Unit IV

TOPICS

- *Biometric system authentication*
- *physiological and behavioral properties of biometric system*
- *Software biometrics systems*
- *Hardware biometrics systems*
- *Security of biometric systems*
- ***Advisory,insider,infrastructure attacks***

TOPICS

- ***Attacks at the user interface***
- ***impersonation ,obfuscation, spoofing***
- ***Attacks on biometric processing***
- ***Attacks on system module and interconnections***
- ***Counter measure: Biometric template security***
- ***Countermeasure:spoof dectection***

TOPICS

- *Challenges in biometric systems like fool proofing, false positives*
- *Developing Tools for Comparing fingerprints*
- *Enhancing pattern when data is minimum.*
- *Biometric failures in special cases like(too much moisture in hands which system can't read)*
- *Mini project: Fingerprint, Face detection*
- *Mini project:signature ,iris detection*

Primary reason

- The primary reasons for using biometric recognition are to apprehend criminals, curtail financial fraud, secure national borders, or control access to physical facilities and logical resources

Biometric system Authentication

- The primary purpose of using biometrics is to provide non-repudiable authentication.

Authentication implies that

(a) only legitimate or authorized users are able to access the physical or logical resources protected by the biometric system

(b) impostors are prevented from accessing the protected facilities or information.

- Non-repudiation ensures that an individual who accesses a certain resource cannot later deny using it. Thus, the *integrity* of a biometric system is determined
- by its ability to guarantee non-repudiable authentication.

Identification vs. Authentication

Identification	**Authentication**
It determines the identity of the person.	It determines whether the person is indeed who he claims to be.
No identity claim Many-to-one mapping. Cost of computation $\propto$ number of record of users.	Identity claim from the user One-to-one mapping. The cost of computation is independent of the number of records of users.
Captured biometric signatures come from a set of known biometric feature stored in the system.	Captured biometric signatures may be unknown to the system.

Biometrics-enabled Authentication Applications

1. Cell phones, Laptops, Work Stations, PDA & Handheld device set.



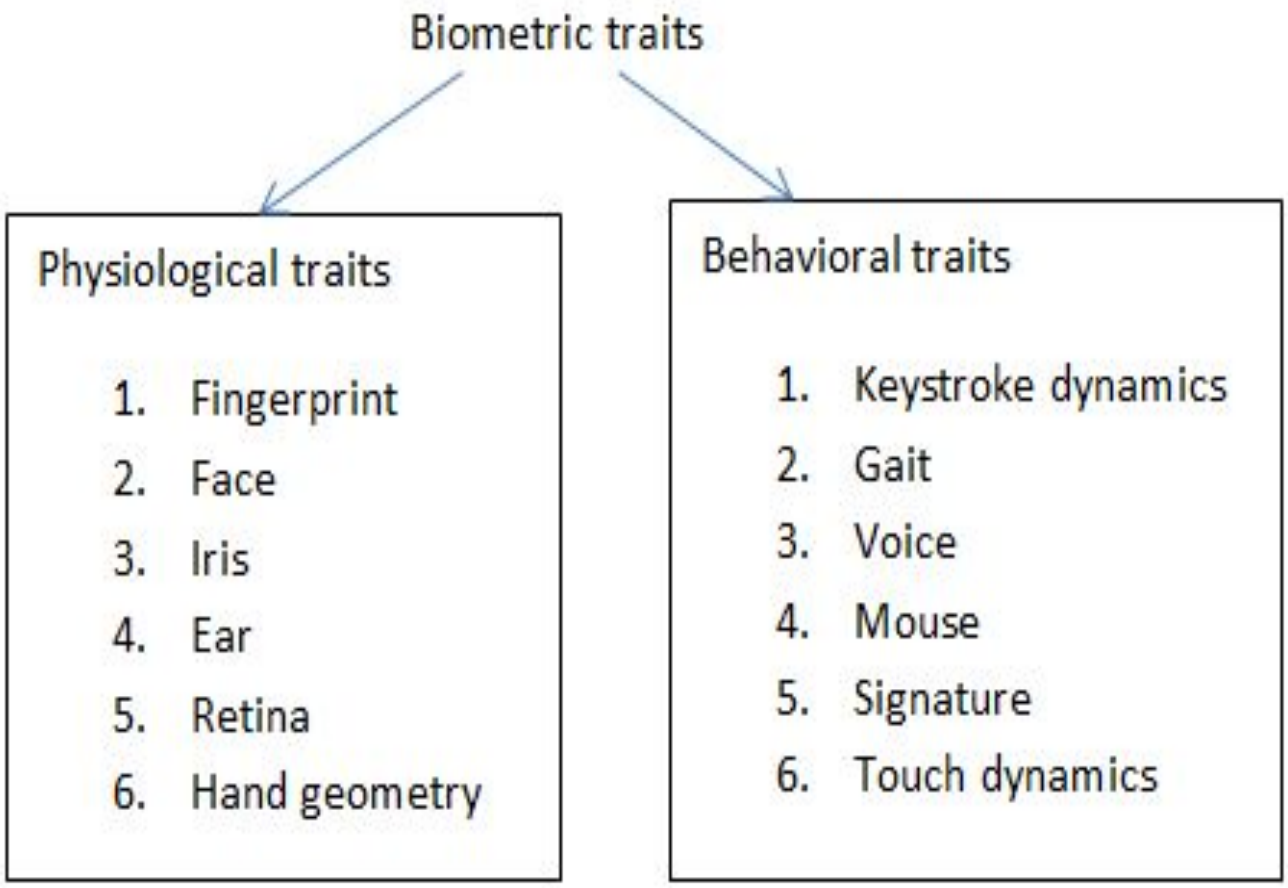
2. Door, Car, Garage Access



3. ATM Access, Smart card

Image Source : http://www.voice-security.com/Apps.html

Classification Of biometrics



Physiological traits

- **Fingerprint**

- Fingerprint biometric technique is widely accepted as cost is low and gives high efficiency. A fingerprint sensor captures the image of the fingerprint of the person. Image enhancement is done followed by the feature extraction and template protection. Ridges (minutiae points), valley, island, lake are the features extracted from the fingerprint image. Feature vectors are acquired from the acquired image. Many sensors like capacitive sensors, thermal sensors, and ultrasound sensor are used to acquire the fingerprint image.

- **Iris**

- Iris biometric system is considered to be the most accurate system. Iris image is collected and feature extraction is done by filters to extract the features. From the image, features like eyelids, eyelashes are extracted. Image acquisition is done by infrared illuminations, the steps in iris image processing is Image segmentation, image normalization, feature extraction and finally classification

Physiological traits

- Face
- Face recognition system is commonly used system for many commercial applications related to public security. The image captured from sensors will have noise, blur and the quality of the image may be weak. To enhance the quality of image, enhancement techniques like pre-processing is done. Fisher discriminant analysis is done for the feature extraction process and feature vectors are generated for recognition process. The features extracted from face are eyes, nose, and mouth.

- **Palm print**

- Palm print recognition uses a scanner to capture the features of palm in human. Thermal or optical scanners may be used. Ridges, wrinkles are the features extracted. The methods used for feature extractions are line based, subspace based (PCA, LDA) and statistical (mean, standard deviation). Neural network is been deployed for classification of final decision.

Physiological traits

- **DNA**

- DNA biometric systems involves Identification of person by using his DNA as a trait. DNA code is comprised of four bases: adenine (A), guanine (G), cytosine (C), and thymine (T). DNA can be extracted from saliva, blood and hair. The investment cost for setting up laboratory for DNA biometrics is high. DNA biometric system helps in crime cases to find the victim and in medical diagnosis.

- **Periocular**

- Periphery of ocular (periocular) is biometric system designed as an alternative to iris system. It contains the features in visible spectrum and infrared spectrum. It has reduced feature set and hence the matching accuracy is fast and suitable for mobile based applications. The key point is detected using reduced phase intensive local pattern method.

- **Palm vein**

- The vein patterns of the palm are captured by the infrared light sensor. The features extracted are black lines. The veins within the hands are internal to the body and it is difficult to forge. It is mainly used in banking sector for ATM, remote banking.

Physiological traits

- **Finger vein**
  -
- There is a unique finger vein pattern inside a finger and it can be captured by IR light transmission. Pre-processing is done on the vein image and noise is removed by applying various filtering techniques and normalization is carried out. Parameters like mean, skewness and response time is calculated and it is used during the matching process.

- **Retina**

- The retinal image is captured from the camera and its blood vessel pattern is recorded for the further processing. The Vascular features and non-vascular features can be extracted from the image. Non-vascular features(mean) does not require blood vessel pattern. Retinal verification is considered to be the fastest processing as its feature vector size is small.

- **Hand geometry**

- Infrared sensors are used to capture the vein patterns inside the person hand. Vascular patterns are captured and principal component analysis is applied on the extracted feature to achieve a very good matching and verification rate. Edge detection methods and texture-based methods are used to extract the features.

Behavioral biometrics

- *Gait*
- The emergence of computer vision has paved the way for smart surveillance system. Gait recognition is mostly used for the surveillance applications. Gait biometrics records the way the person walks, cyclic motion. The background subtraction method is used to find the object in motion. As huge amount of data is involved and hence machine learning techniques are adopted for training the data.

- **Voice**

- Voice print is the unique voice of individual to identify and verify the system. A spectral feature from the voice is measured. It is a pattern recognition approach which uses the speech signal to extract the features. Mel-frequency cepstral coefficients, Linear Prediction cepstral coefficients are the few techniques adopted for feature extraction. Modelling the voice is done by neural network

- **Handwriting**

- Handwriting biometrics helps in identifying the person by his written text. It is extraction of textural features of an individual handwriting and involves various parameters like segment counts, number of pen ups events, number of pens down events, duration of writing, pressure, spatial coordinate etc. The data acquisition is done by digital tablet.

Behavioral biometrics

- **Signature**

- The signature is captured by Pen tablets. Signature verification can be done in two ways namely online signature and offline signature. The image is acquired, pre-processed, feature is extracted and selected template is generated and stored in database. Features like X, Y coordinates, Pressure, Event type is extracted and signature embedding is done in barcode. precision, F measure and recall are calculated. Signature verification is mainly used in many applications like patent office, E procurement. Etc.

- **Keystroke Dynamics**

- It is process of analyzing the typing pattern of the individual. The timing features are extracted; overall typing speed frequency of errors while typing is recorded. Classification and training the patterns is done by artificial neural network and support vector machine. Online courses use this technique of keystroke dynamics to check the verification of the individual during the tests conducted.
-

- **Touch Dynamics**

- All modern devices are touch enabled, hence touch dynamics is considered to be trending biometric. The touch actions like scrolling, swiping, alphabet input, numerical input is monitored and captured and recorded. Probabilistic modelling and cluster analysis are employed for pattern recognition approach of touch patterns. Main application is on the Android smart phones which use the touch logger app.

- **Mouse Dynamics**

- Mouse dynamics is about the capture of mouse movements of the individual. The various mouse movements are drag, drop, move and click. Only few datasets are available for mouse movements. Segmentation is done on the mouse movements and statistical features like mean, standard deviation, min and max is calculated between the mouse movements from one position to other position. Statistical and probabilistic models are used for the feature extraction and classification of mouse movements' patterns.

SOFT BIOMETRICS

- The soft ones are related to faces, as skin color, hair color or facial measurements, to bodies, like height or weight, and to accessories, such as glasses or hats.

Hard biometrics

- The hard ones are also considered classic or traditional, such as faces, fingerprints or signatures

Hidden biometrics

- The hidden ones, called also intrinsic, are based on medical data, as bio signals, MRI images or X-Ray images

Security breach

- When the biometric system fails to meet these objectives, the security of the system is said to be breached.

This breach of security can be in the form of denial-of-service to legitimate users, intrusion by unauthorized users, repudiation claims by authorized users, or misuse of the biometric data for unintended purposes.

- A natural question that arises in biometric recognition is which biometric system is “best” suited for a particular application.
- Of course, the answer to this question depends not only on technical merits and limitations of the biometric system (e.g., matching accuracy and throughput), but also on other socio-economic factors like user acceptability and system cost

REQUIREMENTS OF BIOMETRIC SYSTEM

- legitimate users must have timely and reliable access to the protected resource/service. This is referred to as the *availability* of the biometric system.
- The biometric system and the personal data stored in it must be used only for the intended functionality, which is to control access to a specific resource and not for other unintended purposes. This is known as the *confidentiality*
- requirement.

SECURITY THREAT

- A security threat in a biometric system refers to the possibility of system failure.
- Depending on the type of failure, these security threats can be classified into four major classes.
- **Denial-of-service (DoS)**:
- **Intrusion**
- **Repudiation**
- **Function creep**

Denial-of-service (DoS):

- Legitimate users are prevented from obtaining access to the system or resource that they are entitled to, thereby causing inconvenience to genuine users. This violates the availability requirement.
- Frequent denial-of service is likely to eventually drive the users towards abandoning the biometric system altogether.

Intrusion

- An unauthorized user gains illegitimate access to the system.
- Since intrusion affects the basic integrity of a biometric system, it is generally considered the most serious security threat

Repudiation:

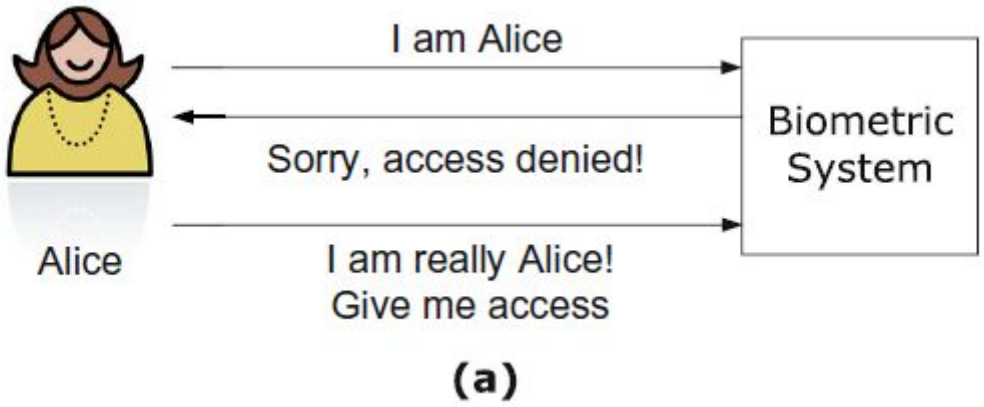
- A legitimate user denies using the system after having accessed it.
- Corrupt users may deny their actions by claiming that illegitimate users could have intruded the system using their identity.

Function creep

- An adversary exploits the biometric system designed to provide access control to a certain resource to serve another application, which the system was never intended to perform.
- For example, a fingerprint template obtained from a bank's database may be used to search for that person's health records in a medical database. This violates the confidentiality requirement.
- Although the problem of function creep has been posed primarily as a security threat, it is also widely perceived as a major threat to user privacy.

