Information Hiding

CS 803 / IT 803

Dr. Zoran Duric

Tuesday 7:20-10:00 in IN 211

zduric@cs.gmu.edu

Office hours: Tuesday 2:00-4:00pm or by appt.

S&T II, Rm 427

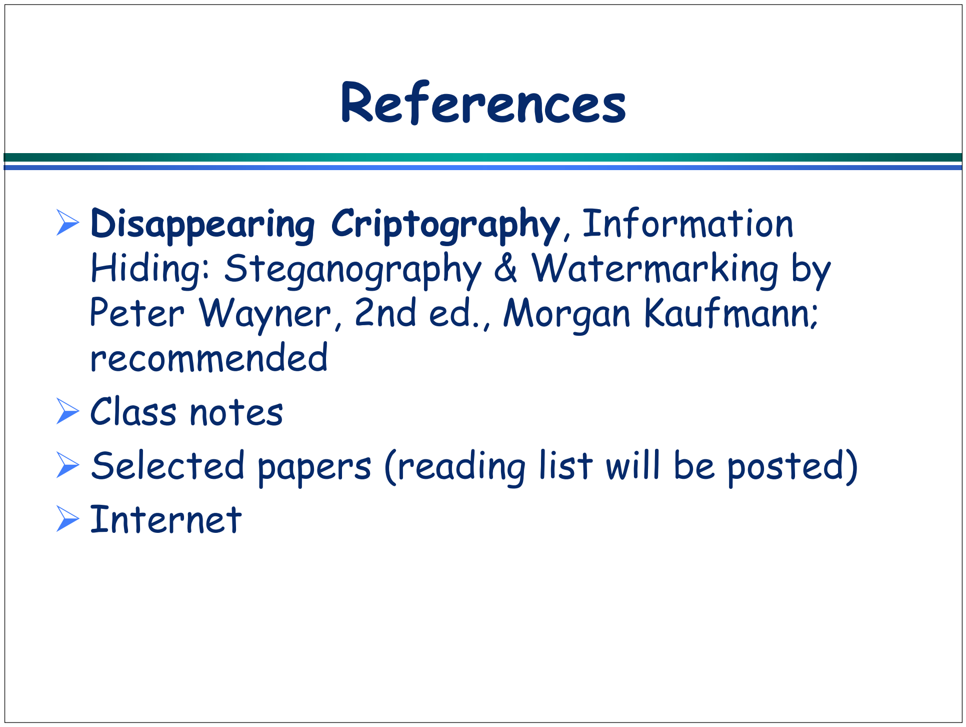
http://www.cs.gmu.edu/~zduric/cs803.html

Course Content

Study of information hiding approaches. Topics include:

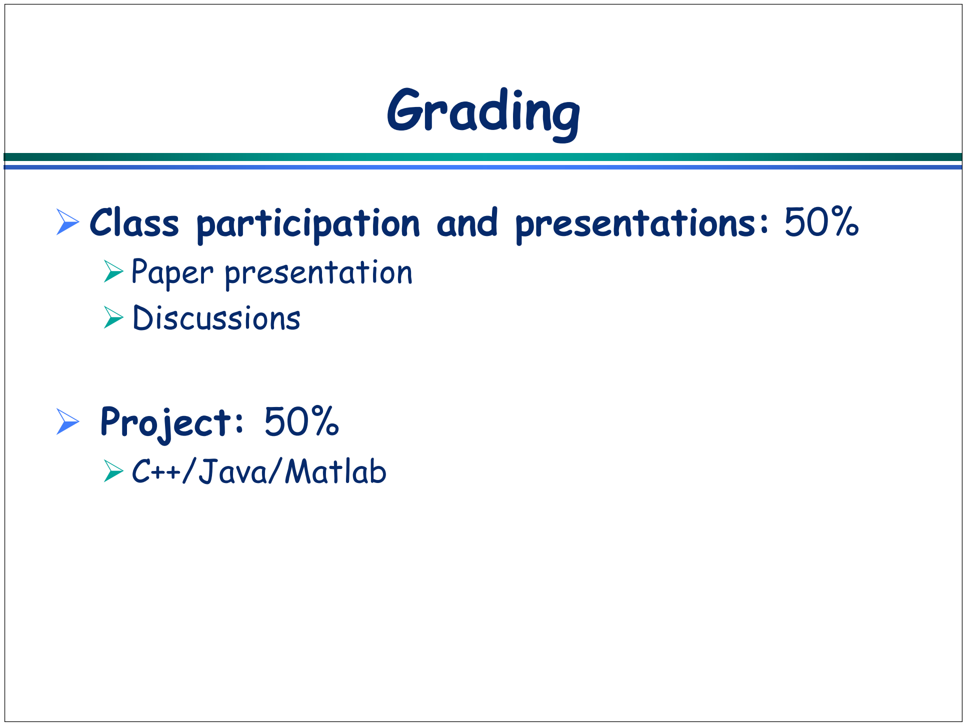
- Overview of information hiding techniques
- Overview of audio, image, and video formats
- Anonimity
- Covert channels
- Steganography and steganalysis
- Watermarking

Many practical techniques will be considered. Class work will include reading and presenting technical papers on information hiding. A programming project in C++/Java/Matlab is required.



