines. However, manual checking systems can be circumvented by someone "punching in" for another person. This process really creates confusion in the tracking of the employees of a company. This also interrupts time management and costs companies millions of dollars in a year.

Replacing the manual checking process with biometric-based scanners prevents all types of system abuses.

Limitations of Biometric Systems

Biometric systems that operate using any single biometric characteristic have the following limitations [17, 18]:

1. **Noise in the captured data:** The data captured by the scanner might be noisy or distorted. A fingerprint with a scar, or a voice altered by catching cold or throat infection are examples of noisy data. Noisy data can be captured also due to the defective or improperly adjusted sensors (e.g., accumulation of dirt on a fingerprint device) or unfavorable ambient conditions (e.g., poor illumination of light on a user's face in a face recognition system). Noisy biometric data can be incorrectly matched with the stored templates in the database which results in a legitimate user being incorrectly rejected.
2. **Intra-class variations:** The biometric data acquired from an individual during the phase of authentication may be largely different from the data that was used to generate the template during enrollment. This can affect the matching process significantly. This variation is typically caused due to incorrect interaction with the sensor, or when sensor characteristics are changed during the verification phase. For example, the varying psychological makeup of a legitimate individual might result in vastly different behavioral traits at various verification events.
3. **Distinctiveness:** A biometric trait is expected to vary significantly across individuals. In some cases, it is possible to have large inter-class similarities in the feature sets used to represent these biometric traits. Golfarelli et al. [19] 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 10^5 and 10^3 , respectively. Therefore, every biometric trait has some theoretical upper bound that limits its discrimination capability.
4. **Non-universality:** While all registered users are expected to possess the biometric trait being acquired, it is possible for a subset of the users in real scenario who do not possess a particular biometric trait. A fingerprint-based biometric system may be unable to extract

the set of features for certain individuals, due to the poor quality of the ridges in his/her hand. Thus, there is a failure to enroll (FTE) rate associated with using every 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 capture through fingerprint sensors and that results in increasing FTE errors. Den Os et al. [20] report the FTE problem in a speaker recognition system.

5. **Spoofing attacks:** An imposter may make different attempts to spoof the biometric trait of a legitimate user in order to circumvent the security of the system. This type of attack is especially relevant when behavioral traits such as signature [21] and voice [22] are used. However, physical traits of an individual are also susceptible to spoofing attacks. For example, it can be 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 [23].

New Biometric Challenges

With the development of sophisticated skin-like facemasks for use in movies and other recreational purposes, such masks can also be used to defeat the face or fingerprint recognition system for illegal access; ■ Fig. 2.22 shows wearing such a face mask.

A research on identity science [2] shows that it is possible to alter biometric features of a person through different medical procedures, which are listed below.

■ ■ Fingerprint Modification:

The fingerprint is a widely used biometric specifically in border control and immigration. As fingerprints cover a little area at the tips of fingers, it is possible to obscure this particular area using various methods such as chewing off the skin or applying acid to scar the fingerprint permanently. Criminals sometimes can modify their fingertips surgically by replacing the skin with that of a donor or some other part of their own body.

■ ■ Plastic Surgery:

Plastic surgery poses significant recognition challenges for face-based biometric systems because they rely on various

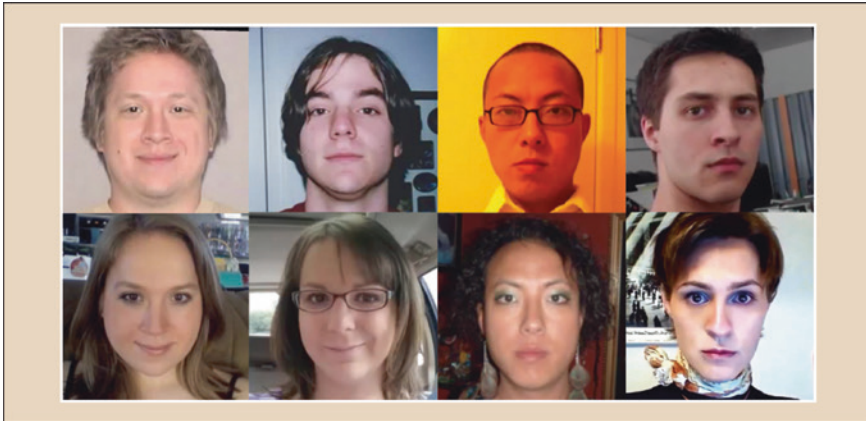


■ **Fig. 2.22** Illustration of the use of mask in obfuscating face recognition. ©aastock/Shutterstock.com

facial characteristics, such as the relative position, shape, and size of the eyes, nose, jaw, and cheekbones. The alteration of the face can be done locally (reshaping and restructuring facial features) or globally (skin peels and facelifts). This type of modification of face presents a big challenge for face recognition algorithms to accurately identify a person in real scenario.