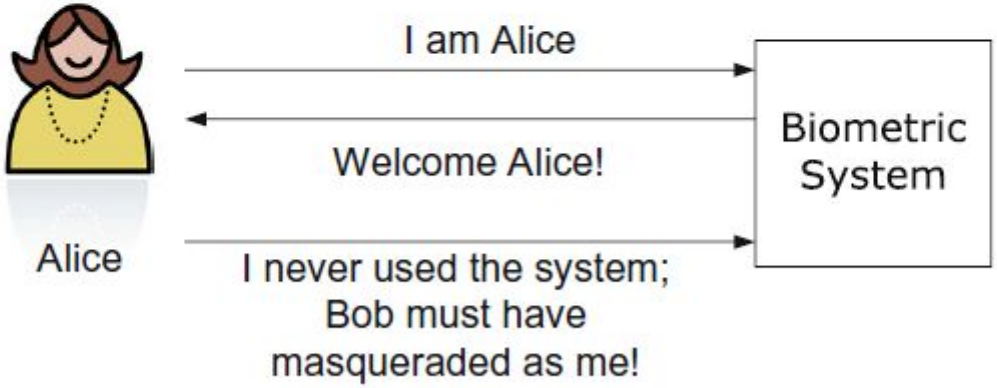
- Public confidence and acceptance of biometric technology will depend on the ability of system designers to guard against all possible security threats.
- However, no system is likely to be absolutely secure and foolproof.
- Given the right circumstances and plenty of time and resources, any security system can be broken

DOS


I am Alice
Biometric System
Sorry, access denied!
Alice
I am really Alice!
Give me access
(a)

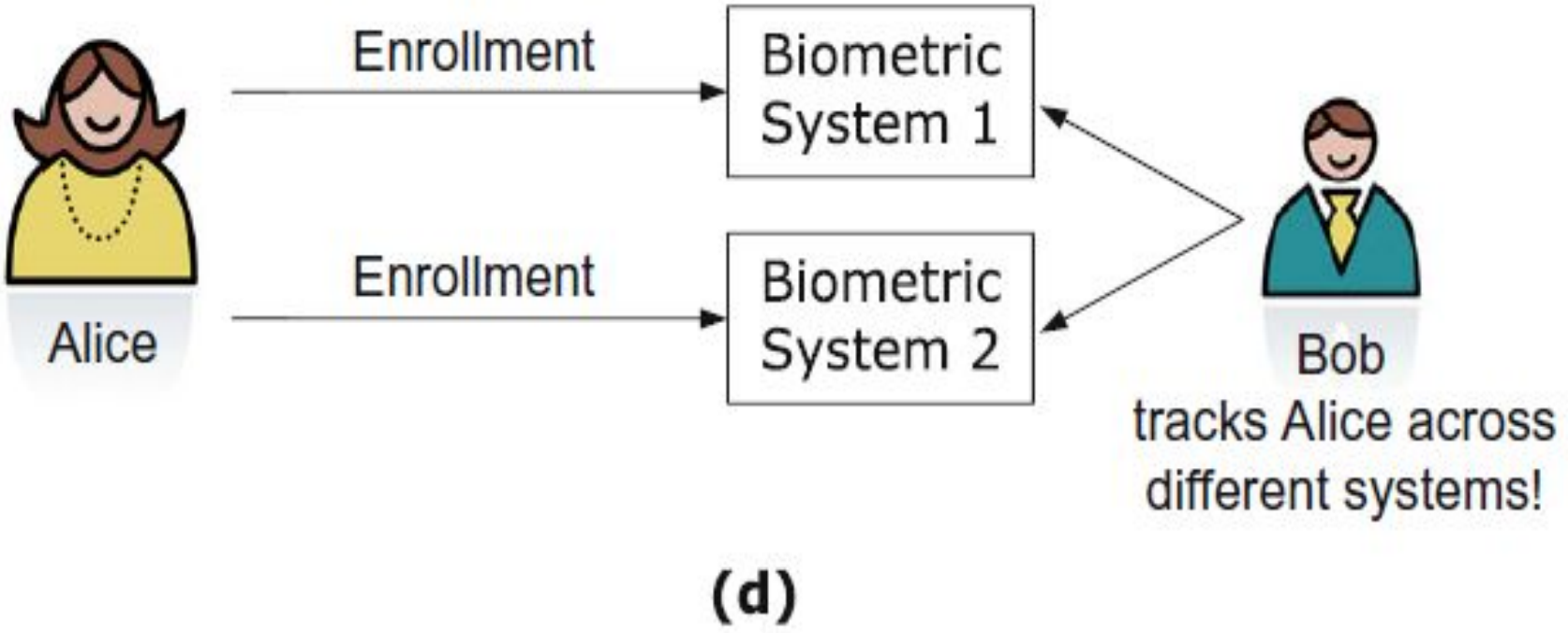
INTRUSION AND REPUDIATION

(b)



(c)

Function creep



(d)

- biometric system designers must strive to plug as many loopholes as possible, the reality is that the level of security ensured is generally based on the requirements of the application

- the level of security in biometric systems used for critical applications like border control can be expected to be much higher than that of a biometric system used for logging in to a personal computer.

THREAT MODEL

- The first step in analyzing the security of biometric systems is to define a threat model, which identifies the various threat agents and attacks.
- *threatagent* can be defined as a person or a thing that can, or has the power to subvert the intended operation of a system.

Intrinsic limitations:

- Even in the absence of any external attacks, a biometric system may fail due to its intrinsic limitations. As discussed in Chapter 1, all biometric systems are prone to two types of errors, namely, false match and false non-match.
- A biometric device may also fail to capture or acquire a sample of the biometric identifier presented to it by the user, leading to failure to enroll and failure to capture errors.
- Since these errors are caused due to intrinsic limitations of various modules in a biometric system like sensor, feature extractor, and matcher, and not by any deliberate attack, the resultant failure or security breach is known as a *zero-effort attack*.

Adversaries:

- A biometric system may also fail due to manipulation by adversaries, who could either be insiders or external entities.
- An insider is an authorized user of a biometric system, which includes both system administrators (super-users) and any other person enrolled in the biometric system.
- External entities can be classified as impostors and attackers.
- While the term impostor refers to any individual who intentionally or inadvertently tries to impersonate another enrolled person, an attacker is one who attempts to subvert the operation of a biometric system.

ATTACK

- An *attack* refers to the actual mechanism or path that can be used to circumvent a biometric system.
- A taxonomy of attacks that can be mounted against a biometric system is shown in Figure 7.2. Based on the threat agent used in the attack, the attack mechanisms can be broadly categorized as those caused by intrinsic limitations(zero-effort attacks) and the ones caused by adversaries.

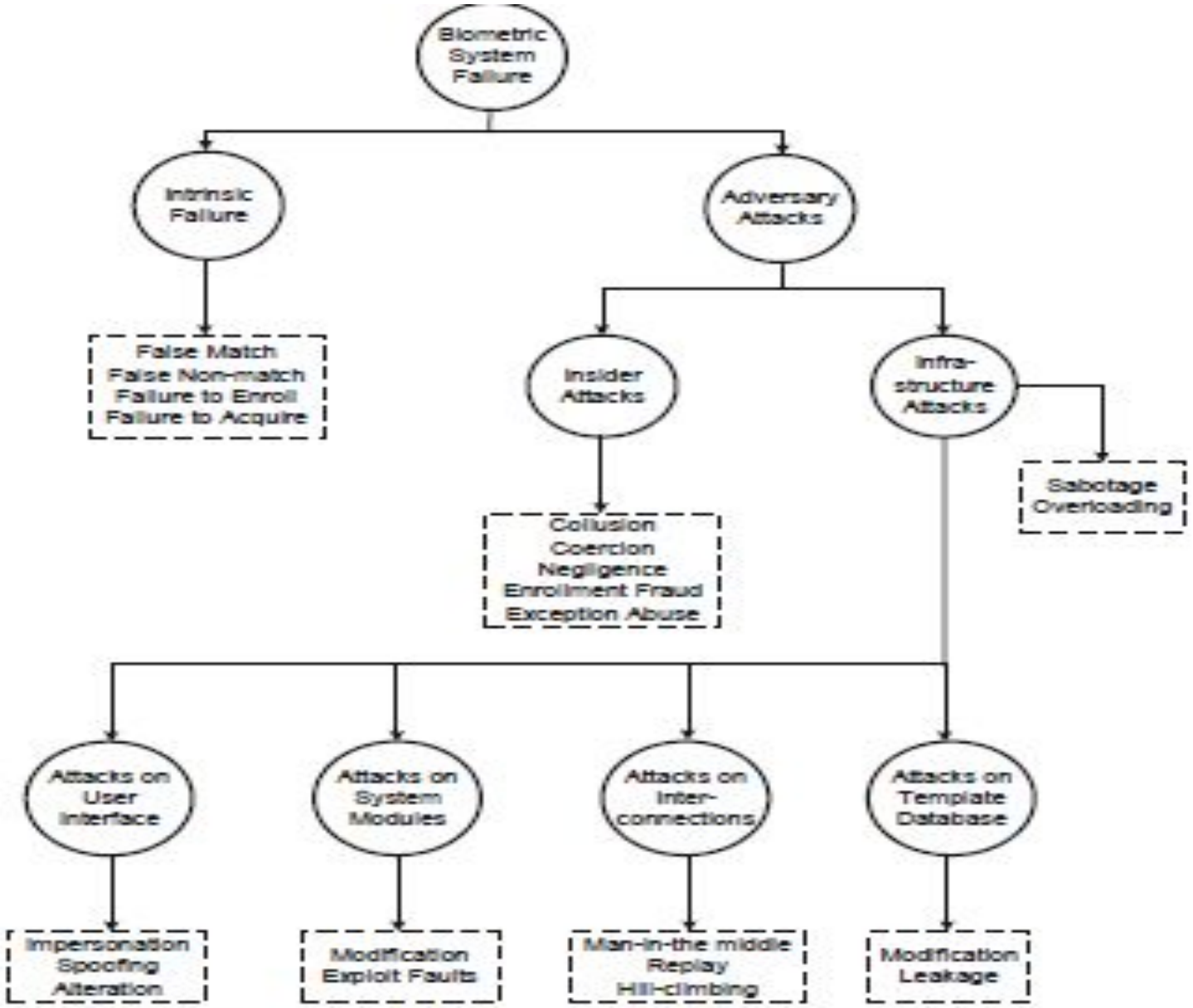


Fig. 7.2 Taxonomy of attacks that can be mounted against a biometric system.

CONSEQUENCES OF ZERO EFFORT ATTACK

- The consequences of a zero-effort attack will depend on the application. For instance, in a biometric verification system, a false non-match error will lead to denial-of-service and inconvenience to genuine users.
- On the other hand, in a negative recognition application such as screening, a false non-match will lead to intrusion and a false match will lead to denial-of-service.
- Since failure to enroll and failure to capture errors necessitate the operators to fall back on traditional (possibly unreliable) authentication mechanisms like ID cards, the effect of these errors is similar to that of a false non-match.
- The intrinsic limitations of a biometric system also make it hard to defend against repudiation claims.

METRICS

- These metrics include
- false match rate (FMR),
- false non-match rate (FNMR),
- failure to enroll rate (FTER),
- failure to capture rate (FTCR),
- false positive identification rate(FPIR), and false negative identification rate (FNIR).

- the probability of success of an adversary attack depends on a number of tangible as well as intangible factors.
- This includes implementation and operational details of the biometric system, how the biometric system is integrated with the overall application (e.g., how does the biometric authentication interact with other modules in a physical access control application), the resourcefulness of the adversary (e.g., available time and computational power), and the behavior of users interacting with the biometric system.
- Therefore, it is relatively difficult to predict in advance all the possible ways in which the biometric system can be attacked.

Adversary Attacks

- An adversary who intends to subvert a biometric system can make use of vulnerabilities either in the human element or in the system infrastructure.
- Adversary attacks can be categorized as *insider attacks* and *infrastructure attacks*

Insider attacks

- It is important to emphasize that the term “insider attacks” not only covers cases where an authorized user himself turns malicious and intentionally subverts a biometric system, but also includes cases where an external adversary circumvents the biometric system through direct or indirect involvement of an insider.

Insider attacks

- Biometric systems require human interaction at a number of stages.
- For example, a human administrator is usually required to carry out the enrollment and deenrollment of users.
- In addition, the administrator may also be involved in adjusting the security parameters controlling the performance of a biometric system such as threshold on the match scores and minimum limits on the quality of the acquired biometric sample.

- In attended applications, the administrator also appoints the operators to supervise the proper functioning of the biometric system and to guide the users.
- The operators are also typically responsible for operation of the fall-back system that will be used in the case of non-availability of the biometric system or when there is a failure to enroll/capture error.

five ways to breach the security of a biometric system.

- These human interactions can be exploited in the following five ways to breach the security of a biometric system.
- **Collusion**
- **Coercion**
- **Negligence**
- **Enrollment Fraud**
- **Exception Abuse**

Collusion

- This refers to the scenario where an authorized user willingly turns malicious and attacks the biometric system either individually or in collaboration with external adversaries (possibly in return for monetary gain).
- Such an attack may lead to serious security breaches, especially if the attacker is a system administrator.
- Since the administrator typically has the status of a super-user with powers to modify or control most modules of the biometric system, it could be extremely difficult to guard against this attack.

To avoid collusion

- The only safeguard against such an attack is to enforce responsible behavior among authorized users through proper training, rigorous monitoring, and auditing of all authentication transactions in order to detect any unusual pattern of activity, and penalizing those who do not conform to the rules.

Coercion:

- A coercion attack is similar to collusion, the only difference being that a coerced user does not carry out the attack willingly.
- Rather the authorized user is forced to turn malicious, possibly through a physical threat (e.g., at gunpoint) or blackmail.
- It is desirable to reliably detect instances of coercion without putting the genuine users at a greater risk from the adversaries.

Negligence:

- External attackers can also exploit the negligence of authorized users in order to circumvent the biometric system.
- A typical example is the failure of authorized users to properly log out of the system after completing their transaction.
- Propping a door open or permitting tailgating in physical access control scenarios can also be considered as negligence, if the intent of the authorized user is not malicious.
- Negligence can be minimized by periodically training the authorized users and constantly reminding them about the guidelines to be followed

Enrollment Fraud:

- The adversary may enroll himself into the biometric system illegally (under a false identity) by producing his biometric traits along with false
- credentials (e.g., fake passports and birth certificates). The reason for including
- this vulnerability under insider attack is that it is primarily caused by a flaw in the biometric system design, namely an over-reliance on existing (legacy) identity management systems for enrollment.

De duplication

- The solution to prevent enrollment fraud is to match the biometric traits of a new user against the traits of all enrolled users in order to detect a duplicate identity even before the new user is added to the system.
- This process is called *de-duplication*, which is a challenging problem because the number of enrolled users can be extremely large.

Exception Abuse

- Most biometric systems are equipped with a fall-back mechanism in order to permit handling of exceptional situations that may cause denialof-service to legitimate users.
- Examples of exceptional scenarios may include processing users with no fingers in a fingerprint-based recognition system and failure of some hardware/software components of the biometric system.
- In such cases, the system administrator has the ability to bypass the recognition system and make decisions based on other credentials like secrets and tokens.
- This provides the motivation for the attacker to trigger the exception processing procedures (e.g., by purposely degrading the quality of his biometric trait) and attempt to exploit the loopholes in the fall-back mechanism.
- The problem can be minimized by improving the reliability of the biometric system and using multiple biometric modalities to enlarge the population coverage.

Infrastructure attacks

- A generic biometric system consists of functional modules such as sensor, feature extractor, template database, matcher, and decision module.
- These functional modules are in turn composed of hardware and software components, and together with the communication channels interlinking them, they constitute the infrastructure of a biometric system.