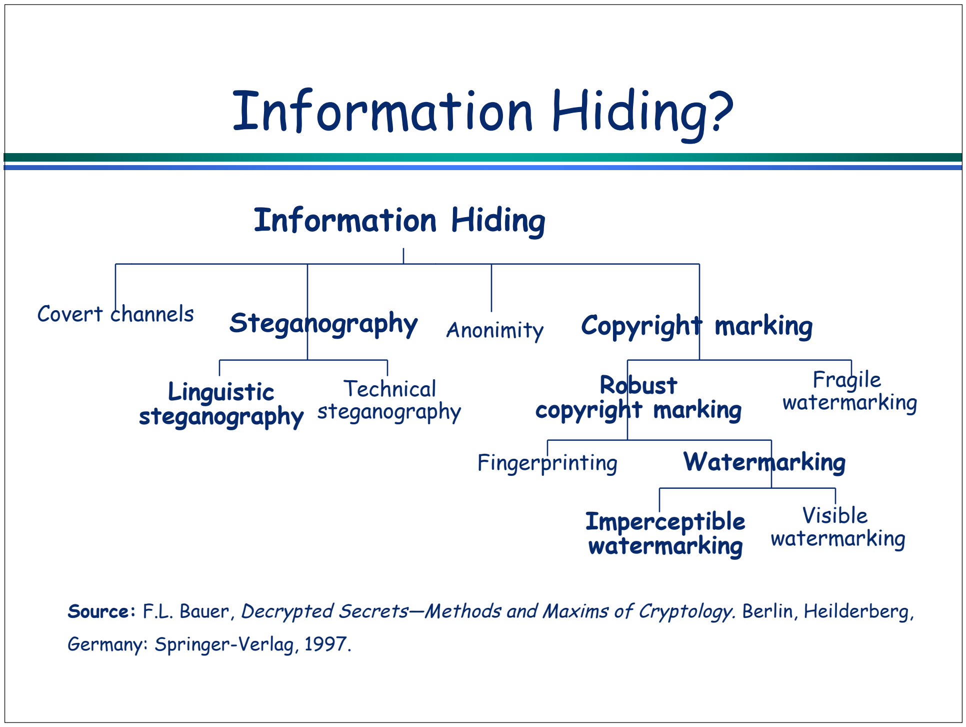
References

- **Disappearing Criptography**, Information Hiding: Steganography & Watermarking by Peter Wayner, 2nd ed., Morgan Kaufmann; recommended
- Class notes
- Selected papers (reading list will be posted)
- Internet



Grading

- **Class participation and presentations:** 50%
  - Paper presentation
  - Discussions
- **Project:** 50%
  - C++/Java/Matlab

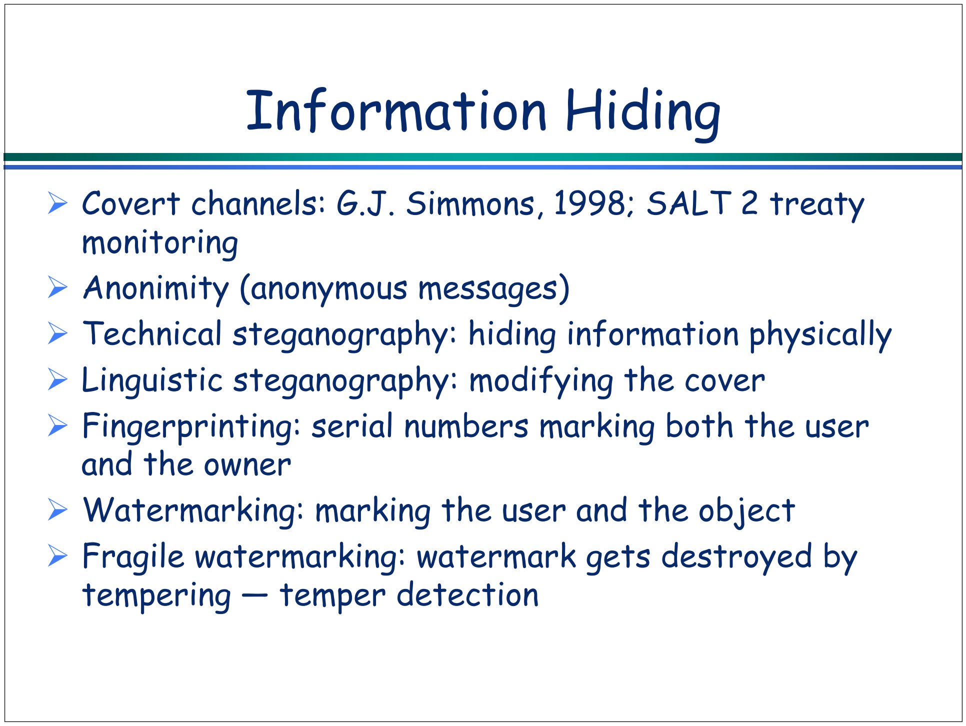


Information Hiding?

