Mustansiriyah University/College of Science/Dept. of CS **2nd Exam/19-11-2019**

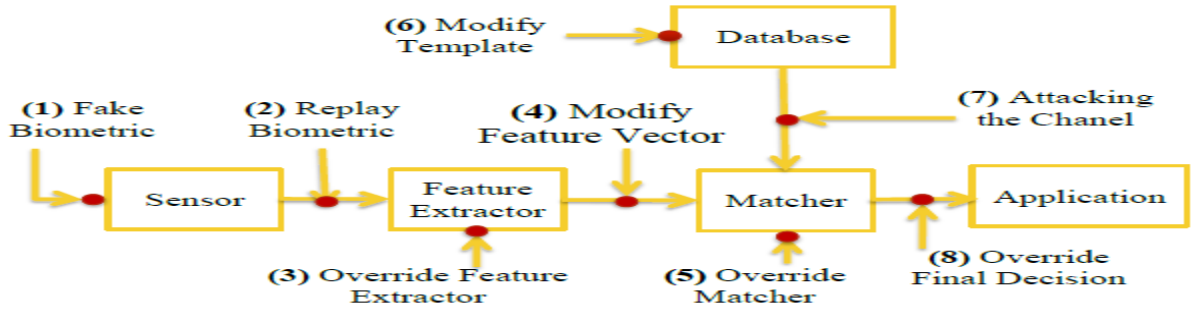
Ph.D Course 2019/2020 **DR. Bashar M. Nema**

Q1) Answer the following MCQ's:

1. One of the Behavioral identifiers in Biometrics is:
   A) Iris B) Fingerprint C) DNA D) Voice
2. One of the biometric system modules is:
   A) Fingerprint B) Classification C) Feature Extraction D) Hardware
3. Keystroke dynamics used to provide user _____.
   A) Identification B) Verification C) Authentication D) Validation
4. One of the techniques of Keystroke is _____, which information processing approach, which is, inspired by the way the brain process information.
   A) Statistical B) Neural network C) Pattern Recognition D) Heuristics algorithms
5. In _____ forgery, elements from multiple images often put together in a single image to convey an idea that could not have been conveyed by any of the original images.
   A) Copy Move B) Slicing C) Composition D) Resampling
6. In Video forgery, _____entail cropping the frames of a video to eliminate evidence of occurrence of a crime in the outermost parts of video.
   A) Upscale B) Copy-Paste C) Framing D) Removing Object
7. One of the major components of the DRM reference architecture who controls the process of DRM Packager is _____.
   A) Metadata B) License Server C) Client D) Content Server
8. _____ One of DRM Protection technologies that belongs to Rights Languages.
   A) Conditional Access B) Inter-operability C) Integrity checking D) Copy Control
9. _____of a watermarking system represent probability of detection after embedding.
   A) Fidelity B) Capacity C) Robustness D) Effectiveness
10. _____ is a special class of watermarking techniques where robustness is undesirable.
    A) Fragile B) Visible C) Imperceptible D) Non-Robust.
11. One of basic types of intellectual properties is _____.
    A) Steganography B) Fingerprint C) Trademark D) None of them.
12. In watermark security, the ability to resist hostile attacks done by unauthorized removal such as _____.
    A) Forgery Watermark B) Collusion C) Scaling D) Noising.

Q2) Describe with Figure the attack points in Biometric system.

ANSWER:



10.1 Fake Biometric

In this type of attack a fake biometric such as a fake finger or image of the face is presented at the sensor.

10.2 Replay Biometric

Biometric Signals In this mode of attack a recorded signal is replayed to the system bypassing to the sensor.

10.3 Override Feature Extractor

The feature extractor is forced to produce feature sets chosen by the attacker, instead of the actual values generated from the data obtained from the sensor.

10.4 Modify Feature Vector

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

10.5 Override Matcher

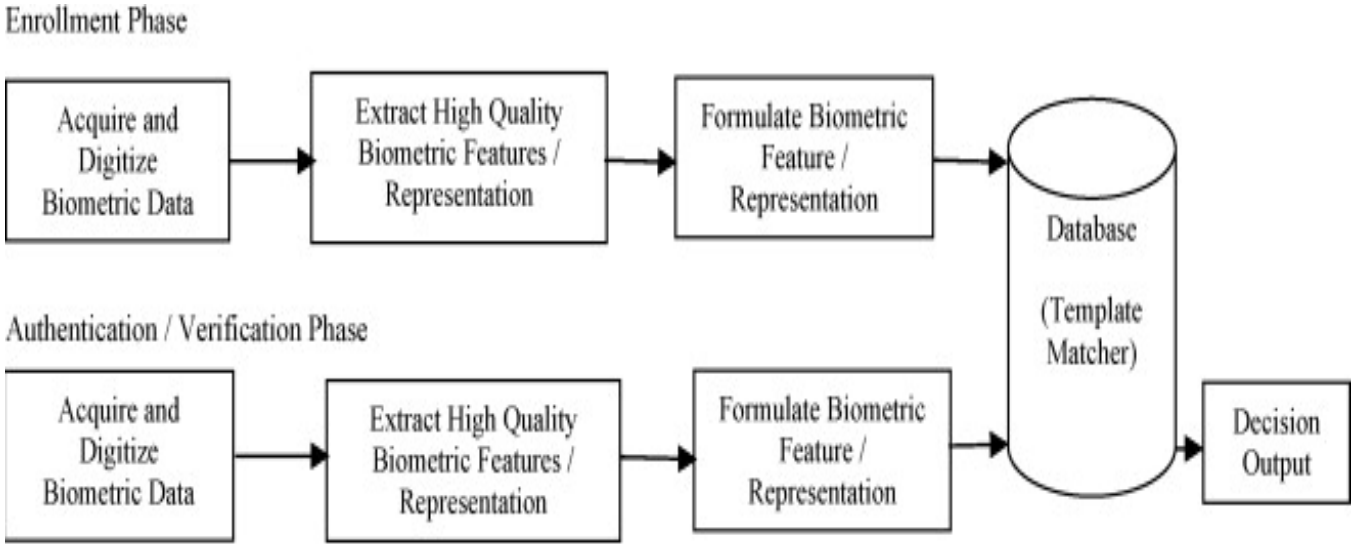
The matcher component is attacked to produce pre-selected match scores regardless of the input feature set.

10.6 Modify Template

Modifying one or more templates in the database, which could result either in authorizing a fraud or denying service to the person, associated with the corrupted template.

Q3) General process for Keystroke based authentication methods require many stages. Describe using Figure only these stages?

ANSWER:



Q4) Answer the following:

A) Why DRM controller on the client side has to check the rendering application at some time?

ANSWER:

- **To avoid making unauthorized copies**
- **To check certain rights limits**

B) What is DRM? Draw the steps of any DRM system?

ANSWER:

DRM is the chain of hardware and software services and technologies governing the authorized use of digital content and managing any consequences of that use throughout the entire life cycle of the content

Q5) Describe the desired Properties of Watermarking?

ANSWER:

- **High fidelity**
  - Finding adequate perceptual quality index is still an open problem
  - Objective distortion measures are often adopted
- **Strong robustness**
  - Robustness is difficult to define
  - Benchmarks testing various attacks exist
- **Large capacity**
  - Required payload length depends on the purpose of different applications
- **Blind detection**
  - Original content is not required in detection side
  - Non-blind detection limits the applicability of watermarking schemes
- **Low computation complexity**
  - Manufacturing cost and time constraints are important concerns