■ **Hormone Replacement Therapy:**

An innovative challenge to face recognition-based systems is the medical alteration of levels of sex hormones to transform gender. Transgender hormone replacement therapy (HRT) impacts fat distribution in the region of the face which changes the overall shape and texture of the face biometric. Hence, the current face recognition algorithm will fail to detect that person from his/her previously registered data. Figure 2.23 shows the significant changes in male faces after undergoing hormone replacement therapy.



■ **Fig. 2.23** Example face images of four male-to-female transgendered women before (top row) and after (bottom row) hormone replacement therapy [2]

Attacks on Biometric-Based Authentication Systems

Biometric systems work accurately if the verifier of the system can validate the following things:

- The biometric data comes from a legitimate person at the time of verification.
- The captured biometric matches with the stored template in the database.

In general, there are eight points in a biometric system which are vulnerable to attack [24]. The details are mentioned below (see ■ Fig. 2.24) [25].

■ ■ Attack the Biometric Sensor:

In this particular type of attack, a fake biometric is presented at the sensor to verify. The fake instance can be false image or fingerprint.

■ ■ Resubmit a Previously Stored Digitized Biometric Signal:

In this mode of attack a previously recorded biometric signal is replayed to the system through bypassing the biometric sensor.

■ ■ Override the Biometric Feature Extractor:

The feature extractor of the biometric system is forced to generate a set of features chosen by the attackers rather than actual values generated from the captured data of the sensors.

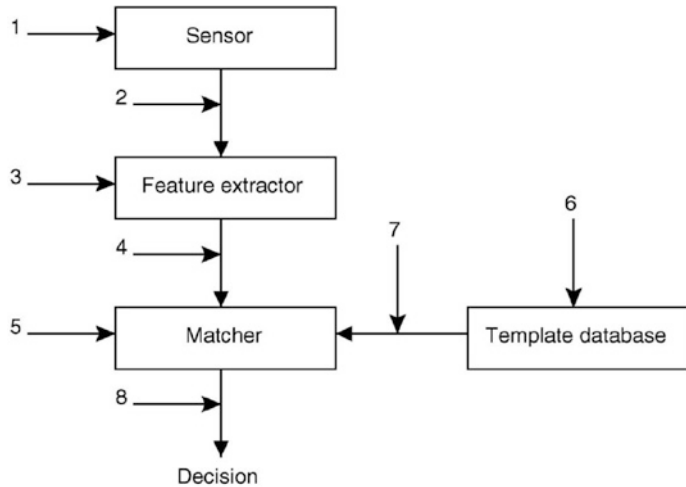


Fig. 2.24 Possible different attack points in a generic biometrics-based system [27]

■ **Tamper with the Biometric Feature Representation:**

The features extracted using the data obtained from the sensor are replaced with a different fraudulent feature set.

■ **Corrupt the Biometric Matcher:**

The biometric matcher can be attacked in order to produce a predefined match score irrespective of the input feature captured by the biometric sensor.

■ **Tamper with the Stored Biometric Templates:**

The attackers can alter any numbers of stored templates in order to allow a fraud to authenticate into the system. In that case an unauthorized person can do the regular biometric scanning and allow access to the sensitive data of a system. Any smart card where the template is stored is equally vulnerable to this type of attack.

■ **Attack the Communicating Channel between the Stored Template and the Biometric Matcher:**

The attack can happen in the communication channel between the stored template in the database and the biometric matcher logic module. In this type of attack, any communicating data can be altered to change the final decision of matching.

■ **Override the Final Decision of Matching:**

The final decision regarding the matching of biometric can even be hacked or overridden by the attacker, which allows the intruders to gain access to a biometric system.