- It is possible to place all the functional modules and the interfaces between them on a single smart card (or more generally a secure processor).
- In such systems, known as system-oncard or match-on-card technology, the biometric information never leaves the card(or the chip) and only the recognition results (match or non-match) are transmitted to the application

- On the other extreme, consider an Automated Fingerprint
- Identification System (AFIS) used in forensic applications.
- In the AFIS scenario, the modules of the biometric system are typically distributed across different physical locations (e.g. sensor may be at the crime scene, feature extractor and decision module may be at the regional investigation office, and matcher and database at a regional or national center).
- Other intermediate configurations where the sensor and feature extractor may reside together at a remote location (e.g., a mobile phone),while the matcher and database reside on the server are also possible.

ATTACKS

- Attacks that are common to any security system such as *sabotage* and *overloading* can also be mounted against a biometric system.

SABOTAGE

- Sabotage usually involves physical damage to one or more components of the infrastructure such that the whole biometric system is rendered useless.
- Examples of sabotage include disabling the power supply, damaging the sensor surface or introducing excessive noise (interference) that prevents the normal operation of the system.

OVERLOADING

- Overloading is an attempt to defeat the system by overwhelming it with authentication requests.
- The motivation for these attacks is typically to deny access to genuine users.
- But it may also be used as a ploy to force the operator to rely on afall-back mechanism that may be easier to circumvent.

- The following four categories can be identified:
- (a) attacks at the interface between the user and the biometric system
- (b) attacks on the system modules (sensor, feature extractor, matcher, and decision module),
- (c) attacks at the interconnection between the modules, and
- (d) attacks on the template database.

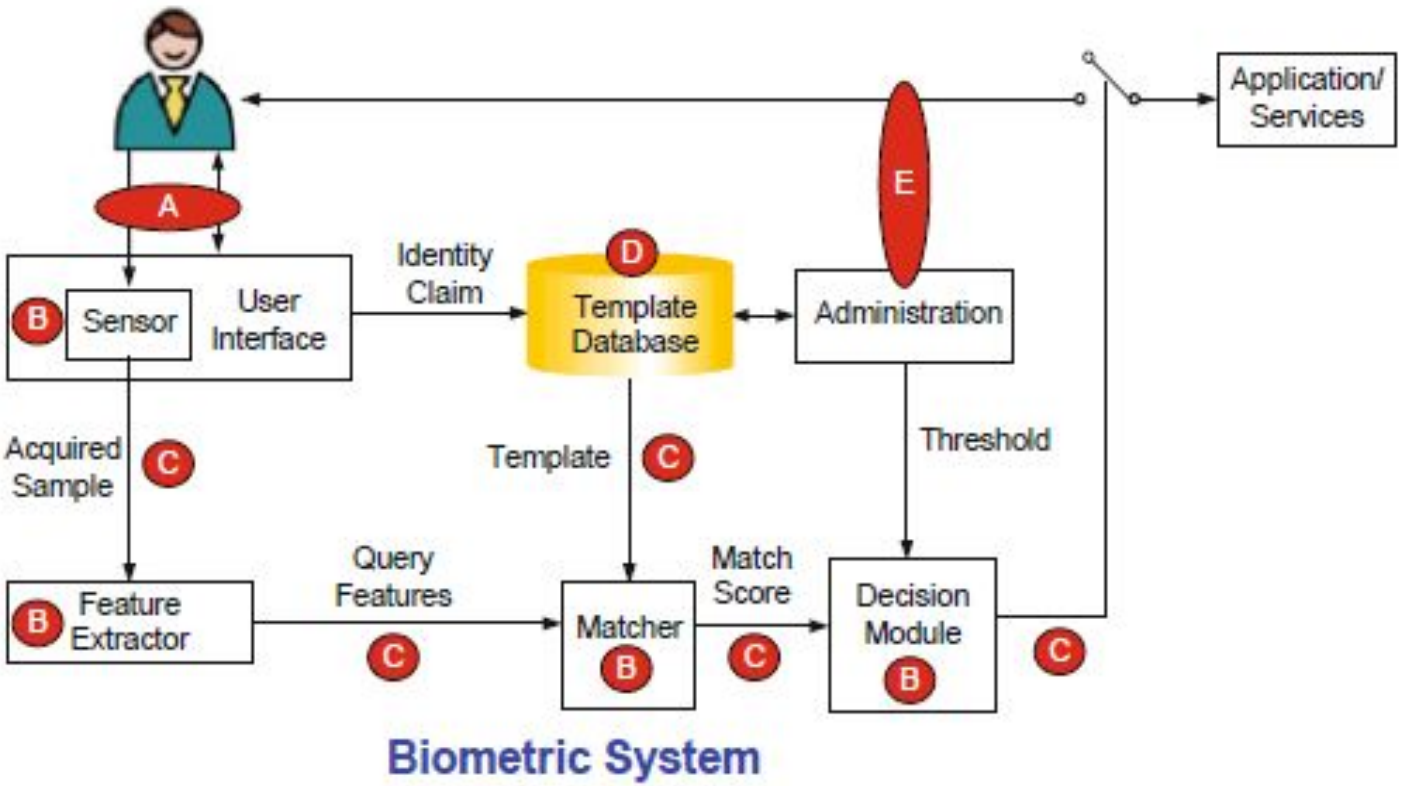


Fig. 7.3 Types of adversary attacks in a biometric system. The five major areas of vulnerability are: (A) user-biometric system interface, (B) biometric system modules, (C) interconnections between biometric modules, (D) template database, and (E) attacks through insiders (administrators or enrolled users).

ATTACKS AT THE USER INTERFACE

- ***Impersonation***
- ***Obfuscation***
- ***Spoofing***

Impersonation

- This refers to the situation where an impostor attempts to intrude the system by posing himself as another authorized user.
- The impersonation could be either casual or targeted.

Casual impersonation

- In *casual impersonation*, the identity to be attacked is chosen randomly and the impostor does not modify his/her own biometric identifiers in any way.
- The probability of success in such an attack is usually measured by the false match rate (FMR) of the biometric system.
- This attack can be countered by selecting a very low value of FMR and by restricting the number of failure attempts allowed within a time-frame.

Targeted impersonation

- Targeted impersonation occurs when the impostor attacks a specific identity enrolled in the biometric system, which is known to be easier to impersonate (also known as a “lamb” in the Doddington’s Zoo).
- This attack exploits the fact that FMR is not uniform across all users.
- The impostor may also target an identity whose biometric characteristics are known to be similar to his traits (also known as “Evil Twin” attack).
- The same countermeasures used against casual impersonation may be employed to limit the success of this type of attack.

MIMICRY

- the impostor may also be able to modify his biometric characteristics to match that of the identity under attack. A common name for such an attack is *mimicry*.
- Examples of this attack include changing one's voice, forging a signature (see Figure 7.4), or mimicking a gait pattern.
- This threat is more common in systems using behavioral biometric traits and in applications with unattended mode of operation.
- Countering this attack requires biometric systems that have low false match rate (FMR) under skilled forgery.

MIMICRY

Fig. 7.4 Example of a mimicry attack. (a) Genuine signature samples of a person, (b) skilled forgeries of the signature in (a) created by impostors. (Source: BioSecure Association)

OBFUSCATION

- Any deliberate attempt by an attacker to change his biometric characteristic in order to avoid detection by the biometric system is called obfuscation.
- Thus, the key difference between mimicry and obfuscation is the motivation behind the attack.
- Obfuscation is mainly applicable in negative recognition applications, where the attacker wants to hide his true identity.
- However, it may also be applicable in verification systems that employ a fall-back mechanism to handle false rejects.
- In this scenario, the adversary may attempt to bypass the biometric system by forcing a false reject decision and then exploit the loopholes in the fall-back mechanism, which may be easier to circumvent.

- Obfuscation can be done in a number of different ways. One possibility is to intentionally present a poor quality image or noisy biometric sample (e.g., face with non-neutral expression or a partially open eye) that may not be matched to his/her template in the database.
- In the case of face recognition, use of makeup, facial hair, and glasses can also lead to a false non-match. Fingerprints can be obliterated through techniques like abrasion, cutting, and burning, or may even be surgically altered or distorted (see Figure 7.5).
- Similarly, face can be altered using plastic surgery and iris transplants have been depicted in popular science fiction (e.g., in the movie Minority Report).
- Knowledge of the details of biometric processing algorithms can further facilitate such attacks. For example, if the attacker knows that a particular face recognition system is not robust to pose variations, he can easily circumvent it by presenting only a profile view of the face.

OBFUSCATION

Fig. 7.5 Examples of fingerprint alteration. (a) Transplanted fingerprints from the friction ridge patterns found on the sole of the feet (http://www.clpex.com/images/FeetMutilation/L4.JPG), (b) fingerprints obliterated by biting off the finger skin, and (c) fingerprints altered by making a Z shaped cut on the fingertip, lifting and switching the two triangles, and stitching them back; left image shows the original fingerprint and the altered fingerprint is shown on the right. The alteration shown in (c) involved a man using the name Alexander Guzman, who was arrested by Florida officials in 1995 for possessing a false passport and found to have mutilated fingerprints. After a two-week search based on manually reconstructing the altered fingerprints and searching the FBI database, the reconstructed fingerprints of Alexander Guzman were linked to the fingerprints of Jose Izquiredo, who was an absconding drug criminal. This example illustrates both the usefulness of a biometric system as well as the desperate measures that criminals often take to circumvent a biometric system.

Spoofing

- This is the most well-known attack at the user interface level, and it involves the presentation of a spoof biometric trait.
- A spoof is defined as any counterfeit biometric that is not obtained from a live person (see Figure 7.6).
- Spoofing includes the presentation of fake or artificial traits (e.g., gummy finger, thin film on top of a finger, photograph or mask of a face, recorded voice, etc.) and things as sinister as dismembered body parts (e.g., a dismembered finger) belonging to a legitimate user to the recognition system.
- If the sensor is unable to distinguish between spoofed and genuine biometric traits, the adversary can easily intrude the system under a false identity.

(a)

(b)

(c)

Fig. 7.6 Examples of spoofed biometric traits. (a) Fake fingerprints made from glue and dismembered fingers (Source: Lumidigm, Inc.), (b) a fake hand made of plaster, and (c) a photograph of an iris (Source: C't magazine).

- This attack requires knowledge of the biometric trait corresponding to the identity to be attacked.
- This knowledge could be obtained in one of the following four ways:
- (a) directly colluding with or coercing an authorized user
- (b) covert acquisition (e.g., lifting residual fingerprint impressions covertly from the sensor or any surface touched by the authorized user, recording the user's voice, or capturing a photograph of the user's face)
- (c) estimating a close approximation of the user's biometric template through brute-force or hill-climbing attacks,
- (d) stealing the biometric template from a database and reverse engineering the template.

Countermeasure

- While traditional password-based authentication systems work under the assumption of secrecy (i.e., only the legitimate user knows his password), such an assumption is generally not required for a biometric system to work.
- In contrast, the strength of biometric authentication is derived from the fact that the biometric characteristic is linked to the user physically.
- Though an attacker may get hold of a legitimate user's fingerprint pattern, it would not be of much use to the attacker if the sensor can ensure that the scanned fingerprint comes directly from the finger of a live user.
- Therefore, the solution to counter spoof attacks is to incorporate liveness detection capability in the biometric sensor.

Spoof Detection

- Spoof detection can be broadly defined as differentiating a real biometric trait presented by a live person from a biometric trait presented through any other source.
- Spoof detection typically involves checking for signs of human vitality or liveness (e.g., blood pulse), a process known as liveness detection.

SPOOF DETECTION

- The susceptibility of a biometric system to a spoof attack depends both on the biometric modality and the specific sensor used to capture the biometric trait.
- For example, a two-dimensional photograph of a human face may be sufficient to fool a camera used in a face recognition system.
- However, it is usually very difficult to circumvent an optical or capacitive fingerprint sensor by using a 2-D reproduction of a fingerprint because such sensors inherently depend on capturing the 3-D variations in the ridge-valley structures.

SPOOF DETECTION

- Firstly, almost all spoof detection solutions increase the cost of the biometric system.
- This is because of the need to have additional hardware to capture new information (e.g., spectral or thermal properties)
- a software module to process the biometric data already collected and distinguish between a spoof and a live trait.
- This additional processing also increases the biometric acquisition time, thereby reducing the throughput of the biometric system

SPOOF DETECTION

- Though there are a number of biometric spoof detection algorithms, they can be classified into three main groups based on the mechanism employed for thwarting a spoof attempt.
- **Spoof detection based on physiological properties**

THREE APROACHES

- The first approach involves measuring the physiological properties of a live person, which includes blood pulse/pressure, perspiration, spectral/optical properties of the human skin/tissues, electrical/thermal characteristics, and deformation of the muscles/skin.
- The second approach is based on identifying voluntary or involuntary human behavioral actions like fluctuations in pupil size, blinking, and pupil/eye/head/body movements.
- The third category is known as the challenger esponse mechanism, where the system presents a challenge to the user and measures whether the user responds to the challenge correctly.

EXAMPLE OF CHALLENGE

- Examples of challenges include prompting a user to recite a randomly generated phrase/text, asking the user to change his or her facial expression (e.g., smile or frown), and requesting the user to present multiple biometric traits in a randomly generated sequence

Spoof detection based on physiological properties

- biometric systems are based on physiological characteristics that are unique to each individual (e.g., fingerprint, iris, face), spoof detection algorithms tend to use characteristics that can easily distinguish a human body from innate materials (e.g.,

silicone gel for fingerprints) used for spoofing.

Pulse rate/ Blood pressure

- This property is generally applicable to biometric traits such as fingerprint and palm print that require the user to be in physical contact with the sensor.
- While the pulse rate is a good vitality sign, special hardware may be needed to record this trait.
- Moreover, the pulse rate and blood pressure vary significantly from one person to another and also within the same person on his physical activity and emotional state at the time of acquisition.
- Furthermore, a single pulse measurement may take up to five seconds. Finally, if a wafer-thin silicone rubber is glued to a real finger, the heartbeat of the underlying finger will result in the detection of a pulse.

Perspiration

- Perspiration refers to the sweating process of a live finger. Live fingers exhibit sweating over a period of time whereas fake fingers will not exhibit the sweating process.
- The perspiration phenomenon starts at the sweat pores on a fingerprint and spreads along the ridge lines, while the valleys do not change.
- Due to the sweating process in live fingers, the regions around sweat pores can be seen to enlarge over time in a sequence of fingerprint images (see Figure 7.7).
- One limitation of this procedure to detect a spoof finger is that to observe the sweating process, the finger needs to stay on the fingerprint scanner for a few seconds.
- The perspiration-based methods are also expected to have some difficulty in dealing with varying amounts of moisture content occurring in live human fingers.

