# Biometric security

- Biometric security measure (or security countermeasure) is a technological or procedural system designed to protect a biometric system from active attack (Biometric security threat).
- Examples of security measures include: liveness detection which is designed to detect spoof biometric samples; and cancelable biometrics and biometric encryption which are designed to protect against attacks on Biometric template security.

# Biometric Security Threat

- Biometric Security Threat is an approach of active attack against vulnerability in a biometric system.
- Threats may be broadly classified as:
  - Presentation attacks (spoofing), in which the appearance of the biometric sample is physically changed or replaced;
  - Biometric processing attacks, in which an understanding of the biometric algorithm is used to cause incorrect processing and decisions;
  - Software and networking vulnerabilities, based on attacks against the computer and networks on which the biometric systems run;
  - Social and presentation attacks, in which the authorities using the systems are fooled.
- To defend against a biometric security threat, a biometric security measure may be used.

# Securing Fingerprint Recognition Systems

Fingerprint recognition systems are security systems and as such they are not foolproof. Despite numerous advantages, fingerprint systems are vulnerable to security breaches and attacks. The system vulnerability depends on the threat model of an application which will use the fingerprint recognition system. The typical threats in a fingerprint recognition system are as follows:

- *Denial-of-service: an adversary can damage the system to cause a denial-of-service to* all the system users.

# Securing Fingerprint Recognition Systems

- *Circumvention or intrusion: an unauthorized user can illegitimately gain access into* the system
- *Function creep: a wrongful acquisition or use of fingerprint data for a purpose other* than intended.
- *Repudiation: a legitimate user may deny having accessed the system.*

# Securing Fingerprint Recognition Systems

- The security issues ensure that the intruders will neither be able to access the individual information/measurements (e.g., obtain user fingerprint information from the database, insert spurious new fingerprints into the database) nor be able to pose as other individuals by electronically interjecting (“replay attack”) stale and fraudulently obtained biometrics measurements (e.g., surreptitiously lifted fingerprints from surfaces touched by the individuals, fingerprint information tapped from a communication channel) into the system.

# Securing Fingerprint Recognition Systems

- The access protection may sometimes involve physical protection of the data or detection of the fraudulent physical access to the data (e.g., tamperproof enclosures).
- When the system and/or its communication channels are vulnerable to open physical access, cryptographic methods should be employed to protect the biometric information[2].

# Securing Fingerprint Recognition Systems

A typical approach to protecting biometric information:

- Encrypting fingerprint data using various standard cryptographic mechanisms.
- Invisible watermarking of fingerprint images may assure the database administrators that all the images in the database are authentic and are not tampered with by an intruder.

# Securing Fingerprint Recognition Systems

- Typical approaches to resist “replay” attacks also follow mainstream cryptographic strategies, which rely on introducing (encrypted) time/session sensitive challenge response mechanisms to authenticate the source/destination of the encrypted transmission.

# Securing Fingerprint Recognition Systems

- One of the measures is that of checking whether the source of the input signal is a live genuine biometric (finger) and distinguishing it from a signal originating from a fraud (e.g., tight-fitting latex glove having impression of the genuine finger). The premise of a liveness test is that if the finger (surface) is live, the impression made by it represents the person to whom the finger belongs.

# Spoofing

- Spoofing is the use of an artifact containing a copy of the biometric characteristics of a legitimate enrolee to fool a biometric system. Examples include: gummy fingers, photograph of a face or iris pattern, artificial hand, etc., depending on the modality of the biometric characteristic.
- Mimicry is imitating someone else's behavior to fool a biometric system that uses human behavior rather than biology as a distinguishing characteristic.
- Examples include signature and voice recognition. Disguise is concealing biometric characteristics to avoid recognition. It can apply to biological and behavioral characteristics and may or may not involve the use of artifacts.

# Spoofing

- Biometric spoofing is a method of attacking biometric systems where an artificial object is presented to the biometric sample acquisition system that imitates the biological properties the system is designed to measure, so that the system will not be able to distinguish the artifact from the real biological target.