Information Hiding

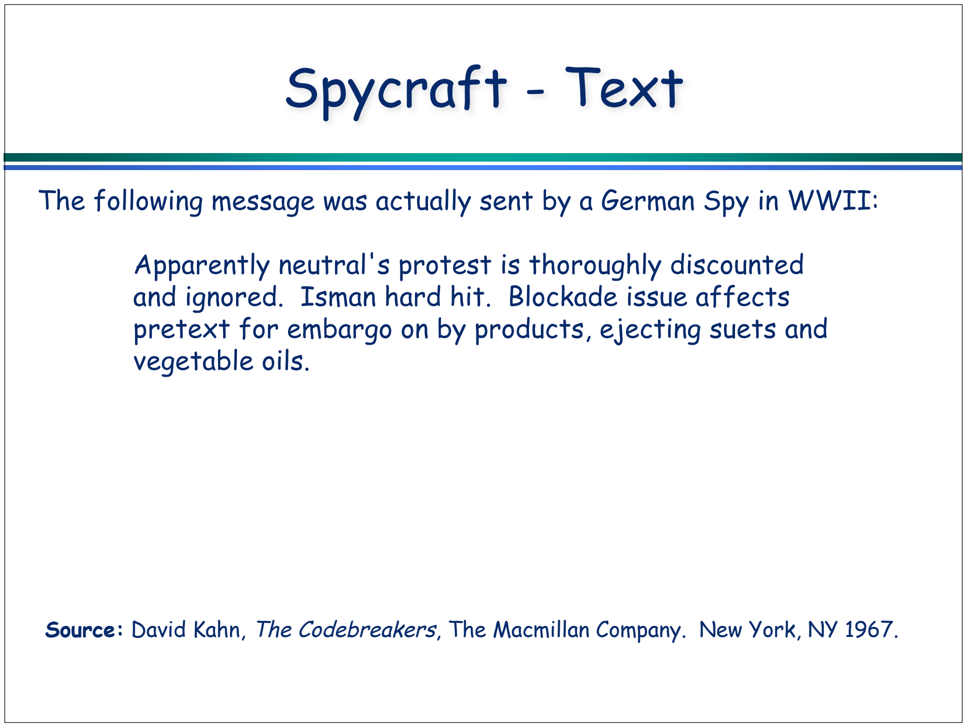
- Covert channels
- Steganography
  - Linguistic steganography
  - Technical steganography
- Anonimity
- Copyright marking
  - Robust copyright marking
    - Fingerprinting
    - Watermarking
      - Imperceptible watermarking
      - Visible watermarking
  - Fragile watermarking

Source: F.L. Bauer, *Decrypted Secrets—Methods and Maxims of Cryptology*. Berlin, Heilderberg, Germany: Springer-Verlag, 1997.



Information Hiding

- Covert channels: G.J. Simmons, 1998; SALT 2 treaty monitoring
- Anonimity (anonymous messages)
- Technical steganography: hiding information physically
- Linguistic steganography: modifying the cover
- Fingerprinting: serial numbers marking both the user and the owner
- Watermarking: marking the user and the object
- Fragile watermarking: watermark gets destroyed by tempering — temper detection

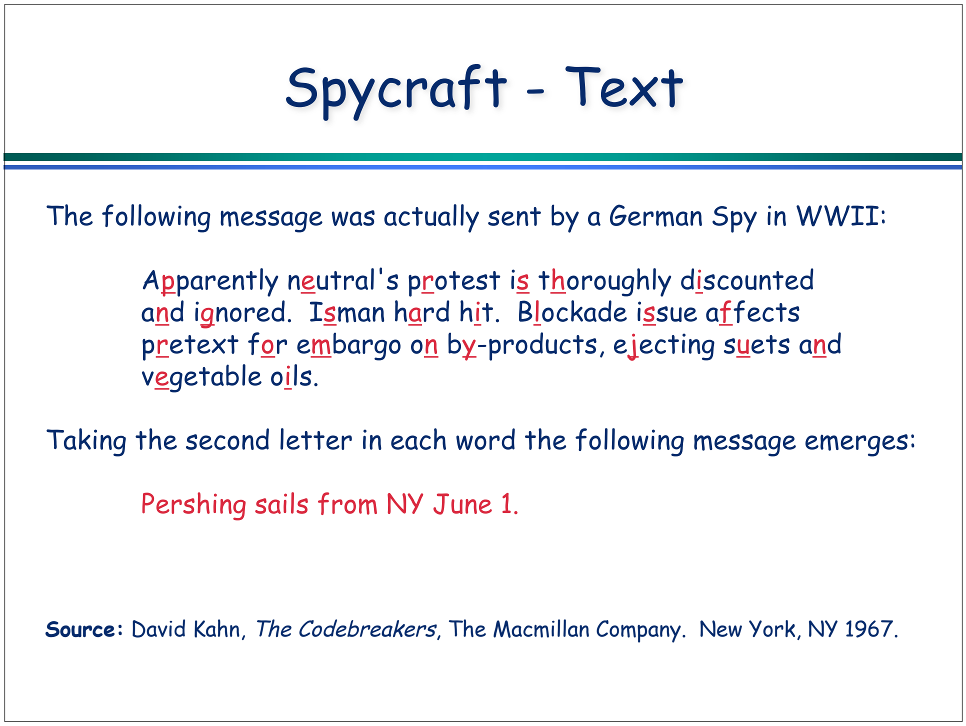


Spycraft - Text

The following message was actually sent by a German Spy in WWII:

> Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.