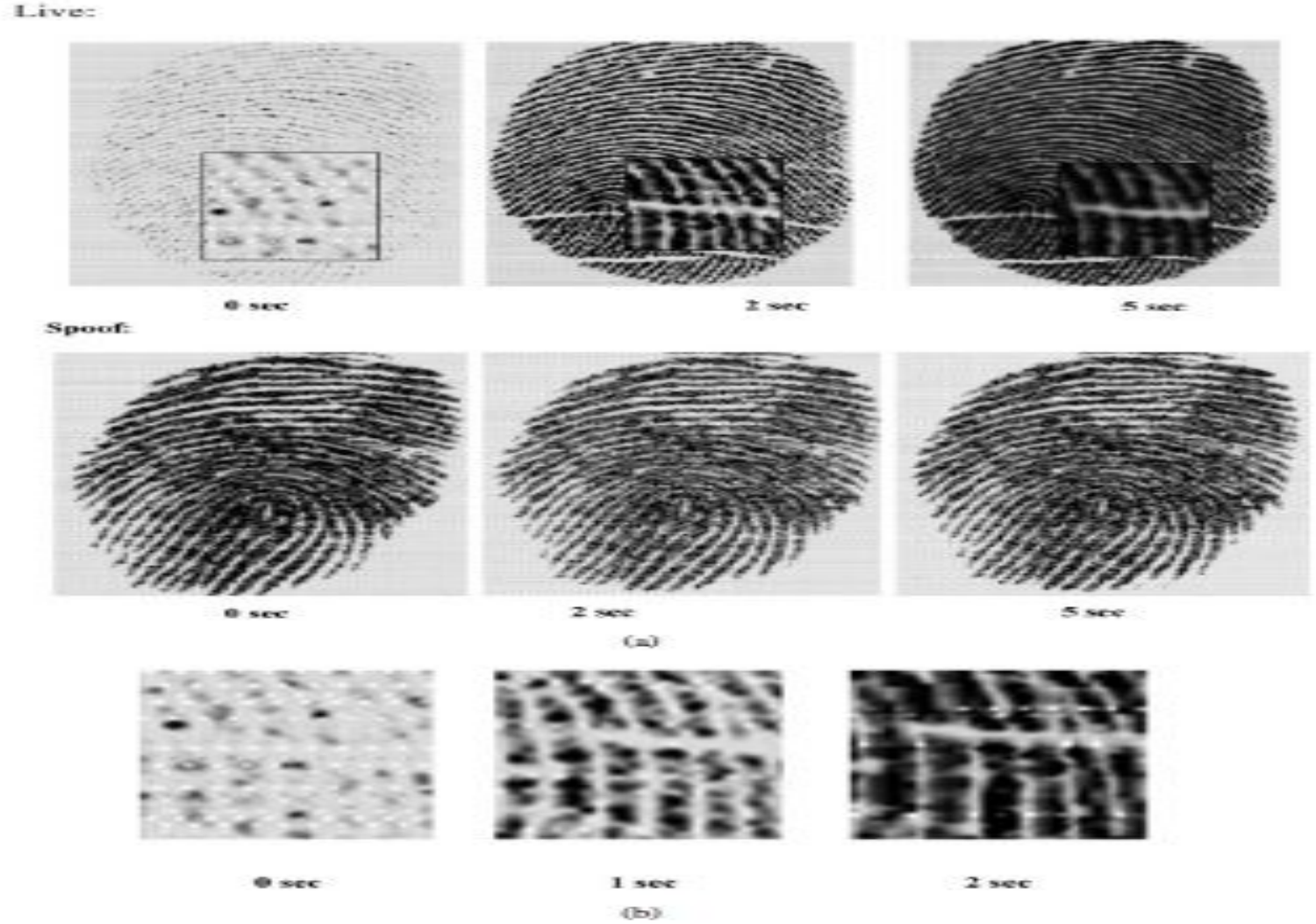


Fig. 7.7 An example of fingerprint spoof detection based on the perspiration pattern of a live finger (adapted from [35]). (a) Example fingerprint images obtained from a live finger (top row) and a fake finger (bottom row) acquired at 0, 2, and 5 seconds after the finger is placed on the sensor, (b) enlarged fingerprint image sequence that demonstrates progression of a perspiration pattern over time in a live finger. ©IEEE

Spectral/optical properties of the human skin

- This is one of the most common characteristics that has been successfully used for spoof detection in many biometric systems, including fingerprint, palmprint, face, and iris.
- The optical properties that may be measured include the absorption, reflection, scattering, and refraction properties under different illumination conditions (such as wavelength, polarization, coherence)

- In the case of fingerprints, multi-spectral analysis may be used to measure the surface properties as well as sub-surface properties of a finger since components of blood (oxygenated and deoxygenated hemoglobin) absorb different wavelengths of light.
- Similarly, the tissue, blood, fat, and melanin pigments in the eyes absorb differentwavelengths of light.
- These properties can be leveraged for liveness detection in fingerprint (see Figure 7.8) and iris recognition systems.

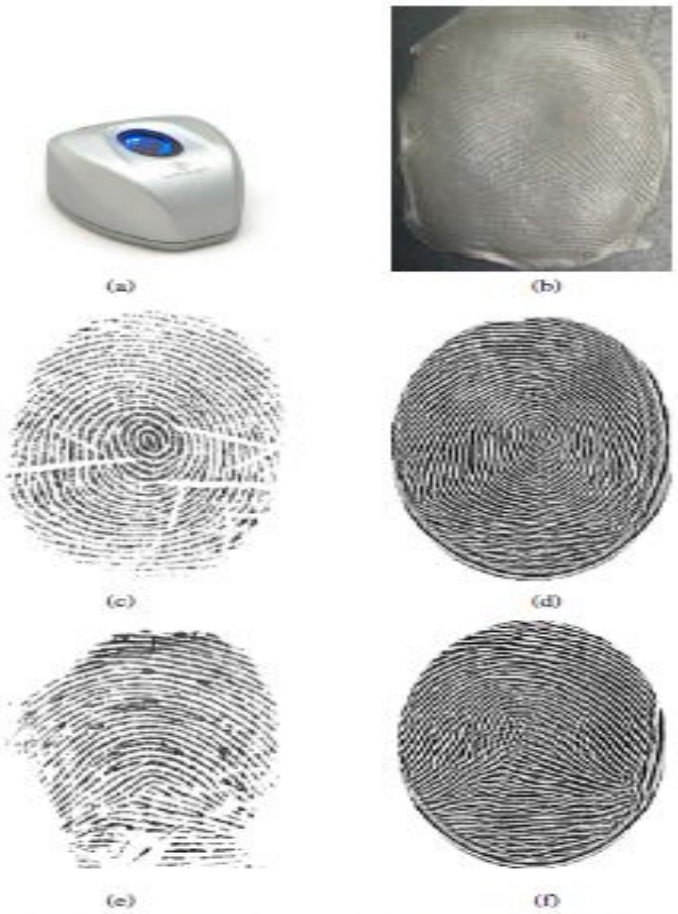


Fig. 7.8 An example of fingerprint spoof detection using the spectral properties of the human tissue. (a) a multi-spectral fingerprint sensor from Lumidigm, Inc. that is capable of capturing the sub-surface properties of a finger, (b) a spoof fingerprint made from glue, (c) an impression of the real finger acquired using a traditional optical fingerprint sensor (based on total internal reflection (TIR) principle), (d) an impression of the real finger acquired using the multi-spectral fingerprint sensor, (e) an impression of the spoof finger (glue spoof overlaid on the real finger) acquired using the optical fingerprint sensor, and (f) an impression of the spoof finger acquired using the multi-spectral fingerprint sensor. It can be observed that the multi-spectral sensor is able to see through the spoof and capture the ridge pattern of the underlying real finger. (Source: Lumidigm, Inc.)

Electrical characteristics:

- The electrical conductivity of human tissue differs from conductivity of many other synthetic materials such as silicone rubber and gelatin.
- The conductivity of the material presented to the fingerprint sensor can be measured to differentiate a live finger from a fake finger.
- However, the conductivity of live fingers varies a lot depending on environmental conditions such as humidity and temperature. If water or saliva is added to a fake finger, its conductivity may be indistinguishable from that of a live finger

Skin deformation:

- The deformation pattern of the human skin can be used for differentiating live fingers from fake fingers.
- Skin is more flexible than most other materials and the ridges and valleys in a fake finger do not deform like a live fingertip.
- Real live skin deforms only in a certain way because the skin is anchored to the underlying derma and the deformation is influenced by the position and shape of the finger bone.
- But measuring these deformation patterns is not easy because it requires capturing a video of the fingerprint at a high frame rate as the finger moves on the sensor surface.
- This is problematic because most fingerprint sensors are designed for single-touch fingerprint acquisition and the users are trained not to move the finger during capture; excessive deformation will affect the matching accuracy of the system.

- One of the common criticisms of the liveness detection algorithms employed in commercial biometric systems is that they are based solely on the principle of *se curity through obscurity*.
- In other words, biometric vendors do not generally reveal the algorithm or implementation details about their liveness detection methodology because if the specifics of the spoof detection techniques are revealed, the system can be circumvented easily.
- Experience in cryptographic systems has shown that this approach does not provide satisfactory results over a period of time.
- Once an attacker identifies a possible vulnerability and successfully carries out a spoof attack, the complete system falls apart. Therefore, one should assume that the attacker has knowledge about the physiological properties used by the system for detecting spoofs

Attacks on Biometric Processing

- The signal processing and pattern matching algorithms that form the crux of automated biometric recognition are implemented in the sensor, feature extractor, matcher, and decision modules.
- Thus, an attacker can subvert the biometric processing either by directly undermining the core functional modules of the biometric system or by manipulating the communication between these modules.
- Though the template database is also one of the modules in the biometric system, the motivation and consequences of an attack on the template database are different compared to the other modules. Therefore, the attacks on the template database will be considered separately.

Attacks on the system modules

- Attacks on the core functional modules can be mounted either through unauthorized modification or by exploiting the faults in their implementation.
- The motivation of these attacks could be to cause denial-of-service to legitimate users or facilitate intrusion.
- **Unauthorized modification**
- **Exploitation of faults**

Unauthorized modification

- The hardware and software components of a biometric system can be modified by attackers.
- A classic example is the modification of an executable program in a module through a Trojan horse attack.
- A Trojan horse is malicious software that appears to perform a desirable function for the user, but instead performs some other function that usually facilitates intrusion by unauthorized users.
- The Trojan horse can disguise itself as one of the modules, bypass that module, and output the values desired by the adversary as input to the subsequent modules.

- For instance, a Trojan horse program can bypass the feature extractor and send the false features determined by the attacker to the matching module (see Figure 7.10).
- Similar attacks can also be carried out at the sensing, quality estimation, matching, template database,and decision modules.

Torjan horse attack

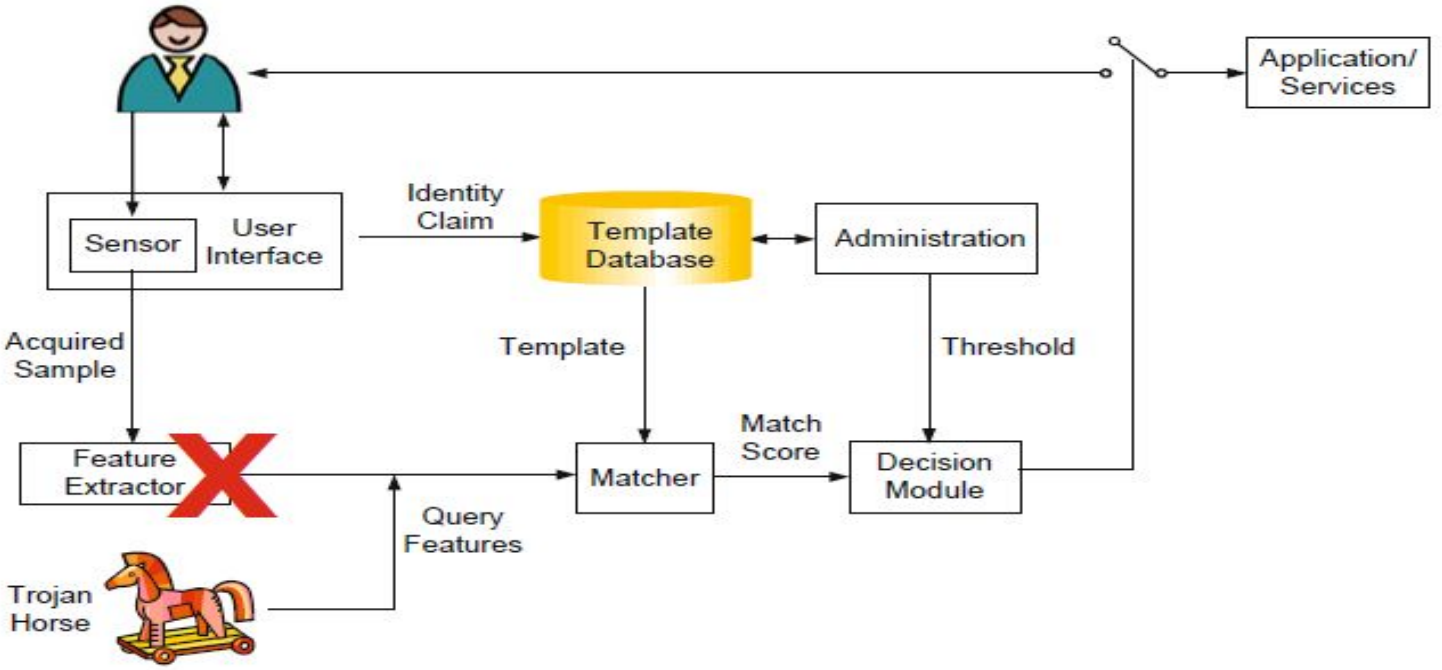


Fig. 7.10 A Trojan Horse attack against the feature extraction module is shown. A Trojan horse is a malicious software that appears to perform a desirable function for the authorized user, but instead performs some other function that usually facilitates intrusion by unauthorized users. In this example, the Trojan horse replaces the feature extractor and outputs the features decided by the attacker instead of the features extracted from the input biometric trait. If the sensor and the matcher modules are unaware of the fact that they are communicating with a Trojan horse, and not with the real feature extractor, it will lead to either denial-of-service to genuine users or intrusion by attackers.

- One method to overcome this attack is to employ a trusted biometric system.
- A trusted biometric system is one in which the different modules are bound together physically and/or logically using mutual authentication between the modules.
- Mutual authentication implies that the trust is established both ways between two communicating parties. This is usually achieved through public key cryptographic protocols and digital signatures.
- In addition to mutual authentication, secure code execution practices or specialized tamper-resistant hardware that can enforce secure execution of software can be used to avoid modification of the module functionalities.

Exploitation of faults

- The attacker may identify and exploit the loopholes in the implementation of the biometric algorithms or insecure configuration to circumvent the biometric system.
- As an example, consider a matching module in which a specific input value, say **b**0, is not handled appropriately, and whenever **b**0 is input to the matcher, it always out puts a “match” decision.
- This vulnerability might not affect the normal functioning of the system because, in practice, the probability of **b**0 being generated from a real biometric data may be negligible.
- However, an adversary can exploit this loophole to easily breach the security without being detected.

Exploitation of faults

- the attacker may need to bypass one or more modules in the biometric system to exploit such implementation faults.
- This attack is also closely linked to the obfuscation attack, because knowledge of the faults in the biometric implementation will allow the attacker to circumvent the system through appropriate alterations of his/her biometric trait.
- This attack can be prevented by using well-tested biometricalgorithms.

Attacks at the interconnections

- The following three attacks are possible when an adversary gains control of the communication interfaces between different modules of the biometric system.
- While the man-in-the-middle and replay attacks are common to the communication channel between any two modules in a biometric system, the hill-climbing attack is specific to the link between the sensor and feature extractor or the link between the feature extractor and matcher.

Man-in-the-middle attack

- In cryptography, a man-in-the-middle attack is a form of active eavesdropping, where the attacker establishes independent connections between two entities already in communication and relays messages between them.
- The victims are led to believe that they are directly communicating with each other, when in fact the entire conversation is controlled by the attacker.

