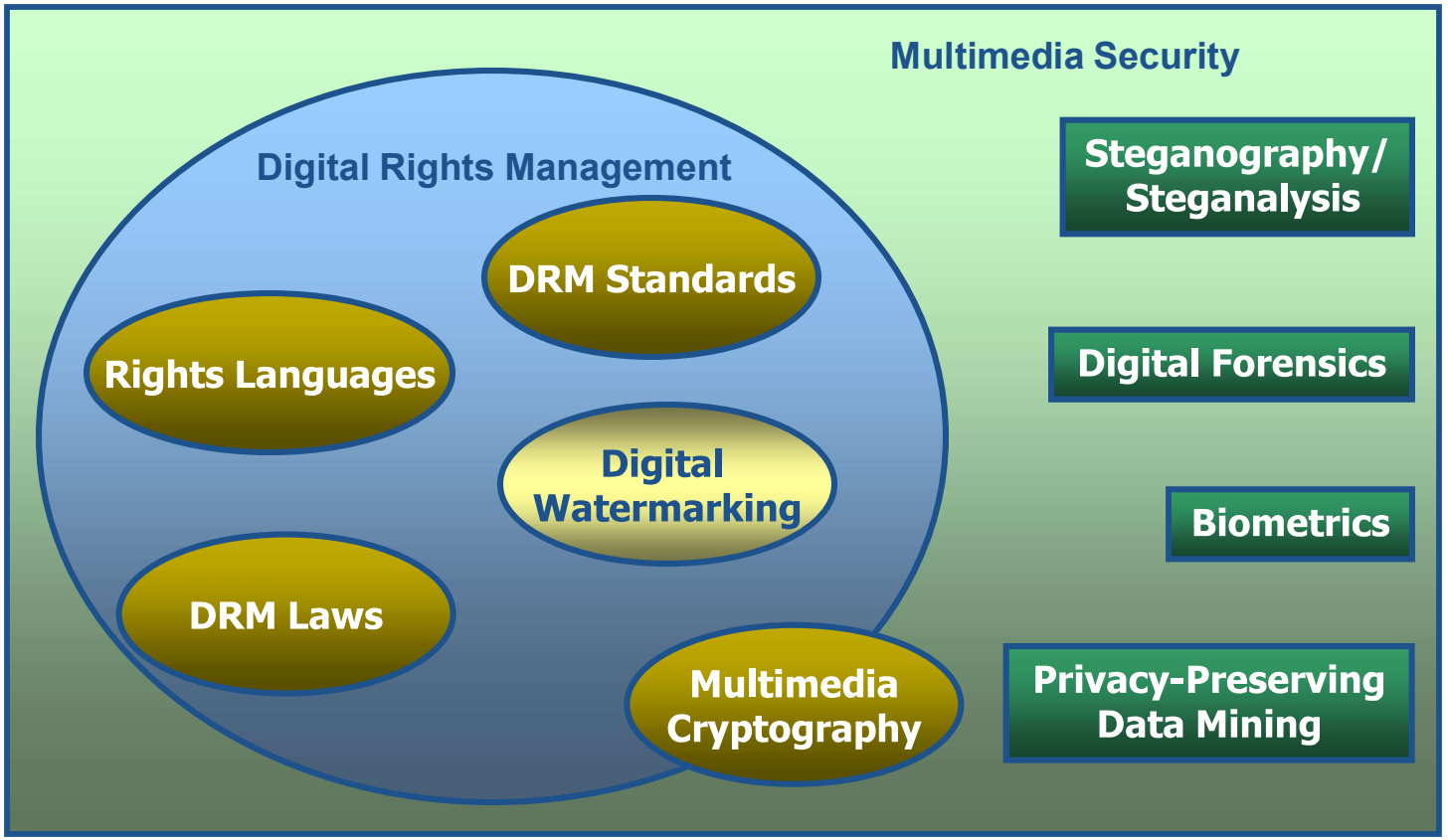
Introduction to Multimedia Security Topics Covered in this Course