Source: David Kahn, *The Codebreakers*, The Macmillan Company. New York, NY 1967.



Spycraft - Text

The following message was actually sent by a German Spy in WWII:

> Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.

Taking the second letter in each word the following message emerges:

> Pershing sails from NY June 1.

Source: David Kahn, *The Codebreakers*, The Macmillan Company. New York, NY 1967.

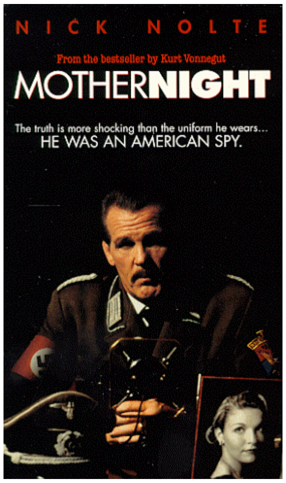
File Systems - Example

- Hidden partitions
- unused, allocated (wasted) space
- Windows 95, FAT16 allocates a minimum of 32 kilobytes to each file
- Headers

Information Hiding in Movies

NICK NOLTE
From the bestseller by
MOTHER
The truth is more shocking than
HE WAS AN AME
VAL KILMER ELISABETH SHUE
INDEPENDENCE DAY
SPECIAL • EDITION
From the Academy Award®-Winning Director of "Forrest Gump" and the Pulitzer Prize-Winning Author of "Contact."
JODIE FOSTER
MATTHEW McCONAUGHEY
A message from deep space.
Who will be the first to go?
A journey to the heart of the universe.
CONTACT
DVD

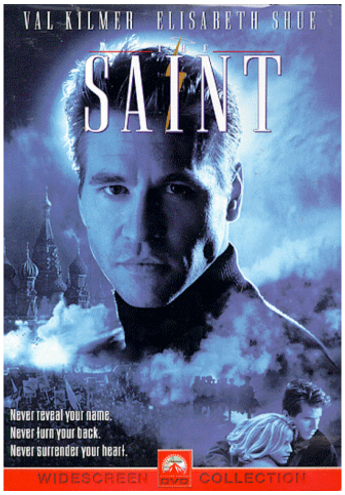
Mother Night


NICK NOLTE
From the bestseller by Kurt Vonnegut
MOTHERNIGHT
The truth is more shocking than the uniform he wears...
HE WAS AN AMERICAN SPY.

U.S. spy in Nazi Germany during WWII passes secret messages in radio broadcasts.

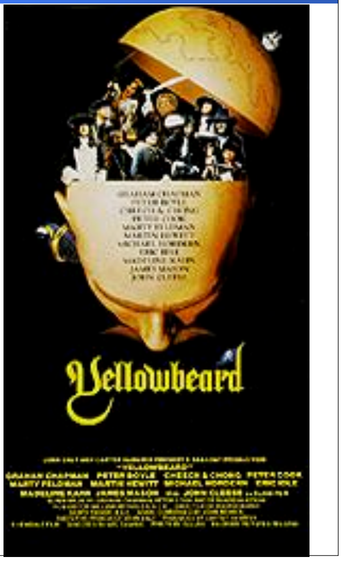
Saint

Receives and sends encoded messages in e-mail.


VAL KILMER ELISABETH SHUE
THE SAINT
Never reveal your name.
Never turn your back.
Never surrender your heart.
WIDESCREEN DVD COLLECTION

Yellowbeard

The Map to Yellowbeard's Treasure is tattooed on his son's head.



Independence Day

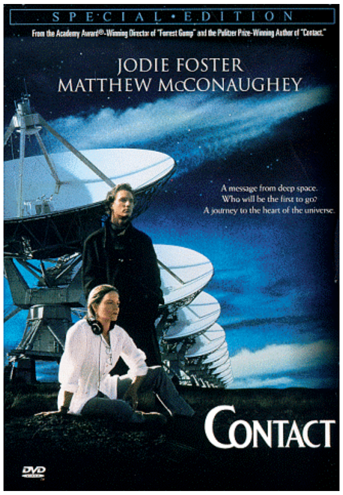
Aliens "hijack" satellite signals to embed a countdown sequence between spacecraft.

Contact

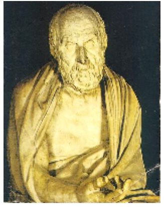
Television broadcast found embedded in a space signal sent to Earth.

Alien code found embedded within the frames of the television broadcast.

The primer to decode the alien message is embedded within the message. "Cracking" the code reveals blueprints to a machine.


SPECIAL • EDITION
From the Academy Award®-Winning Director of "Forrest Gump" and the Pulitzer Prize-Winning Author of "Contact."
JODIE FOSTER
MATTHEW McCONAUGHEY
A message from deep space.
Who will be the first to go?
A journey to the heart of the universe.
CONTACT
DVD

Ancient Steganography



Herodotus (485 – 525 BC) is the first Greek historian. His great work, The Histories, is the story of the war between the huge Persian empire and the much smaller Greek city-states.

