Information Hiding
Applications

Nasir Memon
Polytechnic University, Brooklyn
Information Hiding

- Information Hiding: Communication of information by embedding it in and retrieving it from other digital data.
- Depending on application we may need process to be imperceptible, robust, secure. Etc.
Information Hiding
A Communications Framework

More about this tomorrow!!
Where can we hide?

- Media
  - Video
  - Audio
  - Still Images
  - Documents
- Software
- Hardware designs
- Etc.

We focus on data hiding in media.

We mainly use images but techniques and concepts can be suitably generalized to other media.
Why Hide?

- Because you do not want someone to find it
  - Copy protection and deterrence - Digital Watermarks
- Because you do not want any one to even know about its existence
  - Covert communication – Steganography
- Because it is ugly
  - Media bridging,
  - Meta Data embedding
Applications of Information Hiding

- Ownership assertion.
- Fingerprinting.
- Copy prevention or control.
- Authentication.
- Broadcast Monitoring
- Media Bridging
- Meta data Hiding
- Covert communication
- Etc.
Ownership Assertion

Public-Private Key Pair, Digital Certificate

Alice

Private Key

Original Content

Watermark

Watermarked content

Illegal copy

Bob

Judge

Original Content

Illegal copy

Watermark
Fingerprinting

Illegal copies reveal Bob’s ID

Original Content

Fingerprint 1

Fingerprint 2

Fingerprint n

Copy 1

Copy 2

Copy n

Bob

Illegal copies

Judge
Copy Prevention and Control

Original Content

Content with copy prevention watermark

Bob

Compliant Player

Recorder disallows more than n copies

Compliant Recorder
Requirements

- Requirements vary with application.
  - Perceptually transparent - should not perceptually degrade original content.
  - Robust - survive accidental or malicious attempts at removal.
  - Oblivious or Non-oblivious - Recoverable with or without access to original.
  - Capacity – Number of bits hidden
  - Efficient encoding and/or decoding.

- Requirements are inter-related.
Security

- One requirement often ignored or at least shabbily treated – Security.
- What does security mean?
- This has been generally interpreted as “embedded information cannot be detected, read (interpreted), and/or modified, or deleted by unauthorized parties”
- But there is more to security …
There is More to Security

- Depends on application –
  » Ownership Assertion
  » Authentication
  » Steganography

- Rest of the day we review above applications and proposed solutions and examine security aspects a bit more carefully.

- We shall assume that we know how to meet other requirements like robustness etc. efficiently and effectively.