Man-in-the-middle attack

- In biometric systems, a man-in-the-middle attack can be carried out against any two biometric modules and its effect is the same asa Trojan horse attack on a system module,
- i.e., it allows the attacker to inject false values into the biometric system.
- Mutual authentication between biometric modules is required to counter this attack.

Replay attack

- If the channels between the biometric modules are not secured physically or cryptographically, an adversary may intercept the data being transferred and replay it at a later time.
- The raw biometric data or extracted features can be intercepted and replayed.
- Replay attacks are possible even if the data is encrypted.
- A countermeasure against this attack is to use time-stamps or a challenge/responsemechanism.
- Mutual authentication between the modules and use of one-time session keys during every transaction could also mitigate replay attacks.

Hill climbing attack

- Hill-climbing attacks are possible
- when (a) the adversary has the ability to inject raw biometric sample data or features directly through a Trojan-horse attack or a man-in-the-middle attack, and
- (b) the attacker can obtain the match score output by the matcher (see Figure 7.11).
- Here, the goal of the attacker is to determine a biometric sample or feature set that matches with that of a targeted identity for the specified biometric algorithm.

- This leads to the hill-climbing attack, where an artificially generated biometric sample or feature set is first introduced into the system and the response (match score) is noted.
- The adversary then perturbs the initial sample or feature set, submits it to the system, and records the new match score.
- If the match score in the second iteration is higher than the first one, the changes are retained; else, they are discarded. The above process is iterated several times until the match score exceeds the threshold set by the system administrator.
- In each iteration where the match score is higher than before, the artificially generated sample or feature set becomes more similar to the template that is being targeted

- One can easily see that a hill-climbing attack is more difficult to implement than a Trojan horse or a man-in-the-middle attack.
- The reason for this difficulty is that not only access to match scores is needed, the attacker also needs to have some knowledge of the feature/sample distribution to synthetically generate features/samples in such a way that higher match scores can be obtained in the successive iterations.

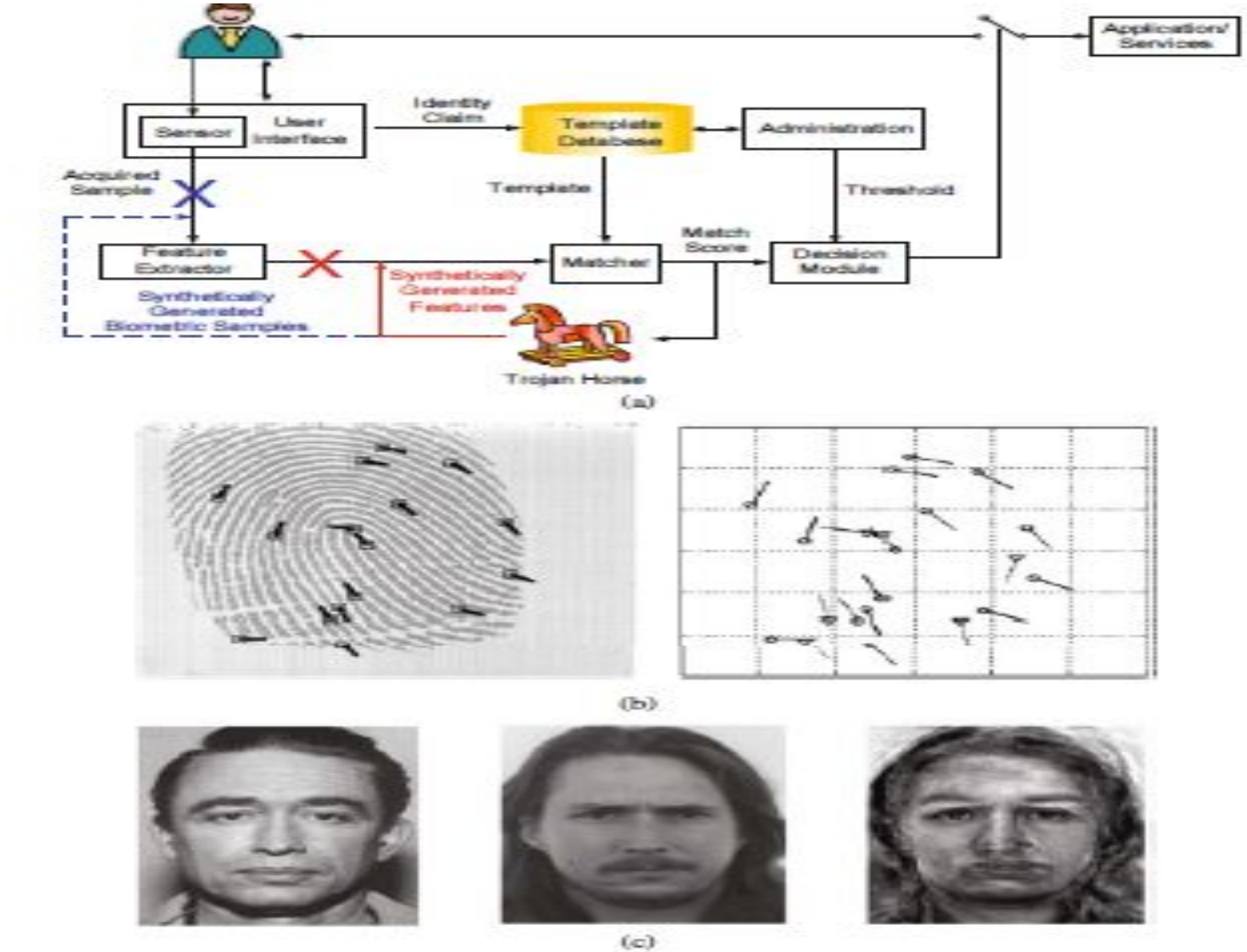


Fig. 7.11 (a) A hill climbing attack can be carried out both in the biometric sample space or in the feature space. Here, the goal of the attacker is to determine a biometric sample or feature set that matches with that of a target identity. Suppose that a Trojan horse replaces the feature extractor and injects synthetically generated features. The feedback obtained through the match score can be used to iteratively modify the synthetic features until a match is found. (b) Regenerated fingerprint minutiae (adapted from [47]). The target fingerprint with labeled minutiae is shown on the left and the minutiae positions learned using hill-climbing attack is shown on the right (solid lines with circle (–o) indicate the original minutiae, dotted lines with triangles (–V) indicate the synthetic minutiae.). (c) Regenerated face images (adapted from [1]). From left to right: the target face image, the initial selected image for hill-climbing, and the regenerated face image.

Attacks on the Template Database

- Two kinds of attacks are possible on the biometric template database

FIRST ATTACK

- First, the templatedatabase could be hacked or modified by an adversary to gain unauthorized access or to deny access to legitimate users.
- This unauthorized template modification can be carried out irrespective of the storage location, be it a central server, a remote client (e.g., personal computer, mobile phone, etc.), or a smart-card
- Similar attack is also possible in password-based authentication systems.
- The common technique used to mitigate such a threat is to have strict control on database access.

SECOND ATTACK

- Second, the stored biometric template information may become available to an adversary.
- Such an attack is referred to as leakage.
- Leakage is not a serious issue in password-based authentication, because only a cryptographic hash of the password is typically stored in the database, and the adversary gains no useful information from learning this hashed password.
- However, leakage is a serious problem in biometric systems

- There are four ways in which the biometric information of a user can be gleaned,namely, (a) collusion or coercion,
- (b) covert acquisition,
- (c) brute-force or hillclimbing attacks, and
- (d) template leakage.

- Among these four possibilities, the first two require the attacker to be in close physical proximity to the user or get the user's cooperation.
- The third method requires the attacker to breach the security of the biometric system and mount a successful intrusion attack. F
- The attacker needs to expend significant effort in the first three methods to acquire knowledge about a single user.
- In contrast, if an attacker can hack into a large biometric database, a task that can be done from a remote location while remaining anonymous, he can easily obtain the biometric information about a large number of users along with their biographic information (such as name, address, etc.).

- The leaked biometric information will lead to intrusion because the attacker can either reverse engineer the template to create a physical spoof or replay the stolen template to gain unauthorized access.

- leakage of biometric templates violates the data confidentiality requirement of a biometric system.
- unlike passwords and tokens, it is not possible to replace compromised biometric traits.
- Once the biometric information falls into the hands of an adversary, it is lost forever and cannot be reissued, updated, or destroyed.

- Thus, the irrevocable nature of biometric traits, which is one of the strengths of biometric recognition, can also be considered a weakness.
- leaked biometric templates can be used for secondary purposes like cross-matching across different databases to covertly track a person without his/her consent, thereby resulting in a function creep.
- leakage attack is not only a serious security threat, but also undermines the user's privacy.

Countermeasure: biometric template security

- The problem of biometric template security is quite similar to the problem of storing passwords securely, it is natural and intuitive to consider reusing the same techniques developed for password security in order to protect biometric templates.

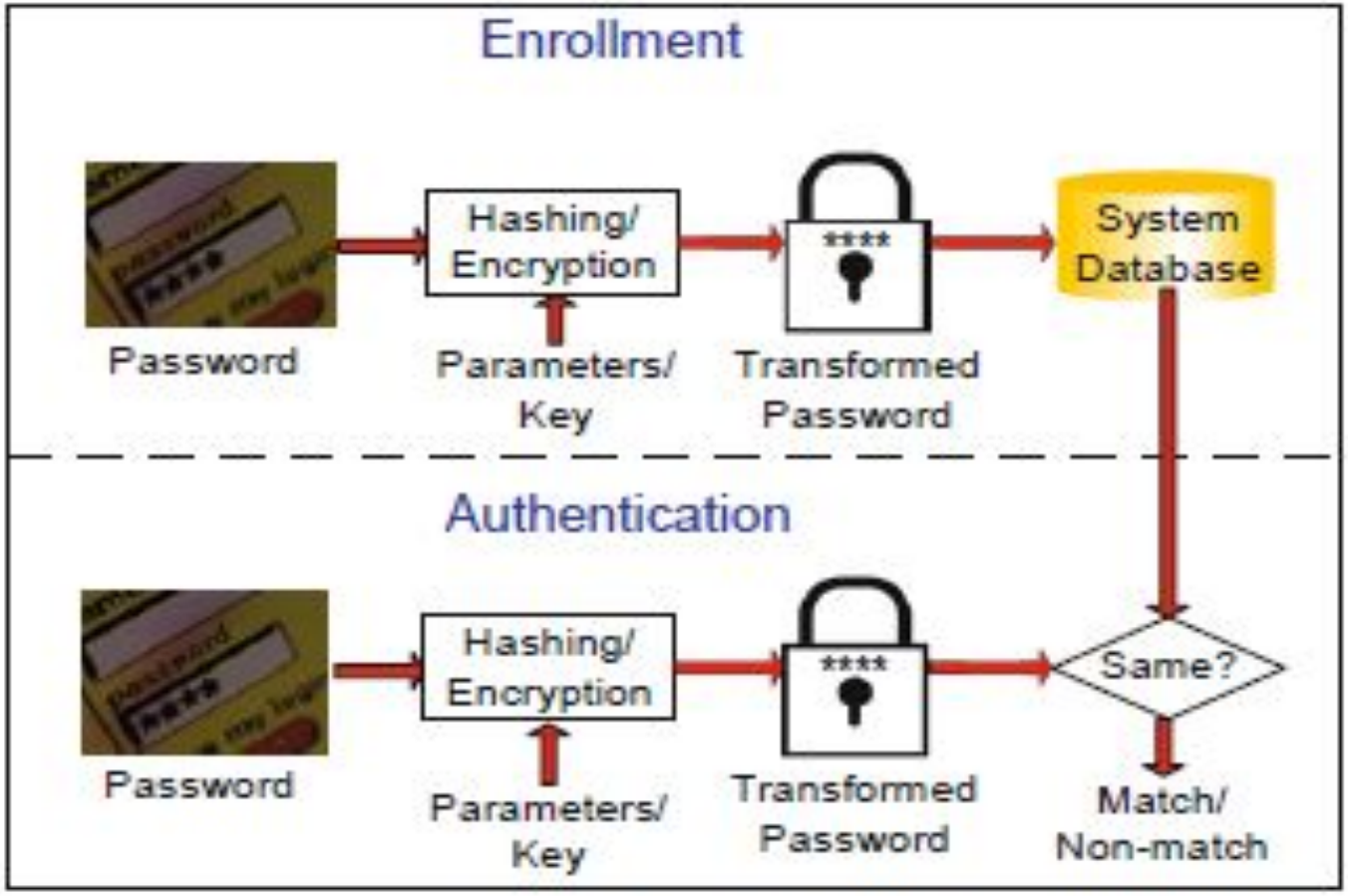
Techniques for securing passwords

- One possible approach for securing passwords is to encrypt them using well-known cryptographic techniques (e.g., Advanced Encryption Standard (AES), Rivest-Shamir- Adleman (RSA) algorithm, etc.) and store only the encrypted password.
- During authentication, the same encryption algorithm can be applied to the input password and directly matched to the stored encrypted password.

- Since an encrypted password can be decrypted if the decryption key is known, the security of encryption depends on the secrecy of the decryption key.
- It is well-known that key management (secure generation, distribution, and storage of cryptographic keys) is probably the most challenging issue in the practical implementation of cryptosystems.
- Even if the decryption key is held securely, an attacker can choose some arbitrary passwords and obtain the corresponding encrypted passwords

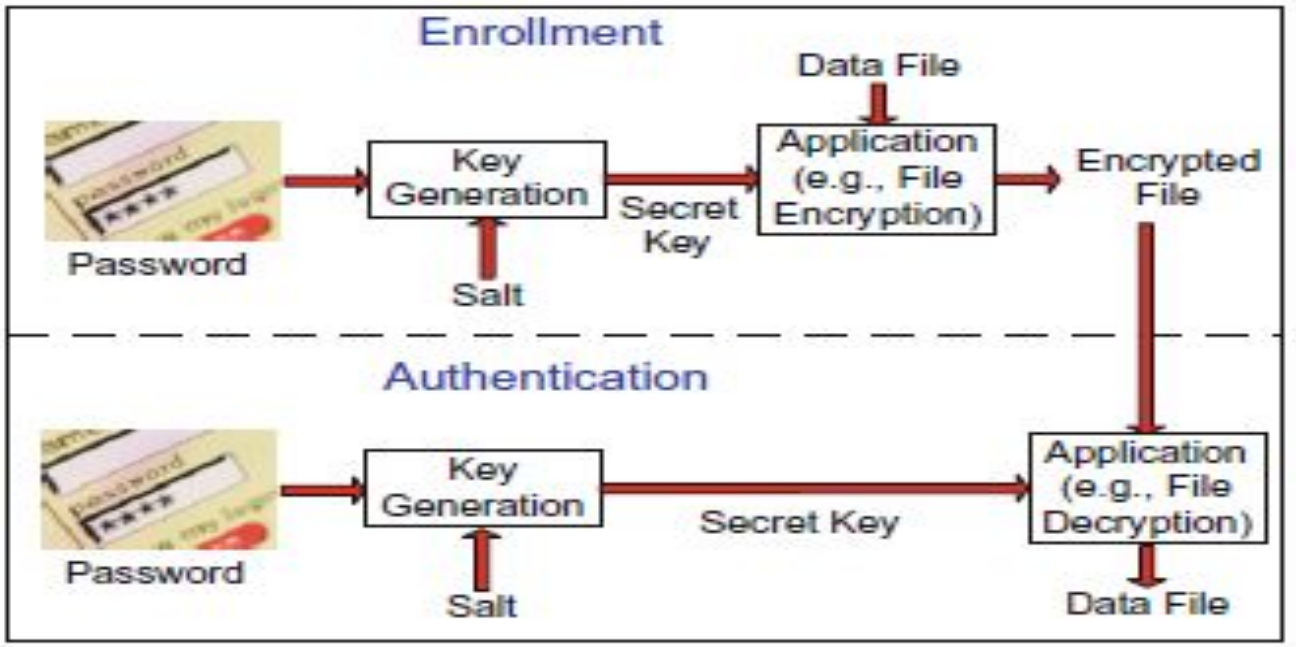
- The second alternative is referred to as password-based key generation.
- the password is never stored anywhere in the system.