# Anti-spoofing

- A biometric spoof is an artificial mimic of a real biometric. Anti-spoofing is a technical measure against biometric spoofing. Liveness detection is one of such techniques.
- ▶Biometric Liveness
- ▶Biometric Spoofing Prevention(encryption)
- ▶Liveness Detection: Fingerprint
- ▶Liveness Detection: Iris

# Spoof Attack Detection Based on Fingerprint Odor Analysis

- As with any other security system, biometric systems are not totally spoofproof[3].
- Recently some studies demonstrated the concrete possibility of fooling commercial recognition systems by presenting artificial biometric samples such as a fake fingerprint, an artificial iris, or a facemask.

# Spoof Attack Detection Based on Fingerprint Odor Analysis

Following are methods able to discriminate a real and live fingerprint from a fake or deceased one.

- **Analysis of skin details:**
  - Acquiring a fingerprint image at a very high resolution (about 1000 dpi) allows the observation of certain fingerprint details, such as the sweat pores or the surface coarseness that are very difficult to reproduce artificially.

# Spoof Attack Detection Based on Fingerprint Odor Analysis

- **Analysis of static properties of the finger:**
  - The use of specialized hardware allows the capture of life signs such as temperature impedance or other electric properties.
  - In spectroscopy-based techniques the spectrum reflected by the skin when exposed to multiple wavelengths of light is analyzed, the response is usually quite different for human tissues and artificial materials.

# Spoof Attack Detection Based on Fingerprint Odor Analysis

- **Analysis of dynamic properties of the finger:**
  - These methods are based on the analysis of life signs such as skin perspiration, pulse oximetry, blood pressure, or skin elasticity.
  - Skin perspiration is one of the most studied phenomena for aliveness detection

# Spoof Attack Detection Based on Electronic Odor Analysis

- Every substance or material that exhales an odor constantly evaporates tiny quantities of molecules called odorants which can be detected by chemical sensors.
- An electronic nose is an array of chemical sensors designed to detect several complex odors and to measure their intensity thus producing the characteristic pattern of an odor.

# Spoof Attack Detection Based on Electronic Odor Analysis

The acquisition of an odor pattern consists of sampling the data coming from an odor sensor during a given time interval, usually a few seconds. A typical **acquisition session is composed of three different phases**.

- **Calibration**
  Performed when the system is idle in order to establish a baseline signal, referred to as “response in fresh air”, that represents the sensor response when no fingers are placed on the sensor surface.

# Spoof Attack Detection Based on Electronic Odor Analysis

- **Recording**
  That consists of the registration of the sensor response in the presence of a finger. In order to measure such response, the user has to position the finger on the surface for a few seconds and then lift it.
- **Restoration**
  Aimed at restoring the initial conditions of the sensor; it starts when the finger is lifted from the surface and its duration may vary according to the sensor characteristics (typically about 10–15 seconds).

# Biometric cryptosystem

- Biometric cryptosystems refer to systems which can be used for securing a cryptographic key using some biometric features.
  - Key generation - for generating a cryptographic key from biometric features, or to a secure biometric template. Cryptographic key is stored together with the biometric template After a successful biometric matching, the key is released.
  - In the key binding mode, the key is bound to the biometric template in such a way that both of them are inaccessible to an attacker and the key is released when a valid biometric is presented.

# Biometric cryptosystem

- Biometric Encryption algorithms- Fuzzy vault, Fuzzy commitment, Secure sketch
- Cancelable Biometrics algorithms- Distorting transforms, Bio-Hashing, Bio-Encoding

# Requirements

(1) **Diversity**: the secure template must not allow crossmatching across databases, thereby ensuring the user's privacy.
(2) **Revocability**: it should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data.
(3) **Security**: itmust be computationally hard to obtain the original biometric template from the secure template. This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.
(4) **Performance**: the biometric template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

# Fuzziness of Biometrics

- The difficulty of binding biometric and user data lies mostly in how the fuzziness of biometrics and the exactitude of user data (key) are bridged.