Herodotus recounts the story of **Histaiaeus**, who wanted to encourage **Aristagoras of Miletus** to revolt against the Persian king. In order to securely convey his plan, Histaiaeus shaved the head of his messenger, wrote the message on his scalp, and then waited for the hair to re-grow. The messenger, apparently carrying nothing contentious, could travel freely. Arriving at his destination, he shaved his head and pointed it at the recipient.

Ancient Steganography

Pliny the Elder.
AD 23 - 79

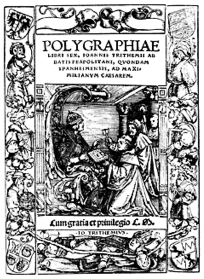
Pliny the Elder explained how the milk of the thithymallus plant dried to transparency when applied to paper but darkened to brown when subsequently heated, thus recording one of the earliest recipes for invisible ink.

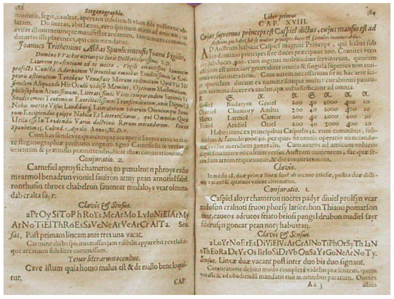
The **Ancient Chinese** wrote notes on small pieces of silk that they then wadded into little balls and coated in wax, to be swallowed by a messenger and retrieved later.

Renaissance Steganography

Johannes
Trithemius
(1404-1472)

1518 Johannes Trithemius wrote the first printed book on cryptology. He invented a steganographic cipher in which each letter was represented as a word taken from a succession of columns. The resulting series of words would be a legitimate prayer.


POLYGRAPHIAE
LIBRI SEX, IOANNIS TRITHEMII ABBATIS PEAPOLITANI, QVONDAM SPANHEIMENSIS, AD MAXIMILIANVM CAESAREM.
Cum gratia et privilegio C. M.

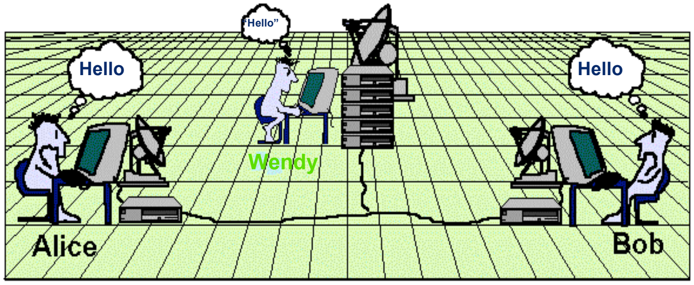


Renaissance Steganography

Giovanni Battista Porta
(1535-1615)

Giovanni Battista Porta described how to conceal a message within a hard-boiled egg by writing on the shell with a special ink made with an ounce of alum and a pint of vinegar. The solution penetrates the porous shell, leaving no visible trace, but the message is stained on the surface of the hardened egg albumen, so it can be read when the shell is removed.

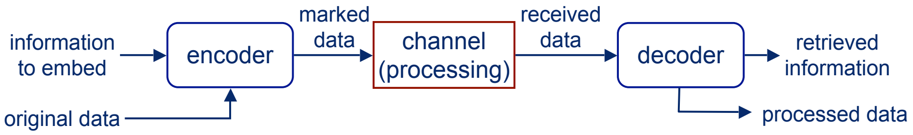
Modern Steganography - The Prisoners' Problem



- Simmons – 1983
- Done in the context of USA – USSR nuclear non-proliferation treaty compliance checking.

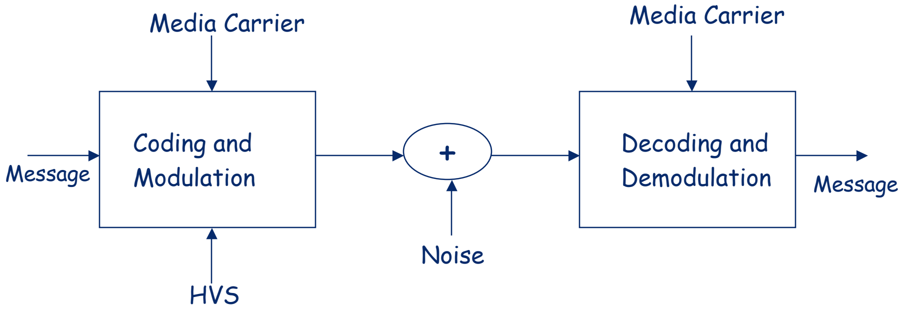
Information Hiding: Definition

- 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.