Password encryption or hashing



(a)

Password based key Generation



(b)

Fig. 7.12 Approaches used for securing passwords. (a) In password encryption or hashing, only the encrypted password or a cryptographic hash of the password is stored in the database. While the encryption approach requires the decryption key to be held securely, the non-invertibility property of the cryptographic hash function protects the password even if the hash function and its parameters are available to the attacker. Hence, hashing is generally preferred to encryption in the context of password security. (b) In password-based key generation, the password is never stored anywhere in the system. Instead, the password is used to derive a cryptographic key usually in combination with additional random information known as a *salt*. This key generated from the password can be directly used in another application such as a file encryption system.

- The password is directly used to derive a cryptographic key usually in combination with additional random information known as a *salt*.
- Another application such as a file encryption system can directly use the key derived from the password for symmetric key cryptography.
- While this approach is beneficial in the sense that the password need not be stored anywhere, it can be used only in applications where the authentication is implicit. For instance, one can decrypt an encrypted file and read its contents only if the right password is presented.

THIRD APPROACH

- The third approach used in most modern password-based authentication systems is to apply a cryptographic hash function to the plaintext password and store only the hashed password.
- When the user enters the password during authentication, the same hash function is applied to the input password and the resulting hash value is directly matched with the stored hash value

CRYPTOGRAHIC HASH FUNCTION

1. *Pre-image resistance*: Given a cryptographically hashed password, say $\mathbf{h}(\mathbf{x})$, it must be computationally hard to find a password $\mathbf{y}$ such that $\mathbf{h}(\mathbf{y}) = \mathbf{h}(\mathbf{x})$.
2. *Weak collision resistance*: Given $\mathbf{x}$ and $\mathbf{h}(\mathbf{x})$, it must be computationally hard to find $\mathbf{y}$, where $\mathbf{y} \neq \mathbf{x}$, such that $\mathbf{h}(\mathbf{y}) = \mathbf{h}(\mathbf{x})$, and
3. *Collision resistance*: It must be computationally difficult to find some arbitrary $\mathbf{x}$ and $\mathbf{y}$, such that $\mathbf{x} \neq \mathbf{y}$, but $\mathbf{h}(\mathbf{x}) = \mathbf{h}(\mathbf{y})$. In other words, it is difficult to find two different passwords that result in the same cryptographic hash. Note that weak collision resistance does not imply collision resistance.

Due to the above properties of the hash function, even if the stored (hashed) password becomes available to an adversary, it does not result in a serious security threat.

Challenges and requirements in biometric template security

- password-based authentication relies on an exact match between the passwords entered during enrollment and authentication, biometric recognition is based on inexact match between the enrollment and authentication samples.

- There can be large intra-user variability in multiple acquisitions of the same biometric trait and handling these intra-user variations is the most important challenge in designing a biometric template protection scheme

- The term “protected” or “secure” template will be used to refer to those templates that are obtained after the application of a biometric template security algorithm to the “unprotected” or “original” template.

THREE PROPERTIES OF TEMPLATE

- A biometric template protection scheme should have the following three properties.
- **Cryptographic security**
- **Performance**
- **Revocability**

- **Cryptographic security**
- Cryptographic security refers to the pre-image resistance property that is typically satisfied by cryptographic hash functions.
- The concept of pre-image resistance is also related to *one-way* or *noninvertible* mathematical functions.
- A function **f** is referred to as a one-way function if it is “easy to compute” (in polynomial time) but “hard to invert” (given **f**(**x**), the probability of finding **x** in polynomial-time is small)

- A non-invertible template protection scheme implies that it will be computationally hard to obtain the original biometric features from the secure template.
- This prevents an adversary from creating a physical spoof of the biometric trait and intruding another biometric system that makes use of the same biometric trait.
- Thus, a secure template must be pre-image resistant and non-invertible.

- **Performance**: The biometric template protection scheme should not degrade the recognition performance (FMR and FNMR) of the biometric system.

- **Revocability**: It is desirable to have a template protection scheme that can generate multiple secure templates from the same biometric data.
- These multiple secure templates must be such that even if an adversary obtains two or more of them, it must be computationally hard to
- (a) identify that they are derived from the same biometric data and
- (b) obtain the original biometric features of the user.

- This revocability or cancelability property ensures that cross-matching across biometric databases is not possible, thereby preserving the user's privacy.
- Revocability also makes it straightforward to discard a compromised template and reissue a new one based on the same biometric data.
- the template protection scheme should satisfy all the three requirements at the same time

DIFFERENT APPROACHES FOR TEMPLATE PROTECTION

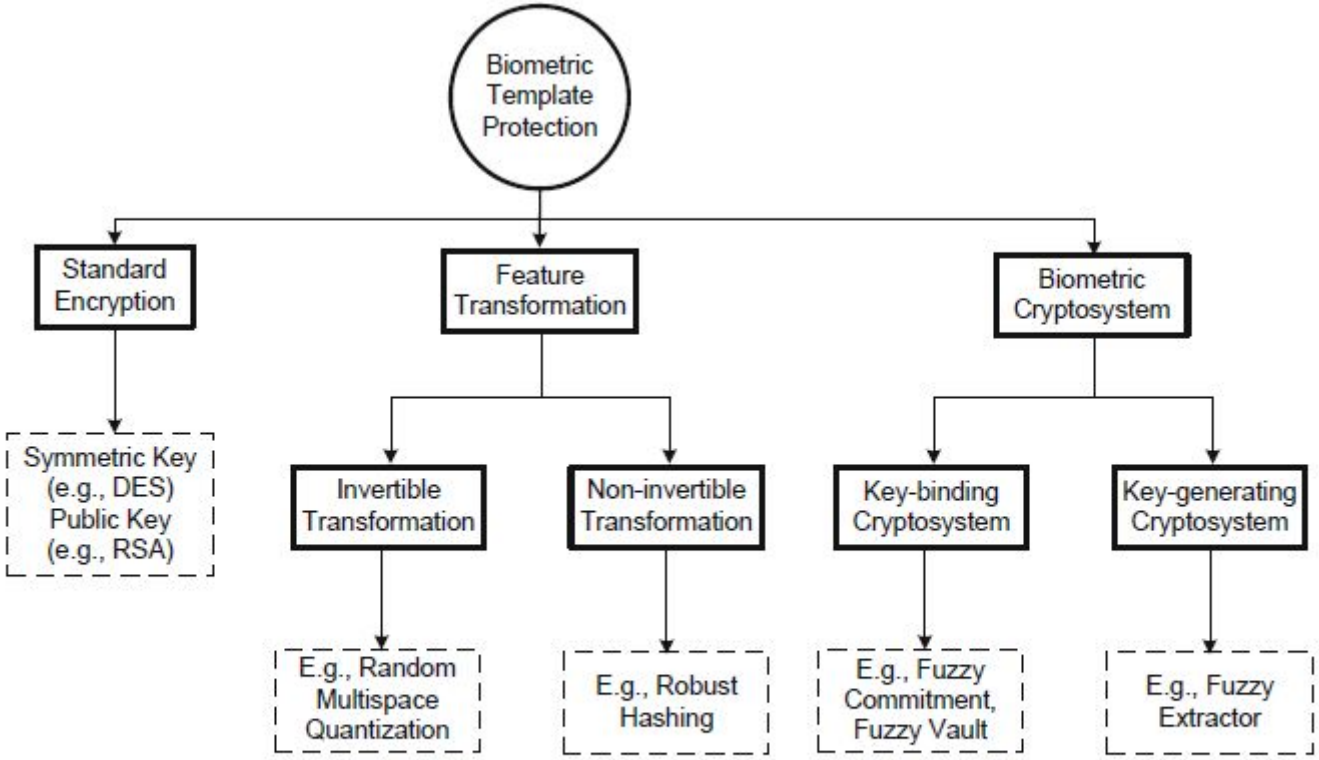


Fig. 7.13 Different approaches for securing biometric templates.

Standard encryption

- multiple acquisitions of the same biometric trait do not result in the same feature set. Typically,
- standard encryption functions are not smooth functions and a small difference in the values of the feature sets extracted from the raw biometric data would lead to very large difference in the resulting encrypted features (see Figure 7.16)

Standard encryption

- The main advantage of the standard encryption approach is that the recognition performance of the biometric system is not affected at all.
- Since the matching actually takes place in the decrypted domain, there is no need to re-design or modify the available matching algorithms

Standard encryption

- However, it must be emphasized the encryption solution is secure and revocable only under ideal conditions (key is kept secret and matching is done at a trusted location).
- If practical issues such as key management or susceptibility to template theft during a matching attempt are taken into account, the standard encryption technique is not good enough for securing biometric templates.

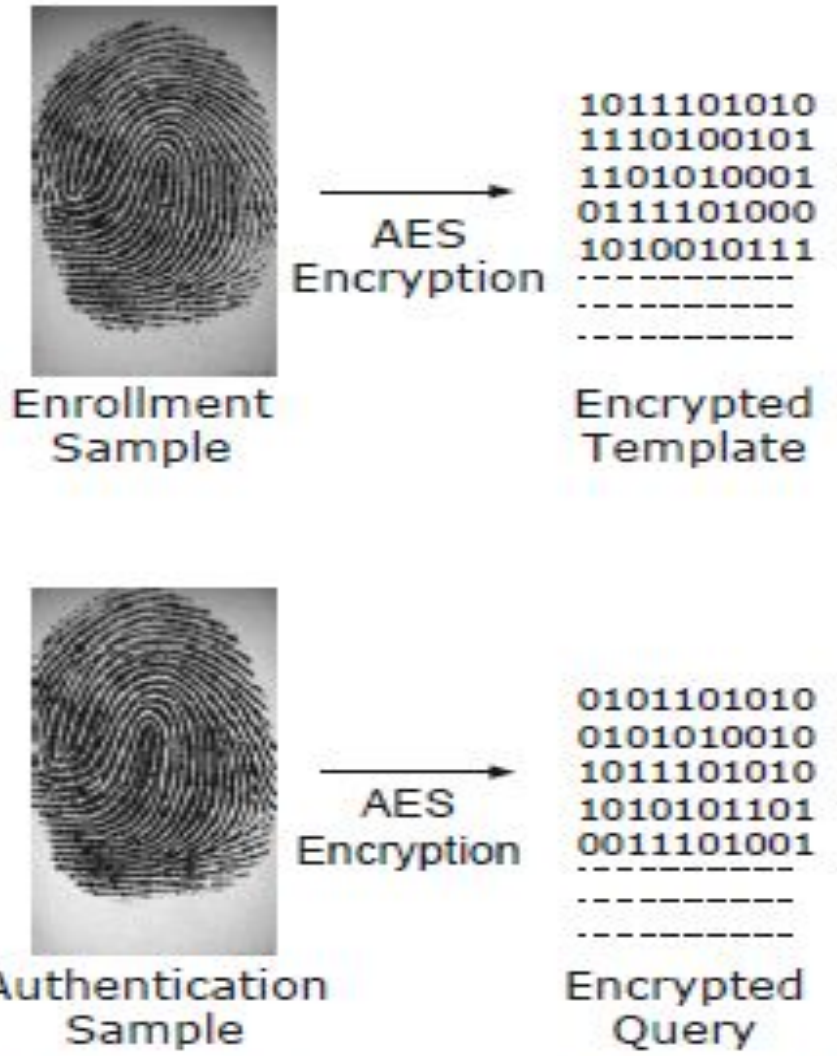


Fig. 7.16 Illustration of the large difference in the encrypted template and encrypted query when features extracted from multiple impressions of the same fingerprint are encrypted using standard encryption techniques (e.g., AES, RSA).

feature transformation approach and *biometric cryptosystem*

- To overcome this problem, a number of techniques have been proposed, which are specifically designed for biometric template security, keeping in mind the unique characteristics of this domain such as intra-user variations.
- These techniques can be roughly classified as *feature transformation* approach and *biometric cryptosystem*.

hybrid biometric cryptosystem.

- When a template security scheme clearly involves elements from both the basic approaches, (*feature transformation* approach and *biometric cryptosystem*)it is referred to as a *hybrid biometric cryptosystem*.

Standard encryption

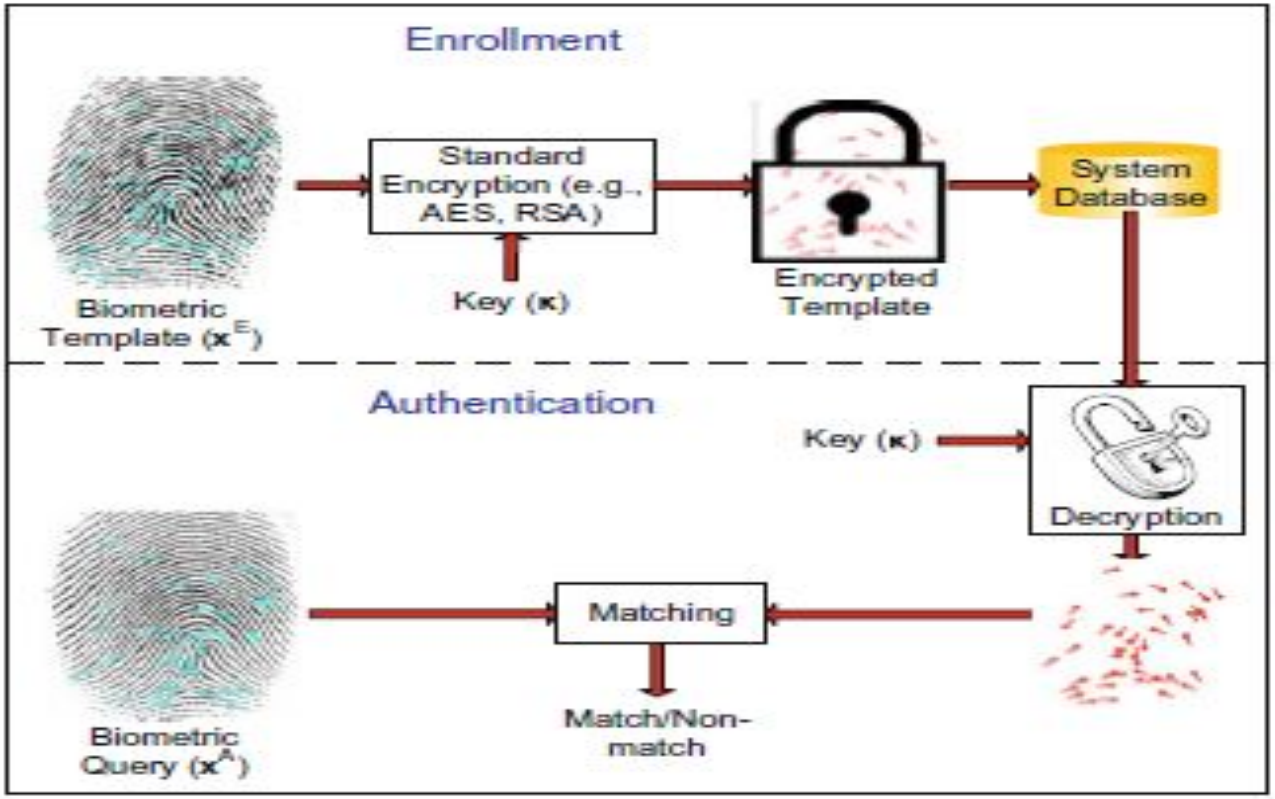


Fig. 7.15 Securing biometric templates through standard encryption techniques. Unlike password encryption, biometric matching cannot be performed in the encrypted domain because of intra-user variations in the biometric data. Since encryption is simple and does not affect the recognition performance, it is widely used in many existing biometric systems. However, the template is secure only if the cryptographic key (κ) is maintained a secret and matching takes place in a trusted environment.