Mitigating Different Attacks on Biometric Systems

In order to resist the previously mentioned attacks, several approaches are taken to ensure the integrity of the each component of a biometric authentication system. Some of these mechanisms are described below [25, 26].

Liveness Detection Mechanisms

Liveness detection in a biometric system guarantees that only ‘real’ biometric data are used to generate templates for enrollment, verification, and identification. Detection of liveness can be done using software or hardware implementation. The first attack point can be mitigated with the incorporation of the liveness detection in the biometric sensor.

One should incorporate extra hardware to capture life signs like temperature, pulse detection, etc., for fingerprint detection and movement of face for face recognition. The drawback of using extra hardware is that the system will be expensive and difficult to deploy for the mass population.

Facial recognition systems can use multiple cameras to obtain 3D properties of the head. This will avoid an attack if a photo is used as authentication. Text-prompted voice systems can ask the person to say a random phrase. Again a combination of face and voice recognition can verify the lip movement.

Liveness detection can also be done through challenge-response based approaches, where a small impulse current is passed into the finger and then response from the finger is captured. Liveness detection through perspiration patterns of a fingerprint image can be done. Moreover, procedural techniques like supervision are greatly effective to detect the liveness of the biometric.

Steganographic and Watermarking Techniques

Steganographic and Watermarking techniques are used to resist attacks at the previously mentioned attack points 2 and 7 (Channel between the sensor and feature extractor and also the channel between the stored template and the matcher). Steganography means secret communication and it involves hiding critical information through unsuspected carrier data. Steganography-based techniques are suitable to transfer critical biometric information from a client

2

application to a secured server. In the following section, two application scenarios are illustrated where hiding process of data is similar, but they (scenarios) vary in the characteristics of the embedded data, host image, and medium of data transfer [27].

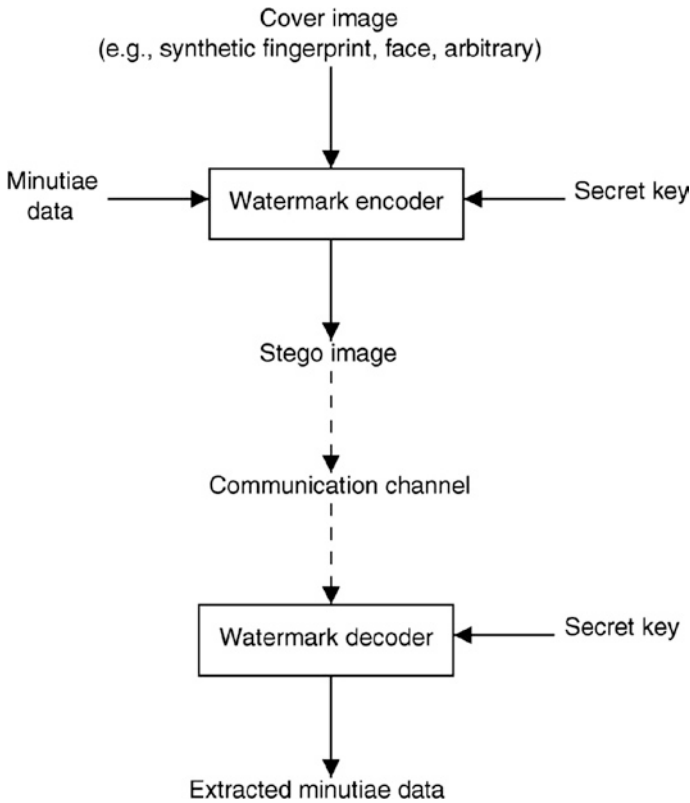
The first scenario shown in ■ Fig. 2.25 involves an application based on steganography. The required biometric data (for example, fingerprint minutiae) to transmit over a communication channel is hidden in a host image. Sometimes it is called carrier image due to its purpose of carrying the data only. The carrier image can be a synthetic fingerprint image, a face image, and any random image. The usage of this synthetic image to carry actual fingerprint data provides more security towards preventing interception of actual fingerprint image. The security of the transmission process can further be increased through encryption technique applied on the stego image before transmitting it.