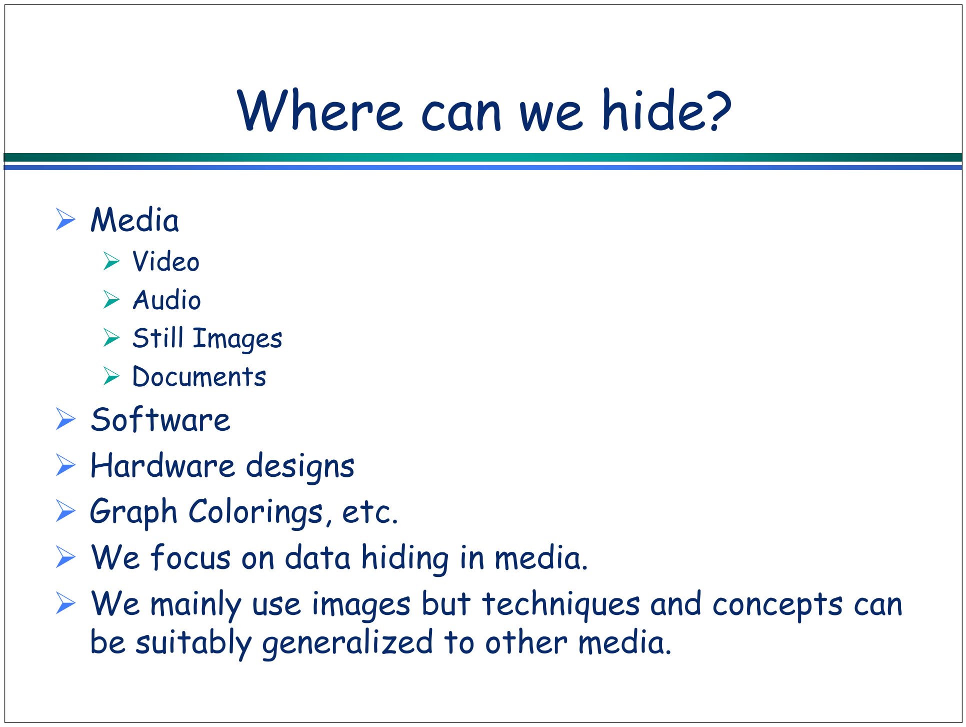


information to embed
original data
encoder
marked data
channel (processing)
received data
decoder
retrieved information
processed data

Information Hiding
A Communications Framework

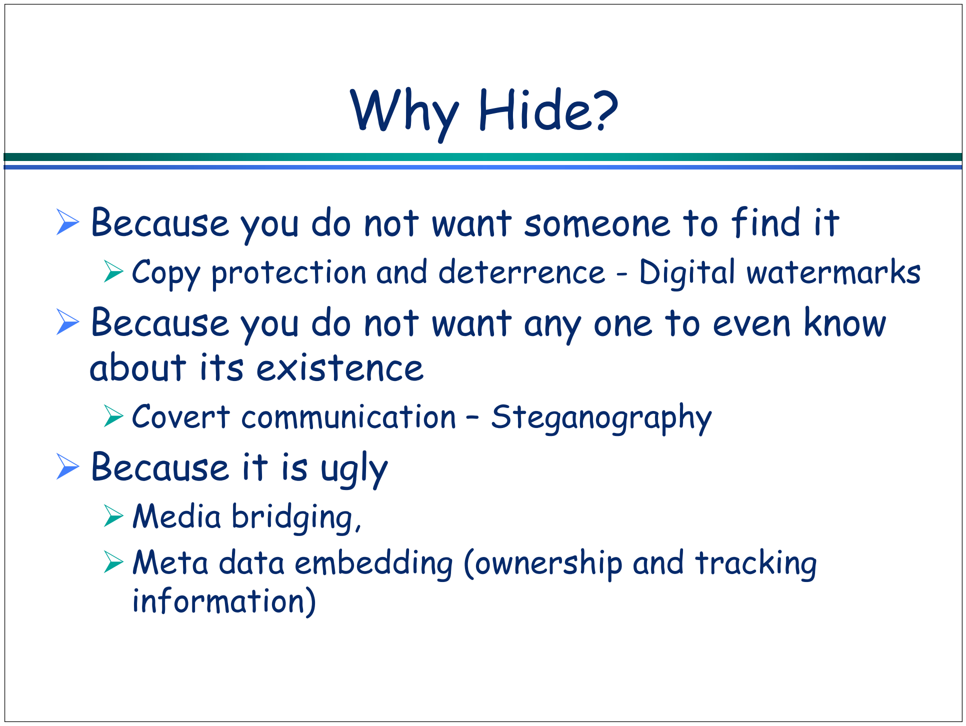


Media Carrier
Message
Coding and Modulation
HVS
+
Noise
Media Carrier
Decoding and Demodulation
Message



Where can we hide?

- Media
  - Video
  - Audio
  - Still Images
  - Documents
- Software
- Hardware designs
- Graph Colorings, etc.
- We focus on data hiding in media.
- We mainly use images but techniques and concepts can be suitably generalized to other media.