Fingerprint

(a)

Minutiae

x

(b)

1011101010
1110100101
1101010001
0111101000
1010010111
- - - - - - - -
- - - - - - - -
- - - - - - - -

Encrypted Template
E(**x**,κ)

(c)

Transformed Template
f(**x**,κ)

(d)

Fuzzy Vault
f(**x**,κ)

(e)

Fig. 7.14 An illustration of different template protection approaches when applied to a fingerprint minutiae template. (a) Fingerprint sample acquired during enrollment, (b) minutiae template extracted from the enrollment sample, (c) a fingerprint template encrypted using a standard encryption algorithm such as AES, (d) a transformed minutiae template obtained using a non-invertible transformation scheme, and (e) a fuzzy vault (biometric cryptosystem) that hides the minutiae template among a large set of random chaff points.

Feature transformation approach

In the feature transform approach, a transformation function $f(.)$ is applied to the biometric template x^E and only the transformed template $f(x^E, \kappa)$ is stored in the database. The parameters of the transformation function are typically derived from a random key, κ, or password. The same transformation function is applied to query features, x^A, and the transformed query, $f(x^A, \kappa)$, is directly matched against the transformed template, $f(x^E, \kappa)$. From Figure 7.17, one can clearly see that the feature transformation approach is analogous to password encryption or hashing.

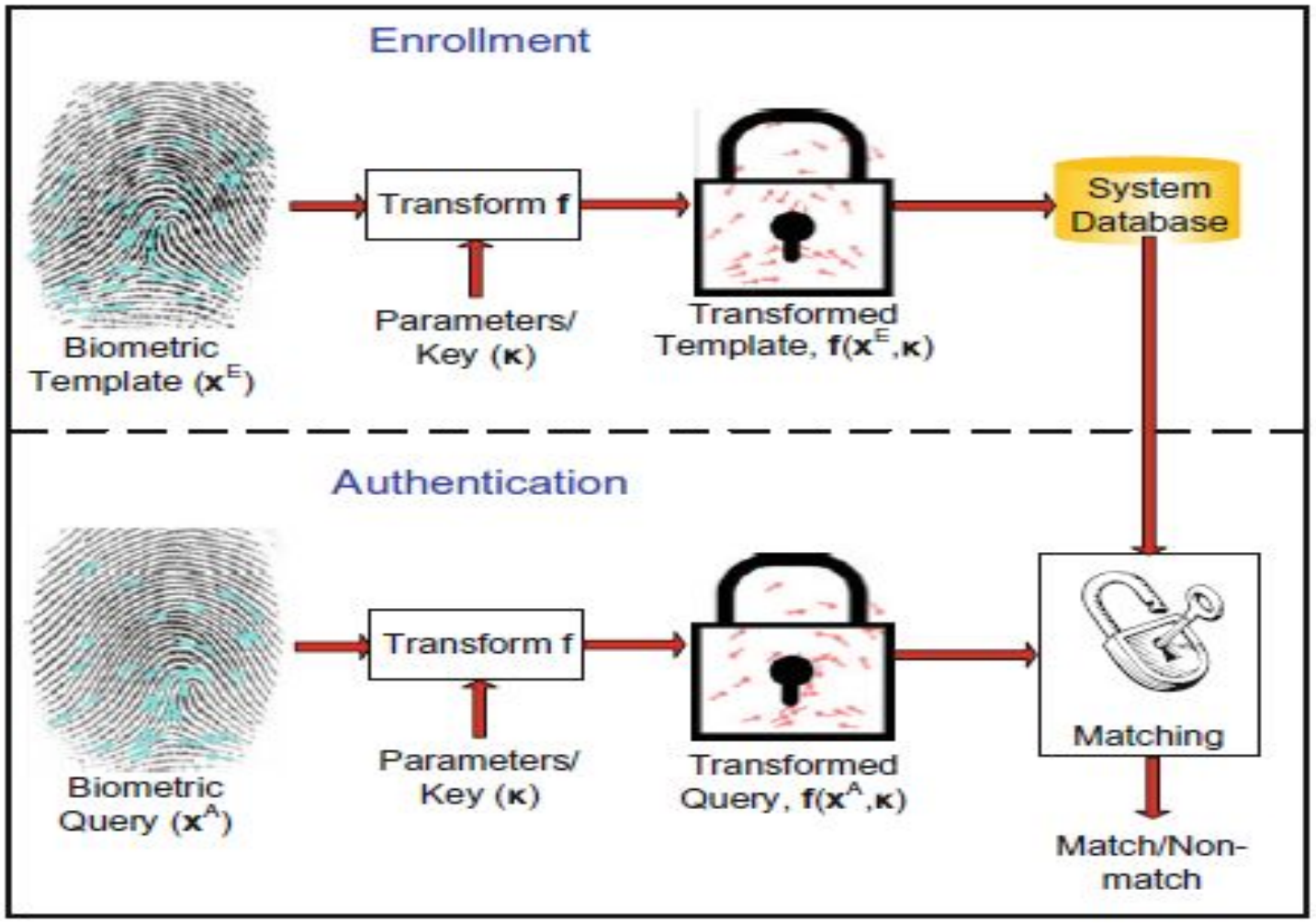


Fig. 7.17 Securing biometric templates using the feature transformation approach. The cryptographic security of the template depends on the characteristics of the transformation function, $\mathbf{f}(.)$. If the transform is invertible, the template is secure only if the key κ is maintained secretly. On the other hand, a template obtained through non-invertible transformation is usually secure, even if the parameters of the transformation are known.

FEATURE TRANSFORM

- The feature transform schemes can be further categorized as
- *invertible*
- *non-invertible* transforms

Invertible transformation

- When the transformation function, **f**(.), is invertible[2], the security of the transformed template is based on the secrecy of the key κ .
- In other words, if an adversary gains access to the key and the transformed template, he can recover the original biometric template (or a close approximation of it).
- Thus, a template protected using the invertible feature transformation approach is similar to an encrypted password.

- A well-known example of invertible feature transformation approach is the random multi-space quantization technique (see Figure 7.18). This scheme can be used to transform a fixed-length (and typically real-valued) biometric feature vector.

Random multispace quantization

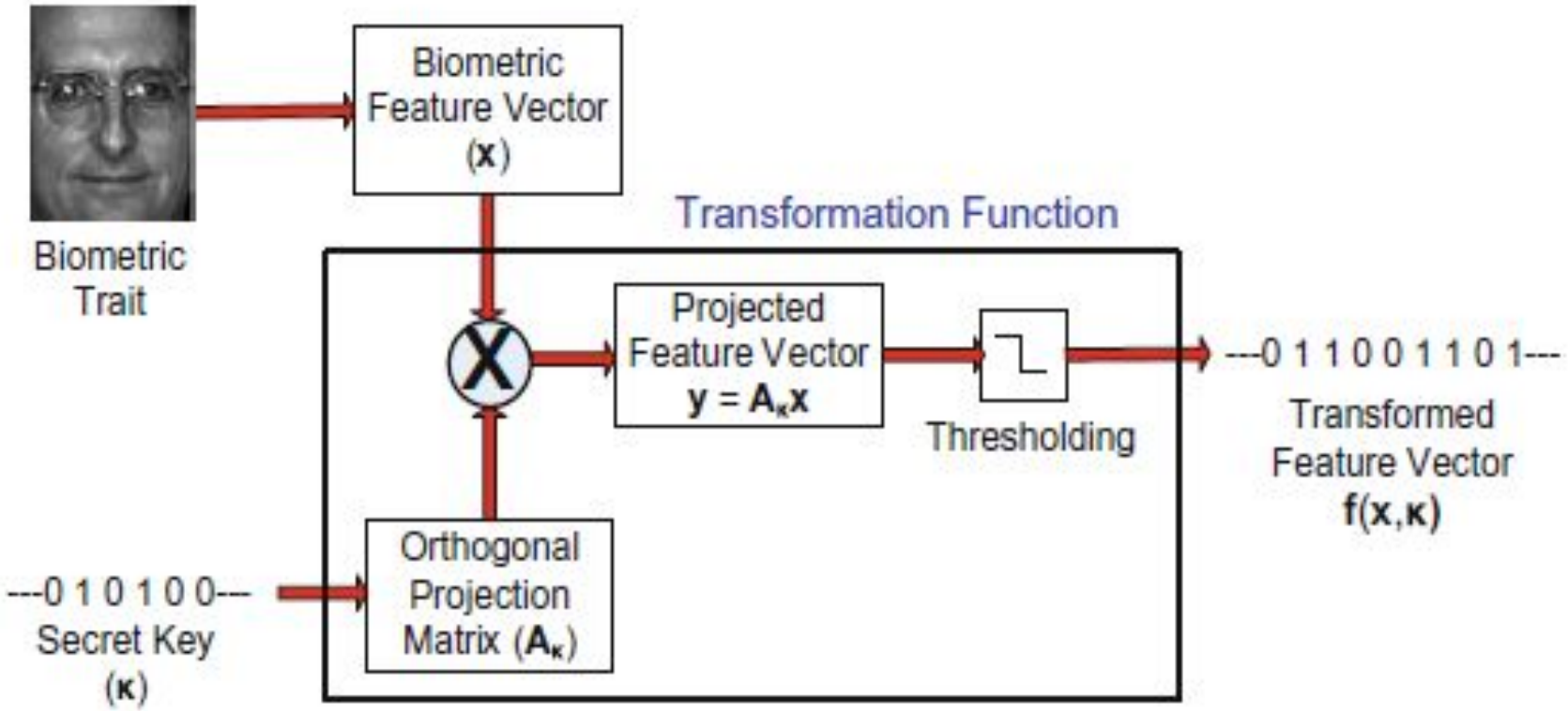


Fig. 7.18 Securing biometric templates using the random multispace quantization technique.

- The security in this scheme is provided by the user-specific random projection matrix $\mathbf{A}_K$.
- If an adversary gains access to this matrix, then the scheme is neither pre-image resistant nor non-invertible.
- Even though the matrix $\mathbf{A}_K$ does not have an exact inverse because its rank is less than *d*, one can easily obtain a pre-image by computing the pseudo-inverse of $\mathbf{A}_K$.
- Further, it may also be possible to recover a close approximation of the original biometric features (some information is lost due to binarization) through a hill-climbing attack.
- Finally, an attack similar to the chosen plaintext attack may be used to recover the random projection matrix directly.

Non-invertible transformation:

- Non-invertible transformation schemes typically apply a one-way function on the template, and it is computationally hard to invert a transformed template even if the key is known.
- Ideally, one should employ a transformation function that is both pre-image resistant and non-invertible.
- If such a transform can be applied, then non-invertible transformation is equivalent to a password hashing scheme.
- Since it is hard to recover the original biometric template even when the parameters of the transformation are compromised, this scheme provides better security than the invertible transformation approach.
- By selecting user-specific transform parameters, this approach can also allow revocability

- The main drawback of this approach is the trade-off between discriminability (recognition performance) and non-invertibility (security) of the transformation function.
- The transformation function should preserve the discriminability (similarity structure) of the feature set, i.e., just like in the original feature space, features from the same user should have high similarity in the transformed space and features from different users should be quite dissimilar after transformation.
- On the other hand, the transformation should also be non-invertible, i.e., given a transformed feature set, it should be hard for an adversary to obtain the original feature set (or a close approximation of it). It is difficult to design transformation functions that satisfy both the discriminability and non-invertibility conditions simultaneously.
- one needs to choose an appropriate transformation function based on the characteristics of the biometric features employed in a specific application.

- Examples of non-invertible functions that have been proposed for the purpose of transforming fingerprint minutiae include cartesian, polar, and functional transformations.
- In cartesian transformation, the minutiae space (fingerprint image) is tessellated into a rectangular grid and each cell (possibly containing some minutiae) is shifted to a new position in the grid corresponding to the translations set by the key κ .
- The polar transformation is similar to cartesian transformation with the difference that the image is now tessellated into a number of concentric shells and each shell is divided into sectors.

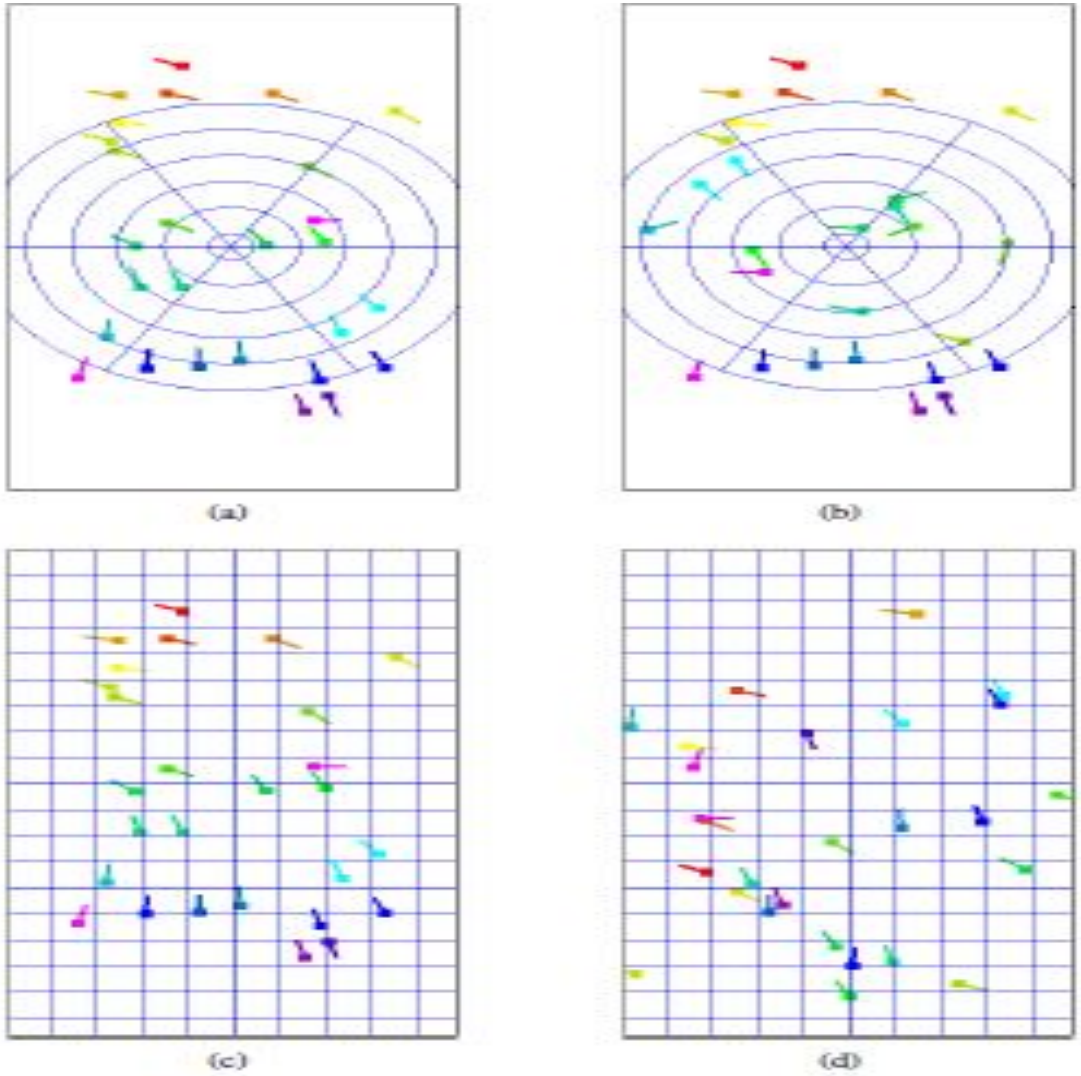


Fig. 7.19 Illustration of cartesian and polar transformation functions for generating cancelable fingerprint templates (adapted from [22]). (a) Original minutiae on radial grid, (b) transformed minutiae after polar transformation, (c) original minutiae on rectangular grid, and (d) transformed minutiae after cartesian transformation. Note that the minutiae are shaded differently to track them after transformation.