The second scenario mentioned in ■ Fig. 2.26 focuses on hiding the facial information (different facial points to identify a person) into a fingerprint image to increase the security of the fingerprint biometrics, and this information is stored on a smart card of a user. At the time of authentication, the fingerprint of a person is compared with the stored information on the smart card. Then the facial information embedded in the fingerprint biometric is recovered. This additional information is a good source to verify the authenticity either in an automated manner or by a human in a supervised biometric application.

Challenge-Response Systems

Challenge-response systems are a better way to prevent replay attacks mentioned in the attack 2 and attack 7 in the previous section. One approach can be to use image-based challenge response method. Using this method, a challenge is presented to the biometric sensor and the output response is computed depending on the asked challenge and the content of the acquired input image [28].

In another approach [29], the smart card containing the biometric data (used to do verification) is protected using a cryptographic checksum. This value is calculated within a security module capable of resisting tamper and integrated with a biometric sensor.



■ Fig. 2.25 Diagrams of steganographic techniques to prevent attacks [27]

Multimodal Biometric Systems

Unimodal-based biometric systems suffer from a variety of problems including noisy data, intra-class variations, restricted degree of freedom, non-universality, spoof attacks, and unacceptable error rates [30]. Some of these limitations imposed by the unimodal biometric system can be mitigated with the inclusion of multiple sources of biometric information to verify user's identity. Multimodal biometric systems are expected to be more reliable because of the multiple independent pieces of information about the same identity. They address the issue of non-universality by ensuring multiple traits with significant population coverage. They also prevent spoofing since it will be really difficult for an impostor to spoof multiple biometric traits of a legitimate user simultaneously. Above all, they can facilitate a challenge-response

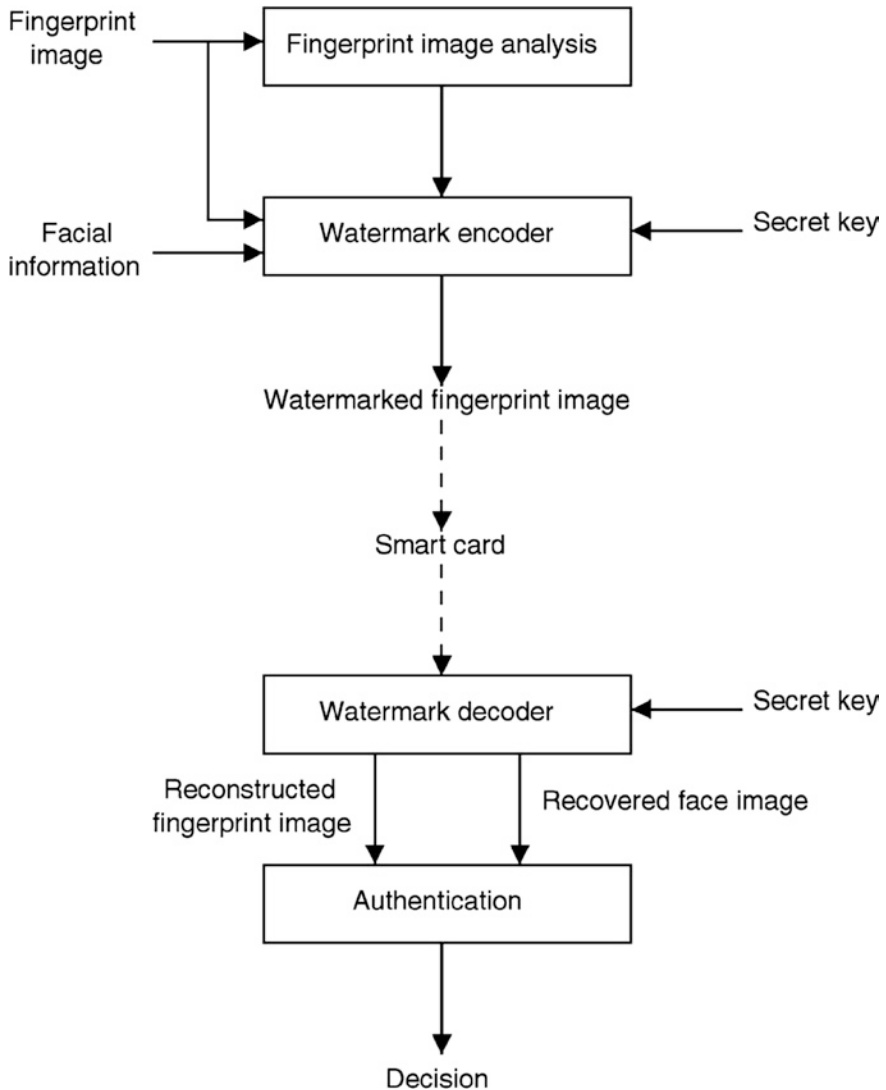


Fig. 2.26 Diagram of watermarking techniques to prevent attacks [27]