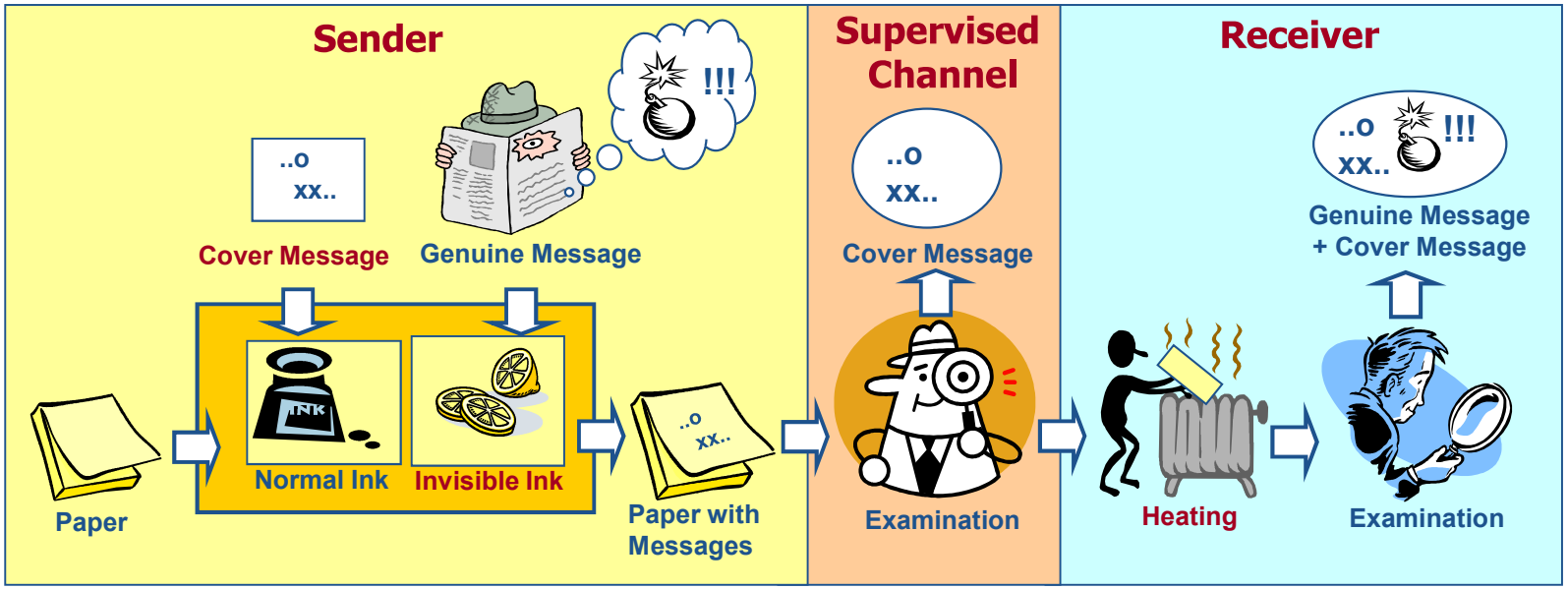
Multimedia Security

Course Coverage



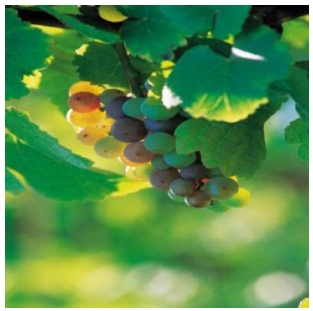
Steganography

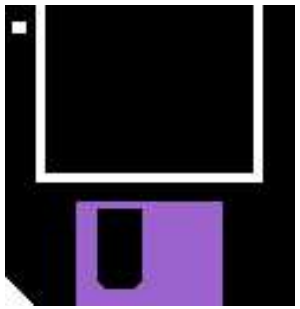
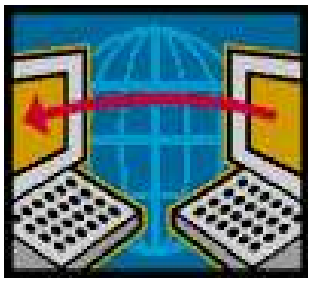
- Steganography="Cover" + "Writing"
  - The art of hiding information in ways that prevent the detection of hidden messages
  - Transmitting secret messages through innocuous cover carriers in such a manner that the existence of the embedded message is undetectable
- Examples
  - Invisible inks, character arrangement, covert channels…