# Fuzziness of Biometrics

- Unlike the password-based identity authentication system, biometric signals and their representations (e.g., fingerprint image and its computer representation) of a person vary dramatically depending on the acquisition method, acquisition environment, and user's interaction with the acquisition device [2].
- Acquisition condition variance: The signal captured by a sensor varies with the identifier as well as the acquisition equipment. For example, fingerprint images are usually captured with contacting sensors.

# Fuzziness of Biometrics

- Circumstances and time variance: Change in outer circumstances may also cause the captured biometric signal to vary more or less. While taking the fingerprint, for example, the environmental temperature and humidity may render the finger too dry or too damp to be captured.

# Fuzziness of Biometrics

- Low-quality fingerprint images are very common in real application systems and enhancing (i.e., preprocessing) them is a challenging research direction in the traditional fingerprint recognition field.
- Generally, the fingerprint does not change with time because the skin on the finger tip may not change much with age. But many modalities cannot resist the temporal change, e.g., face, gait, palm, voice, and so on.
- In particular, the face varies greatly with age; facial images captured from the same person at different ages differ vastly. How one estimates the aging model of a person also makes an important research issue in the face recognition field. In addition, there are other factors which can influence the captured biometric signal for some specific modality.

# Fuzziness of Biometrics

- Feature extraction variance: Almost all the feature extraction algorithms are based on signal processing or image processing methods. They are not exact when processing different biometric samples. Noise is often introduced in the extraction procedure, especially of the low-quality samples.
- All the above factors can make the samples from the same subject seem different and the ones from different subjects quite similar.
- However, a cryptosystem requires exact computing and operation. A tiny change in input may cause an enormous difference in output, for example, for the hash function. So bridging the fuzziness of biometrics and the exactness of cryptography becomes the greatest challenge in the binding of biometric and user data.

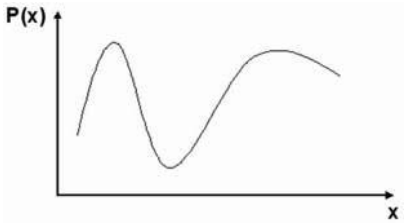
# Fuzzy Vault Scheme

- Juels and Sudan proposed a fuzzy vault scheme in 2002 Suitable for unordered data with arbitrary dimensionality such as fingerprint minutiae Fuzzy vault scheme is an error-tolerant framework by which one can encrypt some secret such as cryptographic key using locking elements set *A* , after locked, the locked data is called vault. Someone who has another data set *B* that is sufficiently close to set *A* will decrypt the vault successfully. A Reed-Solomon code is introduced into the scheme to deal with the variances between *A* and *B* . However, as some researchers point out [8, 9], special use of the Reed-Solomon code in the UNLOCK algorithm in the scheme is not appropriate, which result in much extra work to reduce the differences between sensed samples of the same user, such as alignment [5], feature transformation [6], extra storage of error correction data [7] etc., which may cause leakage of biometric data.

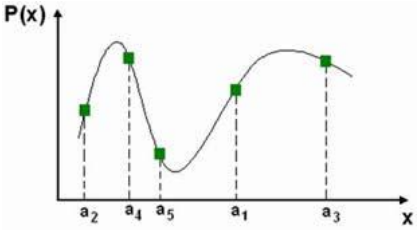
# Fuzzy Vault Scheme

- A polynomial P is used to embed a secret key k in
- A minutiae point set $A = \{a_1, a_2, \ldots, a_t\}$ is evalua with P, if $x_i = a_i, y_i = P(x_i)\ for\ i = 1..t$
- Add chaff points $x_i$ such that, $x_i \notin A, for\ i = t +$ and $y_i \notin P(x_i), for\ i = t + 1..r$
- Vault is, $V_A = \{x_i, y_i\}, for\ i = 1..r$
- If $B = \{b_1, b_2, \ldots, b_t\}$ is input set obtained at verif vault is constructed $V = \{x_j, y_j\} and\ x_j \subset B$
- If set B is input given by genuine user, decoding is