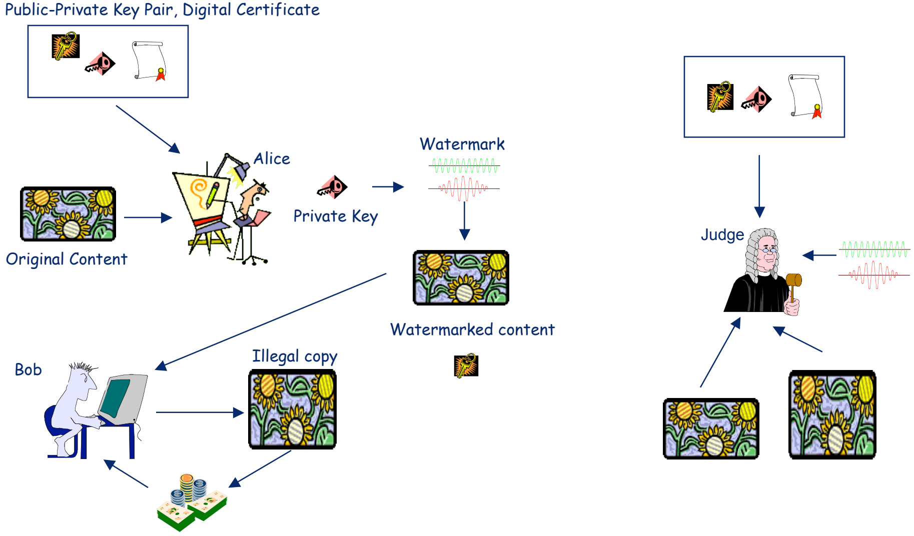
Why Hide?

- 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 (ownership and tracking information)

Applications of Information Hiding

- Ownership assertion.
- Fingerprinting (traitor tracking).
- Copy prevention or control (DVD).
- Authentication (original vs. forgery).
- Broadcast Monitoring (Gibson, Pattern Recognition)
- Media Bridging
- Meta data hiding (tracking information)
- Covert communication
- Steganographic file systems