Digital Steganography Schemes

- Various message carriers
  - Digital contents
    - Texts, images, audio, video
  - Storage devices
    - Unused space or hidden partition
  - TCP/IP packets
    - Unused or reserved bits in the header



Steganalysis

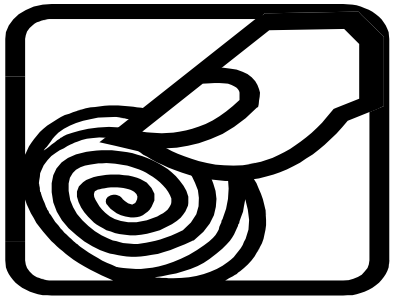
- Hiding information within electronic media requires alternations of the media properties that may introduce some form of degradation or unusual characteristics
- Forms of attacks and analysis on hidden information
  - Detecting
  - Extracting
  - Disabling/destroying

- The attacking approaches vary depending upon the methods used to embed the information into the cover media
  - An arms race?

Biometric Recognition

- Biometrics = “life”+”measure”
- Automatic recognition of individuals based on their physiological and/or behavior characteristics

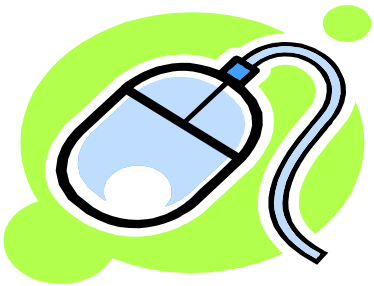
face



fingerprint

iris

…

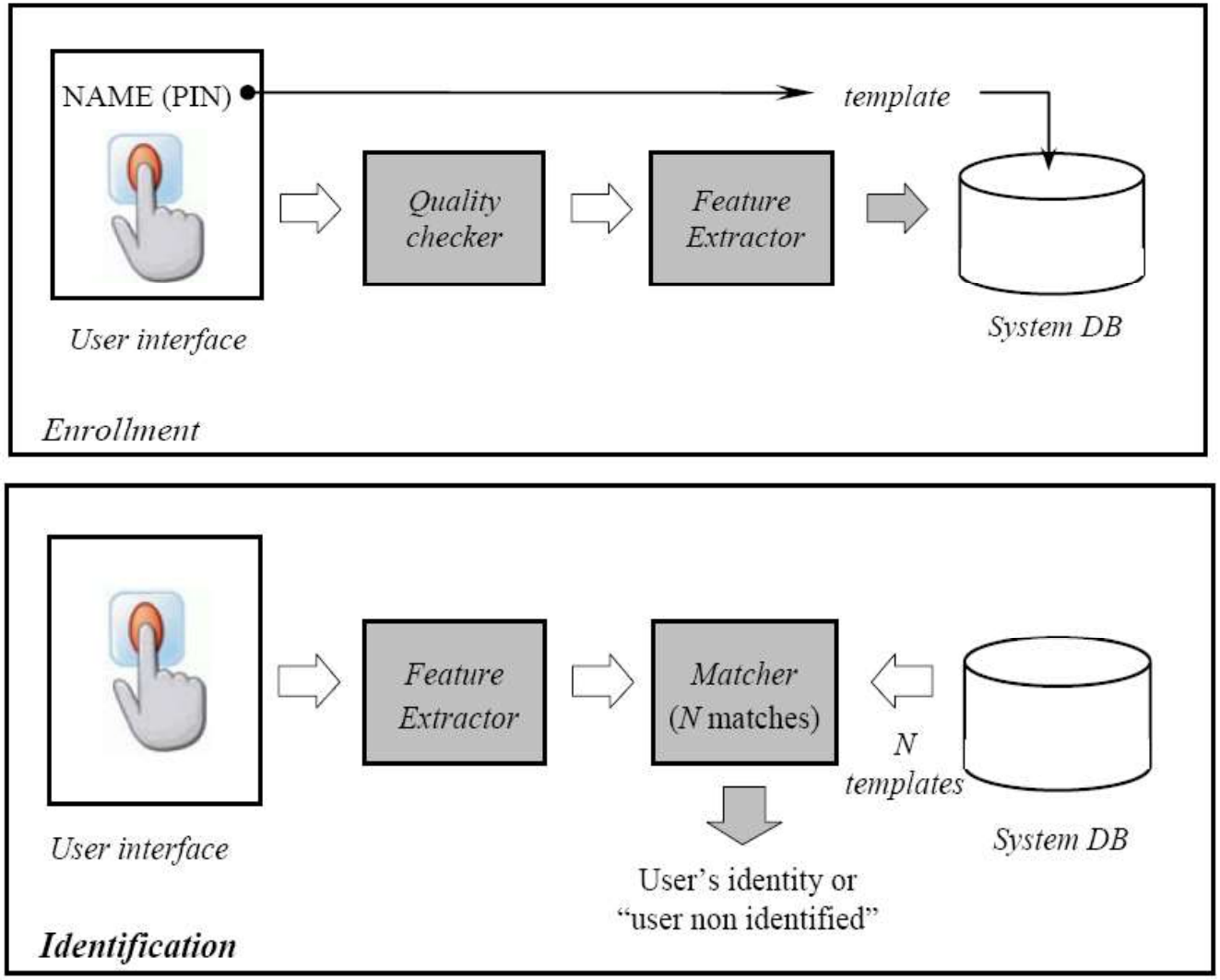


user input

Requirements of Biometrics

- A biological measurement qualifies to be a biometric if it satisfies
  - Universality
  - Distinctiveness
  - Permanence
  - Collectability
- A practical biometric system must satisfy
  - Performance
  - Acceptability
  - Circumvention

A Biometric System



Applications of Biometrics