type of mechanism by requesting the user to present a random subset of biometric traits (authentication modalities) which ensure the liveness of a user at the point of data acquisition. The choice and the number of biometric traits are determined by the type of application using the required computational resources and the cost required to do the authentication.

The combination of different biometric traits can be achieved at the feature extraction level, matching score level, or decision level. At the feature extraction level, features from different biometric traits are combined to make the new sets of features and this new set is going to be used in matching an identity. While in the case of matching level, the individual scores produced by every biometric trait are integrated to generate a new score. The generation step depends on the system administrator regarding what metric should follow to combine them. The new score is then compared with the new threshold value and makes the decision regarding allow or deny the identity. For the case of decision level, each biometric system decides its individual decision regarding the entity and then a majority voting scheme is used to come to the final decision. In practice, the fusion of matching score of the different biometric system is more preferred as it gives more flexibility to choose the importance of one biometric trait over the others.

The issues of noisy data can easily be solved using the fusion of the biometric traits as we can adjust the weight (different degrees of influence) based on the existing operating conditions. The performance of the multi-modal-biometric system depends on computational time and cost. Hence, the cost versus performance measurement should be put into consideration before deploying these systems.

Soft Biometrics

Soft biometrics traits are some characteristics of humans based on their physical, behavioral, or adhered attributes. Skin color, eye color, height, weight, etc., are examples of soft biometrics. Biometrics can be used to defend attacks at points 1 and 8 (mentioned in the previous section). These traits lack the distinctiveness to clearly distinguish two individuals. In general, many biometric systems collect auxiliary information about the registered users during enrollment time. This auxiliary information is stored either in the central database or in the smart card of the user. The soft biometric traits can help to filter out a large biometric database to a significantly smaller number of templates to match. It thus helps the speed and efficiency of the biometric authentication system.

Soft biometric nowadays are used to tune the parameters of the biometric systems as the human biometric traits are

going to change over time. So, the adjustment of the threshold value for the matching score or the threshold value to weight different biometric traits can be done with the help of soft biometrics. In addition to that, soft biometrics will decrease the FAR and FRR values of biometric-based authentication that help in preventing spoofing.

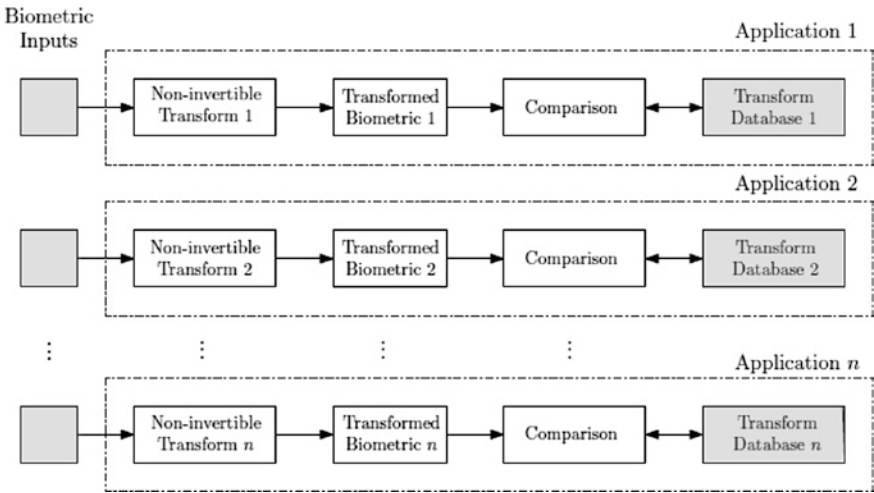
Cancelable Biometrics

Cancelable biometrics requires some intentional and repeatable distortion of a biometric trait based on some non-invertible transform [28]. This is done to protect sensitive user credentials. In the case of compromise of the cancelable biometric feature, the distortion process can be changed and the same set of biometric traits can be mapped to a new template and can be used for authentication purpose. This approach is considered as one of the major ways for protecting biometric templates from being compromised.