Ownership Assertion



Public-Private Key Pair, Digital Certificate

Alice

Watermark

Private Key

Original Content

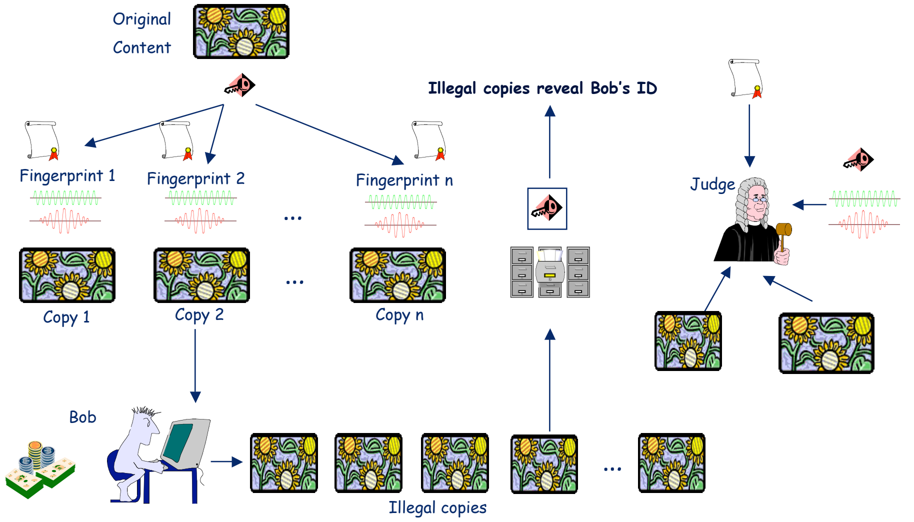
Judge

Watermarked content

Bob

Illegal copy

Fingerprinting



Original Content

Illegal copies reveal Bob's ID

Fingerprint 1

Fingerprint 2

…

Fingerprint n

Judge

Copy 1

Copy 2

…

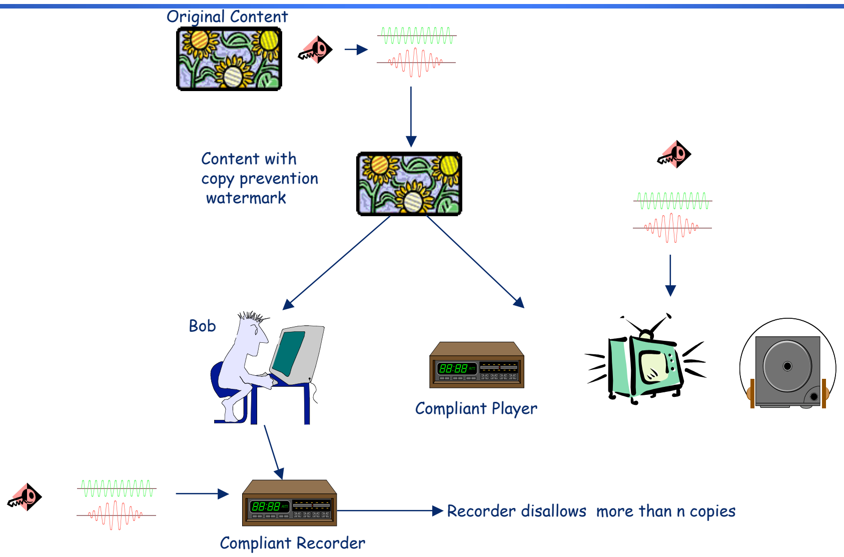
Copy n

Bob

…

Illegal copies

Copy Prevention and Control



Original Content

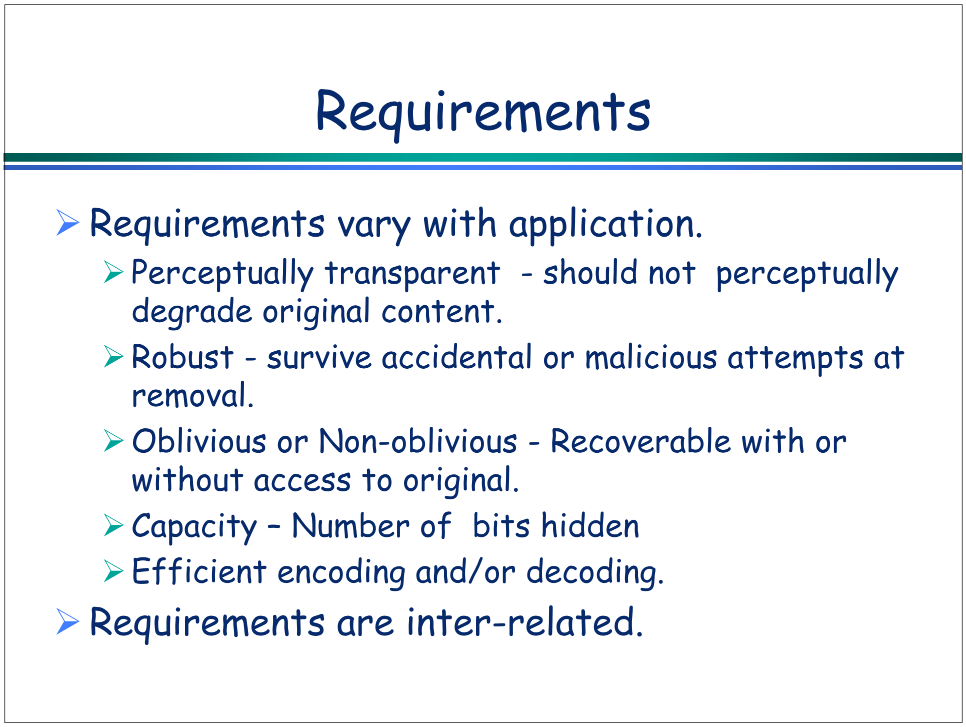
Content with copy prevention watermark

Bob

Compliant Player

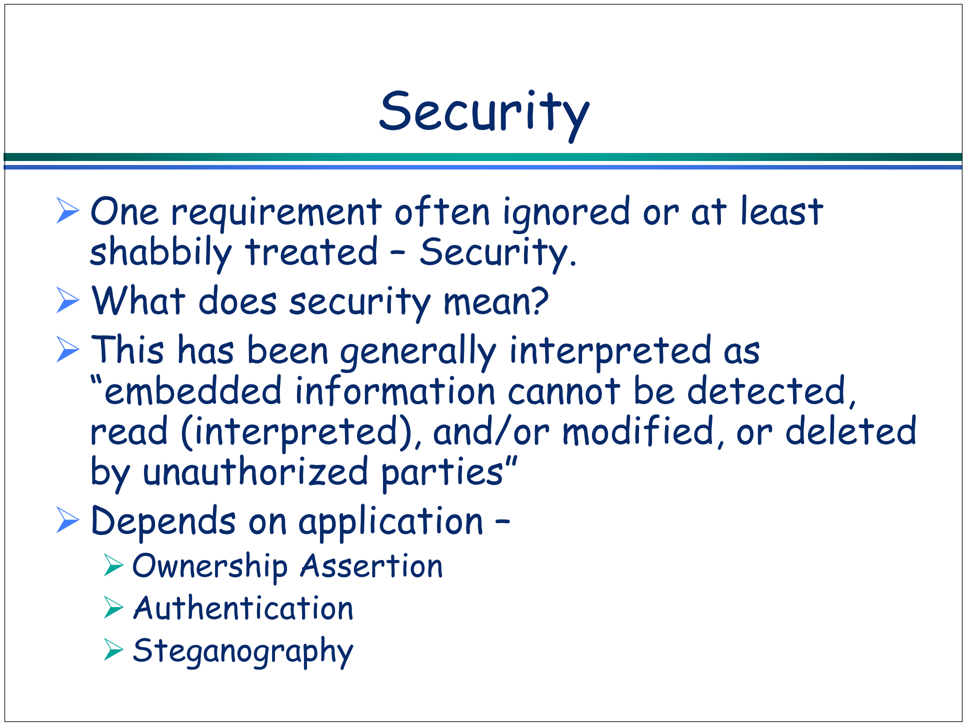
Compliant Recorder

Recorder disallows more than n copies



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

Attacks

- Steganography:
  - Detect stego (carrier) objects
  - Remove the message
  - Read the message (easy if we have know/have which method was used to embed the message)
  - Password attack – guess password/key
- Watermarks:
  - Copy objects
  - Remove/distort watermarks
  - Replace/overwrite watermarks

Assignment

- Read:
  - P. Moulin & R. Koetter, "Data Hiding Codes".
  - F.A. Petitcolas, R.J. Anderson, and M.G. Kuhn, "Information Hiding—A Survey", Proc. of IEEE, 87:1062-1078, 1999.
  - G.J. Simmons, "The History of Subliminal Channels", IEEE J. on Selected Areas in Communications, 16:452-462, 1998.