Biometric cryptosystems

- Biometric cryptosystems are somewhat similar to password-based key generation systems because they were originally developed for the purpose of either securing a cryptographic key using biometric features or directly generating a cryptographic key from biometric features.
- Since the biometric features available during enrollment and authentication are different, these features cannot be directly used for generation of cryptographic keys.
- In order to facilitate key generation, some public information about the biometric features is stored in the database during enrollment.
- This public information is usually referred to as *helper data* or *secure sketch* and hence, biometric cryptosystems are also known as helper-data-based methods.
- The secure sketch is used during authentication to extract a cryptographic key from the query biometric features through a process known as the recovery mechanism.
- Matching is performed indirectly by verifying the validity of the extracted key or by directly using the key in another application.

Key binding and key generation

- Biometric cryptosystems can be further classified as *key binding* and *key generation* systems depending on how the secure sketch is obtained.
- When the secure sketch is obtained by binding a cryptographic key (that is independent of the biometric features) with the biometric template, it is referred to as a *key binding biometric cryptosystem.*
- If the helper data is derived only from the biometric template and the cryptographic key is directly generated from the helper data and the query biometric features, it leads to a *key generation biometric cryptosystem*

- Thus, biometric cryptosystems solve the challenging problems of cryptographic key management and biometric template protection simultaneously.
- Due to this reason, this topic is under active research in both the biometric and cryptographic communities.

Key binding cryptosystem

- key binding cryptosystem, the biometric template is secured by monolithically binding it with a secret key within a cryptographic framework. As shown in Figure 7.20,
- a single entity that embeds both the key and the template is stored in the database as the secure sketch.
- This secure sketch does not reveal much information about the key or the biometric template, i.e., it is computationally hard to decode the key or the template without any knowledge of the user's biometric data.
- Matching in a key binding system involves recovery of the key from the helper data using the query biometric features and verifying the validity of the key.

Key binding

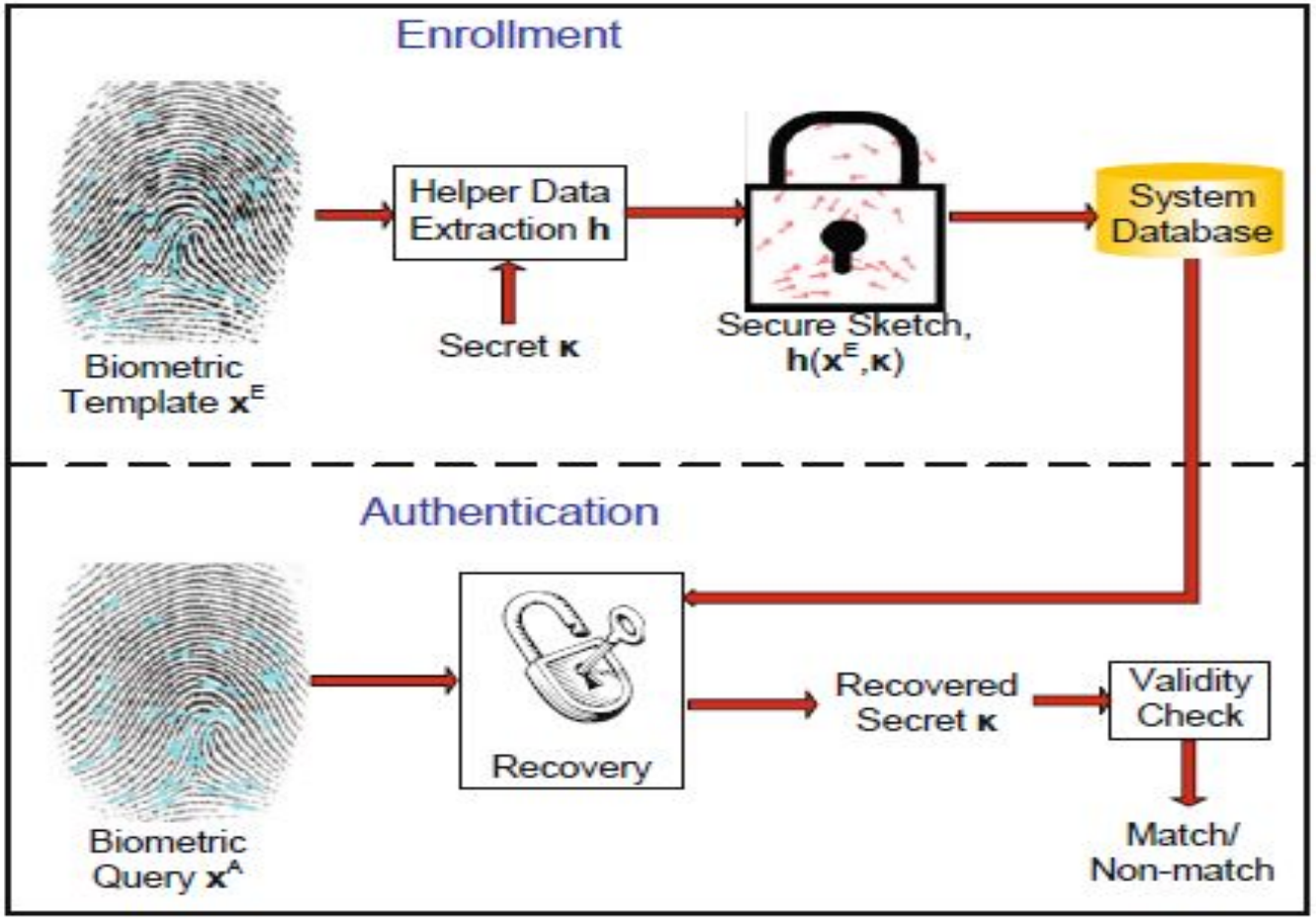


Fig. 7.20 Authentication mechanism when the biometric template is secured using a key binding biometric cryptosystem.

Fuzzy commitment scheme

- One of the earliest and most well-known key binding biometric cryptosystems is the fuzzy commitment scheme.
- Suppose that the enrollment template $\mathbf{x}^E$ is a binary string of length *d* bits. During enrollment, an error correcting codeword **c** of the same length (*d* bits) is selected.
- This codeword is uniquely indexed by a secret key κ of length *m* bits (there is a one-to-one correspondence between **c** and κ). Here, *m* is less than *d* and the parameter (*d* −*m*) is a measure of the redundancy in the error-correction code.
- The codeword **c** is then committed (bound) to the biometric feature vector **x***E* to generate the secure sketch.
- The secure sketch or helper data consists of the fuzzy commitment ($\mathbf{x}^E \oplus \mathbf{c}$) and **g**(κ), where **g**(.) is a cryptographic hash function and $\oplus$ represents exclusive-or (XOR) operation (modulo-2 addition).

During authentication, the user presents a biometric vector x^A. Now one can compute the codeword with errors, c', as $c' = x^A \oplus (x^E \oplus c)$. If x^A is close to x^E, c' is close to c since $x^A \oplus x^E = c' \oplus c$. Therefore, c' can now be decoded to obtain the nearest codeword c^*, which would be equal to c provided that the distance between c and c' is less than the error correcting capacity of the code. From c^*, one can compute κ^*. The matching is successful if $g(\kappa^*) = g(\kappa)$.

Key generating biometric cryptosystem:

- Direct cryptographic key generation from biometrics is an attractive proposition, but it is a difficult problem because of two reasons:

(a) the intra-user variability of the biometric features, and

(b) the non-uniform nature of the probability distribution of biometric features.

The concept of secure sketch or helper data can be used to solve the first issue.

In this scenario, the secure sketch is derived using only

- the biometric template and the recovery mechanism facilitates exact reconstruction of the template when presented with a query that is close to the template as illustrated in Figure 7.21.

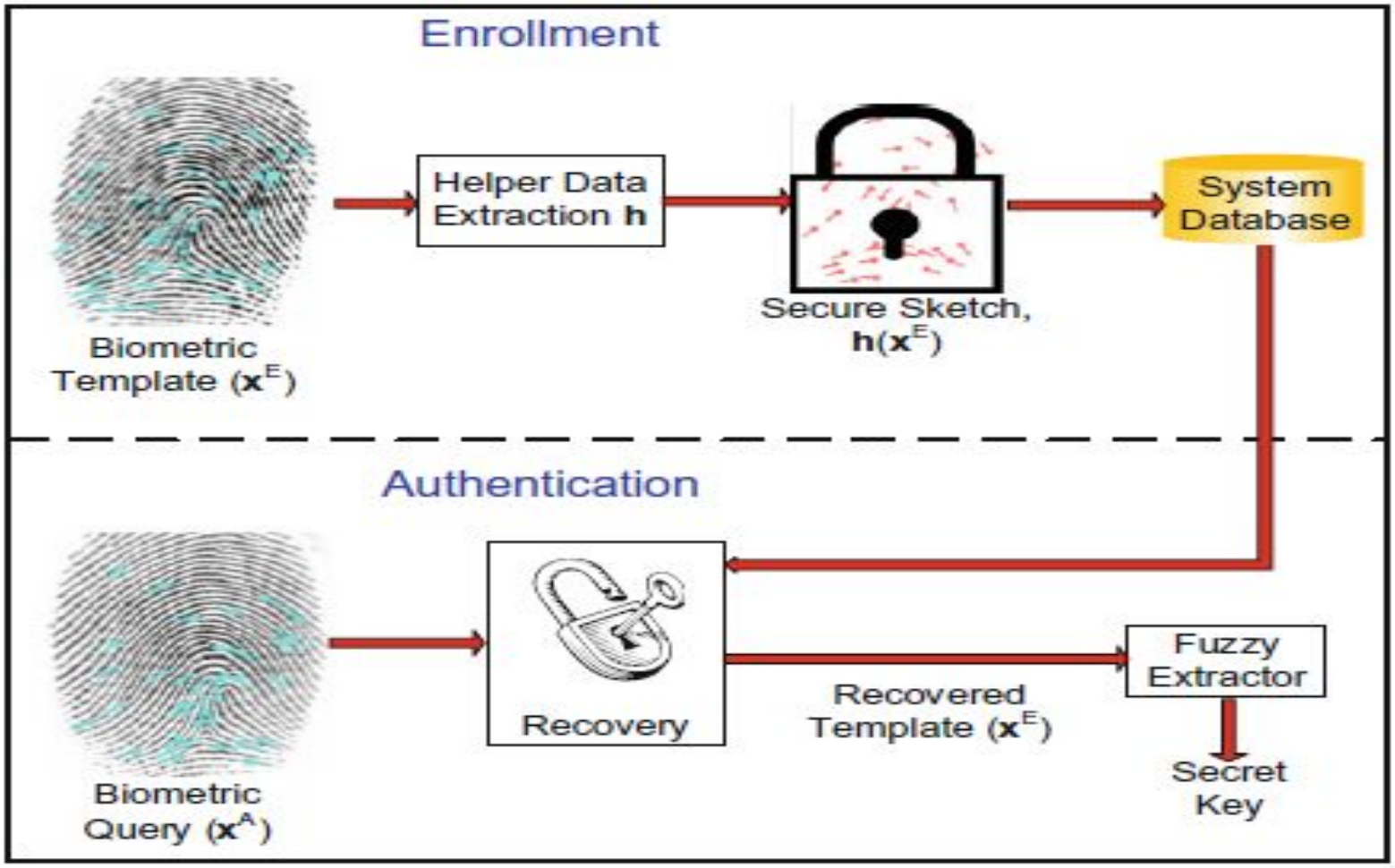


Fig. 7.21 Authentication mechanism when the biometric template is secured using a key generating biometric cryptosystem.

- Early biometric key generation schemes employed user specific quantization schemes.
- Information on quantization boundaries is stored as helper data, which is used during authentication to account for intra-user variations.
- It is also possible to make use of error correction coding schemes to generate the secure sketch from the biometric features.

Table 7.1 Summary of different template protection schemes. Here, $\mathbf{x}^E$ represents the biometric template, $\mathbf{x}^A$ represents the query presented during authentication, and κ is the key (or parameters) used to protect the template or is generated from the template. In feature transformation approach, $\mathbf{f}$ represents the transformation function and m_t represents the matcher that operates in the transformed domain. In biometric cryptosystems, $\mathbf{h}$ is the helper data extraction scheme and $\mathbf{m}$ is the error correction recovery mechanism that allows reconstruction of the key κ.

Approach	Security Feature	Entities Stored	Mechanism to handle Intra-user variations
Invertible transform	Secrecy of key κ	Public domain: Transformed template $\mathbf{f}(\mathbf{x}^E, \kappa)$ Secret: Key κ	Quantization and matching in transformed domain $m_t(\mathbf{f}(\mathbf{x}^E, \kappa), \mathbf{f}(\mathbf{x}^A, \kappa))$
Non-invertible transform	Non-invertibility of the transformation function $\mathbf{f}$	Public domain: Transformed template $\mathbf{f}(\mathbf{x}^E; K)$, key κ	Matching in transformed domain $m_t(\mathbf{f}(\mathbf{x}^E; K), \mathbf{f}(\mathbf{x}^A, \kappa))$
Key-binding biometric cryptosystem	Level of security depends on the amount of information revealed by the helper data H	Public domain: Helper Data $H = \mathbf{h}(\mathbf{x}^E, \kappa)$	Error correction and user specific quantization $\kappa = \mathbf{m}(\mathbf{f}(\mathbf{x}^E, \kappa), \mathbf{x}^A)$
Key-generating biometric cryptosystem	Level of security depends on the amount of information revealed by the helper data H	Public domain: Helper Data $H = \mathbf{h}(\mathbf{x}^E)$	Error correction and user specific quantization $\kappa = \mathbf{m}(\mathbf{h}(\mathbf{x}^E), \mathbf{x}^A)$