In order to design a cancelable biometric; four criteria below should be fulfilled:

- (a) **Diversity:** The set of cancelable features can be used in only one application. Other application should use a different set of cancelable features. Hence, a large number of templates need to be created for the same biometric feature (or trait).
- (b) **Reusability:** In the event of compromise or data breach, it should be able to revoke the existing templates and reissue a new set of templates.
- (c) **Non-invertibility:** This property ensures that the template creation process is non-invertible and hence it prevents the recovery of original biometric data from the template.
- (d) **Performance:** Due to some extra processing of original biometric data, the performance of recognition should not deteriorate.

The transformation steps of biometric inputs for different applications are shown in ■ Fig. 2.27. In general, at enrollment phase, different non-invertible transforms are applied to biometric inputs based on application-dependent parameters. During authentication, captured biometric inputs are transformed and then a comparison with the stored transformed template is done.



■ Fig. 2.27 The basic concept of cancelable biometrics based on non-invertible transforms [37]

Comparative Evaluation

As there are a good number of biometric traits available, some metrics are necessary to make a comparative analysis of all these traits. In general, a biometric trait has to follow some requirements to be applied in identifying persons [31]:

Universality: Every person should possess the biometric trait.

Distinctiveness: Any two persons should be significantly different in terms of their traits or characteristics.

Permanence: Biometric trait should perform in the same way irrespective of the matching criterion.

Collectability: A biometric trait is able to be measured quantitatively.

In a practical biometric system, other metrics should be considered for choosing the biometric trait. They are:

Performance: Measured in terms of recognition accuracy, computational time, error rates (FAR, FER), etc.

Acceptability: Which set of users can accept to go for the biometric sensor in everyday life.

Circumvention: Measured in terms of how easy to bypass the biometric authentication system.

The following table ■ (Table 2.1) shows a comparison of various biometric traits with the above-mentioned characteristics.

Table 2.1 Comparison of commonly used biometric traits. Entries in the table are based on the perception of the authors [31]. High, Medium, and Low are denoted by H, M, and L, respectively								
Biometric identifier	Universality	Distinctiveness	Permanence	Collectability	Performance	Acceptability	Circumvention	
Face	H	L	M	H	L	H	H	
Fingerprint	M	H	H	M	H	M	M	
Hand geometry	M	M	M	H	M	M	M	
Hand/finger vein	M	M	M	M	M	M	L	
Iris	H	H	H	M	H	L	L	
Signature	L	L	L	H	L	H	H	
Voice	M	L	L	M	L	H	H	

■ **Table 2.2** Advantages and drawbacks of the different protection techniques [25]

Techniques	Advantages	Drawbacks
Liveness detection	Resists spoofing attacks	Increased cost for the extra hardware and software, user inconvenience and increased acquisition time
Watermarking	Prevents replay attacks and provides integrity of the stored templates	Problem of image degradation and lack of algorithms to deal with it
Soft biometrics	Provides improved performance through filtering and tuning of parameters	Lack of techniques for automatic extraction of soft biometric techniques
Multi-modal biometrics	Improves performance, resists spoofing and replay attacks, and provides high population coverage	Increased system complexity, computational demands and costs

■ Table 2.2 highlights the advantages and drawbacks of different protection schemes of biometric authentication techniques.

Chapter Summary

This chapter covers different biometric authentication methods and provides details on various aspects of each biometric modality. It also covers the limitations and error rate of each biometrics which can be used as a performance measure while adopting in different applications. While Face Recognition, Fingerprint are in wide use, there is continued search for the Holy Grail, the perfect biometric, and many other biometric modalities are emerging. Some of these are called soft biometrics and others are behavior biometrics which are gradually in adaptation. Recent reports predict that biometric analytics may soon be used to discover potentially interesting information about a person other than verifying identity using biometric signal patterns. These include person's emotional state, longevity, aliveness, continuous

authentication, ethnicity, gender, age (demographics, in general), honesty, concentration, mood, attitude, and even frustration in some situations.