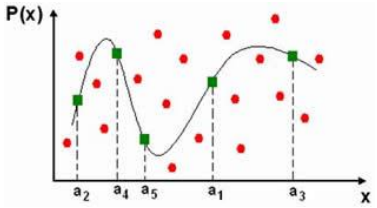
# Fuzzy Vault Scheme



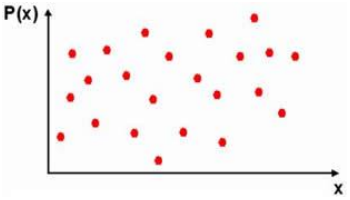

Polynomial




Minutiae points evaluated by polynomial




Chaff points added




Vault

# Fuzzy Commitment Scheme

- Proposed by Juels and Wattenberg in 1999
- Template must be an ordered bit string of a fixed length
- Minutiae feature cannot be used directly

- Fuzzy Commitment scheme [8] is one of the earliest methods of binding biometric and user data. It is actually an ordinary commitment scheme (a primitive in cryptography) taking biometric templates as private keys, and employing error correcting codes to tackle the fuzziness problem of biometric templates.

- As an ordinary cryptographic commitment, the fuzzy commitment scheme has two procedures: committing and decommitting. To commit a bit string x, first generate a codeword c from x according to a prespecified error correcting code, then apply some cryptographic hash function (or one-way function) to c, the ultimate commitment is (h(c), w + c), where w is a biometric template related string with the same length of c. To decommit a commitment, the user has to provide a biometric template related string w' which is close to that in the committing procedure; the verifier uses it to decode the correct codeword c, then checks whether the hash value of c equals the stored hash value in the commitment, and accepts the commitment if they are equal, rejects otherwise.
- The fuzzy commitment scheme is essentially a Secure Sketch as observed by Dodis et al. [5].

# Fuzzy Commitment Scheme

- Proposed by Juels and Wattenberg in 1999
- Template must be an ordered bit string of a fixed length
- Minutiae feature cannot be used directly

# Fuzzy Commitment Scheme

- Binary length fixed feature b is given as input Codeword c is randomly selected
- Encrypted template is: $e = b \oplus c$
- Hash function h(c) is stored along with e
- In verification phase, query biometric b’ is given as input
- Decrypted as: $e' = b' \oplus e = b' \oplus b \oplus c$
- By decoding e’ codeword c’ is obtained
- If $h(c) = h(c') then\ c = c'$

# Performance Evaluation

- Performance evaluation of the binding of biometric and user data should be conducted based mainly on two aspects: accuracy and security.
- Accuracy reflects the effect after binding of biometric and user data as an enhanced identity authentication way, and security can provide information on the probability that the system will be attacked successfully.

- Accuracy: The accuracy of biometric-like identity authentication is due to the genuine and imposter distribution of matching. The overall accuracy can be illustrated by Receiver Operation Characteristics (ROC) curve, which shows the dependence of False Reject Rate (FRR) on False Accept Rate (FAR) at all thresholds. When the parameter changes, FAR and FRR may yield the same value, which is called Equal Error Rate (EER). It is a very important indicator to evaluate the accuracy of the biometric system, as well as binding of biometric and user data.

- Security: The security of the binding of biometric and user data depends on the length of user data, which is converted to binary 0/1 expression. It assumes the attacker has full knowledge about the binding method, but can only mount brute-force attack on the system. So the system security is weighed by bit length of the user data. Typically, the security of the iris binding system is 140-bit,and that of fingerprint is 128-bits. However, typical face binding algorithm holds only 58-bit security

# References


1. “Handbook of fingerprint recognition”, A. K. Jain, Prabhakar.
2. “Encyclopedia of biometrics”, Stan Z. Li, Anil K. Jain.
3. “Advances in Biometrics”, Nalini K. Ratha, Venu Govindaraju.