- Secure access to
  - Buildings
  - Computer systems
  - Laptops
  - Cell phones
  - ATMs
- "who he is" instead of "what he possesses" and "what he remembers"

Content Tampering

- Image tampering
  - Object removing
  - Composition
  - Morphing
  - Re-touching
  - Enhancing
  - Computer graphics
  - Painting



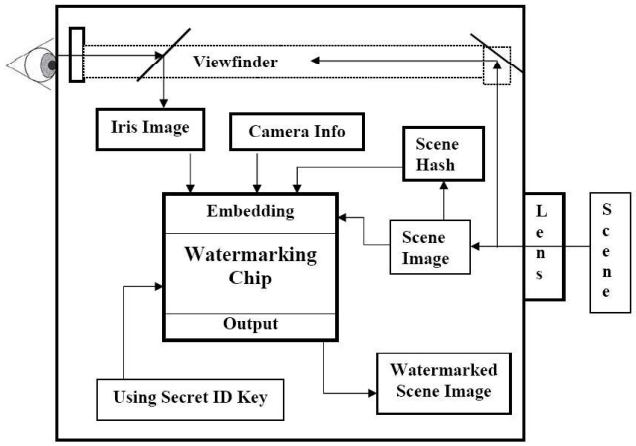






Watermarking-Based Forensics

- Watermarking-based schemes
  - Fragile watermarking
    - Watermarks will be undetectable when the content is changed in any way
  - Semi-fragile watermarking
    - Watermark will survive only legitimate distortion
  - Watermarks enabling distortion localization or restoration
- A major drawback
  - Watermarks must be embedded either at the time of recording or afterwards by a person authorized to do so



Example: A Secure Digital Camera

Statistical Techniques for Detecting Traces

- Assumption
  - Digital forgeries, though visually imperceptible, alter some underlying statistical properties of natural images
- Techniques
  - Re-sampled images
    - Correlations between neighboring pixels
  - Color Filter Array (CFA) interpolated images
    - Correlations are destroyed when the image is tampered
  - Double compressions
  - Duplicated regions
  - Inconsistent noise patterns