Review Questions

Descriptive Questions

- Q1: State four reasons to choose biometric-based authentication system.
- Q2: Describe the taxonomy of biometric traits.
- Q3: Difference between physiological and behavioral biometrics.
- Q4: Describe the biometric authentication process.
- Q5: What are different performance metrics used for biometric authentication? What is the most dominant error rate in biometrics?
- Q6: Describe a few applications that use biometric-based authentication.
- Q7: What are the drawbacks of a biometric system? Describe any two of them.
- Q8: What are the possible attack points of a biometric authentication system? Illustrate with diagram.
- Q9: What is liveness? Describe a process of liveness detection mechanism for biometric systems.
- Q10: Distinguish between the following:
- (a) Behavioral and Physiological biometric
 - (b) Soft biometrics and actual biometric
 - (c) Liveness detection and watermarking technique
 - (d) Unimodal biometric and multimodal biometric.

Multiple Choice Questions

Question 1:

A company is looking into adding biometric scanners to their building for added security. Which option would NOT be a good idea?

- A. Facial recognition
- B. Weight recognition
- C. Gait recognition
- D. None of the above

Question 2:

Which of the following does not use behavioral characteristics of users for authentication?

Multiple Choice Questions

- A. Voice
- B. Signature
- C. Veins
- D. Keystrokes

Question 3:

Jason is the type of person who does not like to give out his personal information and is overly suspicious of other people. What would be the best authentication type for Jason?

- A. Cognitive-based Authentication
- B. Token-based Authentication
- C. Biometric-based Authentication
- D. Any of the above

Question 4:

What is true for equal error rate?

- A. Lower the error rate, higher the accuracy
- B. Higher false positive make lower equal error rate.
- C. Lower false negative make higher equal error rate.
- D. None of the above.

Question 5:

In which of the following biometrics, will the most sophisticated camera be used to capture the biometrics?

- A. Face recognition
- B. Fingerprint recognition.
- C. Iris recognition
- D. Retina recognition

Question 6:

Which biometric has higher universality?

- A. Face recognition
- B. Hand Geometry
- C. Signature
- D. Voice

Question 7:

Which biometric has lower distinctiveness?

- A. Face
- B. Hand Geometry
- C. Iris
- D. Fingerprint

Question 8:

Which biometric has higher performance?

- A. Face
- B. Hand Geometry

- C. Iris
- D. Signature

Question 9:

Which biometric has higher acceptability?

- A. Face
- B. Fingerprint
- C. Iris
- D. Hand Geometry

Question 10:

Which biometric has lower circumvention?

- A. Iris
- B. Face
- C. Fingerprint
- D. Signature

References

1. The International Biometric Society website. ► <http://www.biometricsociety.org/>
2. Ricanek K (2013) The next biometric challenge: medical alterations. *Computer* 46:94–96. doi:10.1109/MC.2013.329
3. Ashbourn J (2014) *Biometrics: advanced identity verification: the complete guide*. Springer, Berlin
4. Jain AK (2008) Biometric authentication. *Scholarpedia* 3(6):3716
5. Maltoni D, Maio D, Jain AK, Prabhakar S (2009) *Handbook of fingerprint recognition*. Springer Science & Business Media, Berlin
6. Vielhauer C (2005) Biometric user authentication for IT security from fundamentals to handwriting, vol 18. Springer, Berlin (2005)
7. Johnson B, Maillart T, Chuang J (2014) My thoughts are not your thoughts. In: *proceedings of the 2014 ACM international joint conference on pervasive and ubiquitous computing*, Adjunct Publication, ACM, pp 1329–1338
8. Ruiz-Blondet MV, Jin Z, Laszlo S (2016) CEREBRE: a novel method for very high accuracy event-related potential biometric identification. *IEEE Trans Inf Foren Secur* 11(7):1618–1629
9. Lucas BD, Kanade T (1981) An iterative image registration technique with an application to stereo vision. *IJCAI* 81:674–679
10. Bowyer KW, Chang KI, Yan P, Flynn PJ, Hansley E, Sarkar S (2006) Multi-modal biometrics: an overview. In *second workshop on multi-modal user authentication*, vol 105
11. Woodward JD, Orlans NM, Higgins PT (2003) *Biometrics*. McGraw-Hill/Osborne ISBN: 0-07-223030-4
12. Lipowicz A (2012) NIST tests accuracy in iris recognition for identification. Date accessed 1 Jan 2017. Url: ► <https://fcw.com/articles/2012/04/23/nist-iris-recognition.aspx>
13. Bartlow N (2009) Keystroke recognition. In: *Encyclopedia of biometrics*. Springer, US, pp 877–882
14. Bartlow N, Cukic B (2006) Evaluating the reliability of credential hardening through keystroke dynamics. In: *null*, IEEE, pp 117–126

References

15. BenAbdelkader C, Cutler R, Nanda H, Davis L (2001) Eigengait: motion-based recognition of people using image self-similarity. In: audio-and video-based biometric person authentication, Springer, Berlin, Heidelberg, pp 284–294
16. Ng H, Ton HL, Tan WH, Yap TTV, Chong PF, Abdullah J (2011) Human identification based on extracted gait features. *Int J New Comput Architect Appl (IJNCAA)* 1(2) 358–370
17. Blum RS, Liu Z (eds) (2005) *Multi-sensor image fusion and its applications*. CRC press
18. Jain AK, Ross A, Prabhakar S (2004) An introduction to biometric recognition. *IEEE Trans Circ Syst Video Technol* 14(1):4–20
19. Golfarelli M, Maio D, Malton D (1997) On the error-reject trade-off in biometric verification systems. *IEEE Trans Pattern Anal Mach Intell* 19(7):786–796
20. den Os E, Jongbloed H, Stijssiger A, Boves (1999) Speaker verification as a user-friendly access for the visually impaired. In: *EUROSPEECH*
21. Harrison WR (1981) *Suspect documents, their scientific examination*. Nelson-Hall, Chicago, IL
22. Eriksson A, Wretling P (1997) How flexible is the human voice?—a case study of mimicry. *Target* 30(43.20):29–90
23. Matsumoto T, Matsumoto H, Yamada K, Hoshino S (2002) Impact of artificial gummy fingers on fingerprint systems. In: *Electronic imaging. International Society for Optics and Photonics*, pp 275–289
24. Ratha NK, Connell JH, Bolle RM (2001) An analysis of minutiae matching strength. In: *audio-and video-based biometric person authentication*, Springer, Berlin, Heidelberg, pp 223–228.
25. Ambalakat P (2005) Security of biometric authentication systems. In: *21st computer science seminar, SA1-T1*, pp 1–7
26. Matyáš V, Říha Z (2010) Security of biometric authentication systems. In: *international conference on computer information systems and industrial management applications (CISIM)*, IEEE, pp 19–28
27. Jain AK, Uludag U (2003) Hiding biometric data. *IEEE Trans Pattern Anal Machine Intell* 25(11):1494–1498
28. Ratha NK, Connell JH, Bolle RM (2001) Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst J* 40(3):614–634
29. Waldmann U, Scheuermann D, Eckert C (2004) Protected transmission of biometric user authentication data for oncard-matching. In: *Proceedings of the ACM symposium on applied computing*, ACM, pp 425–430
30. Ross A, Jain AK (2004) Multimodal biometrics: an overview. In: *2004 12th European Conference on Signal Processing*, IEEE, pp 1221–1224
31. Maltoni D, Maio D, Jain AK, Prabhakar S (2009) *Handbook of fingerprint recognition*. Springer Science & Business Media, Berlin
32. Zhang DD (2013) *Automated biometrics: technologies and systems*, vol 7. Springer Science & Business Media, Berlin
33. Mansfield AJ, Wayman JL (2002) *Best practices in testing and reporting performance of biometric devices*. Centre for Mathematics and Scientific Computing, National Physical Laboratory, Teddington, Middlesex, UK

34. Jain AK, Chen Y, Demirkus M (2007) Pores and ridges: High-resolution fingerprint matching using level 3 features. *IEEE Trans Pattern Anal Mach Intell* 29(1):15–27
35. The thin blue line. ► <http://www.policensw.com/info/fingerprints/finger06.html>. Oct 2006
36. Nieuwendijk HVD (2006) Fingerprints. ► <http://www.xs4all.nl/~dacty/minu.htm>. Oct 2006
37. Rathgeb C, Uhl A (2011) A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J Inform Secur* 1:1–25

Advances in User Authentication

Dasgupta, D.; Roy, A.; Nag, A.

2017, XIV, 360 p. 165 illus., 128 illus. in color.,

Hardcover

ISBN: 978-3-319-58806-3