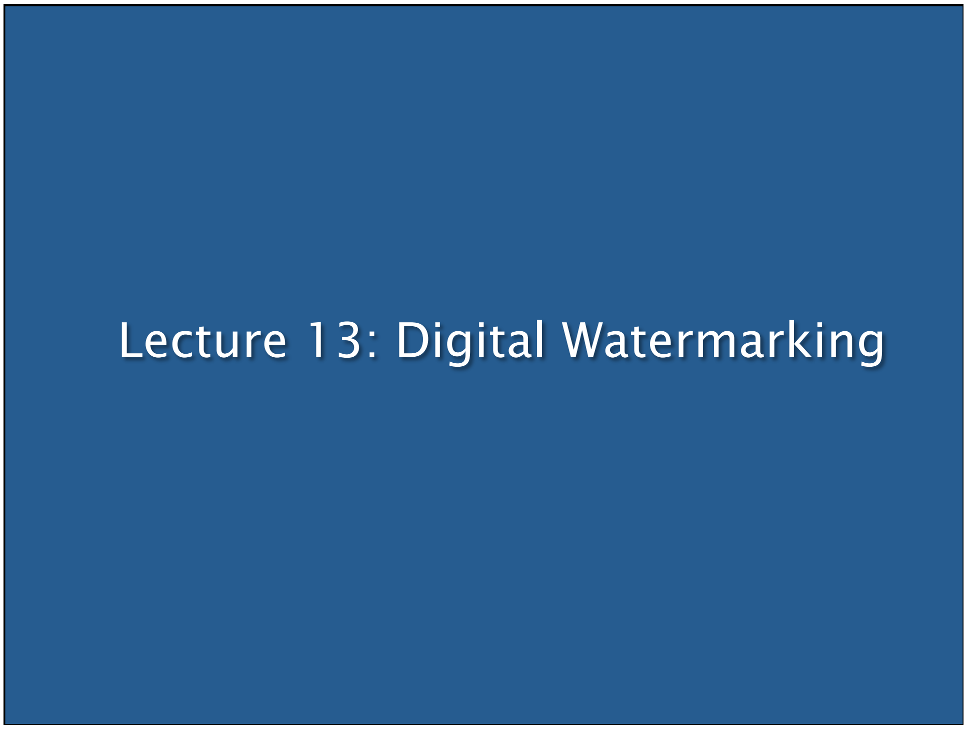
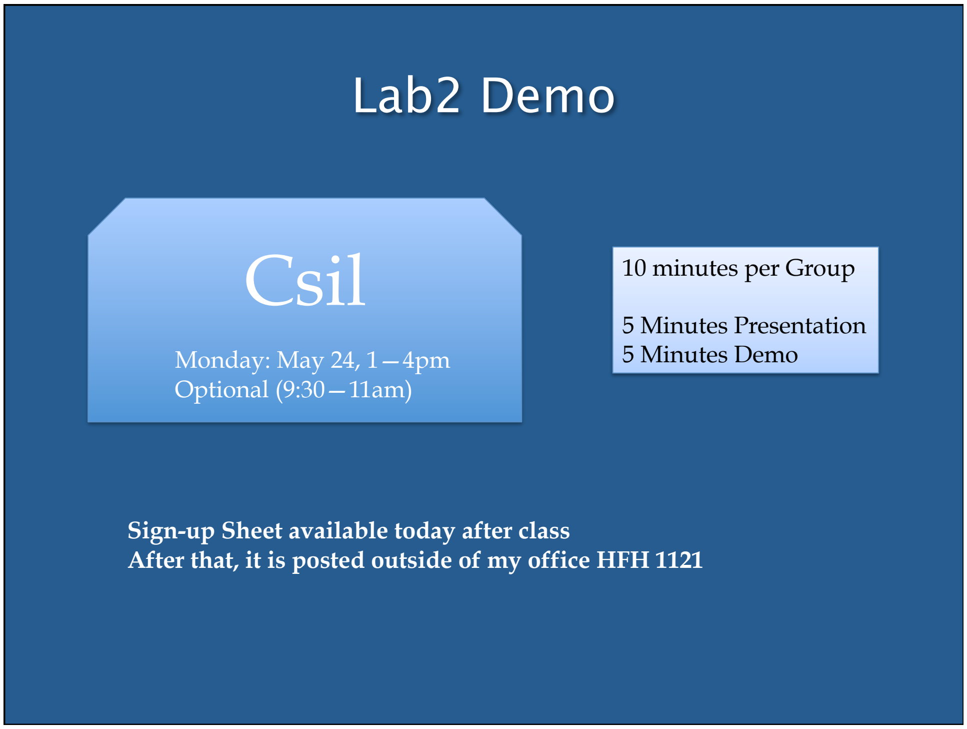


Lecture 13: Digital Watermarking



Lab2 Demo

Csil

Monday: May 24, 1 – 4pm
Optional (9:30 – 11am)

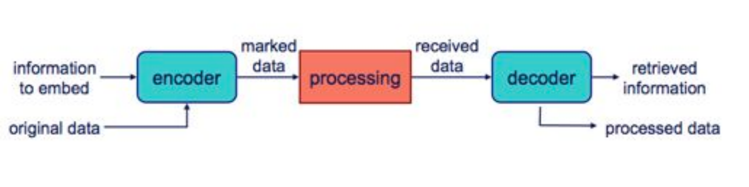
10 minutes per Group

5 Minutes Presentation
5 Minutes Demo

Sign-up Sheet available today after class
After that, it is posted outside of my office HFH 1121

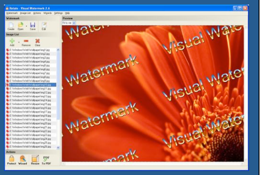
Information Hiding

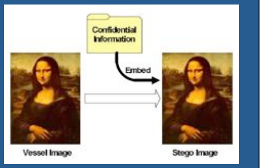
- Communication of information by embedding it in and retrieving it from other digital data.
- Depending on application we may need process to be imperceptible, robust, secure. Etc.



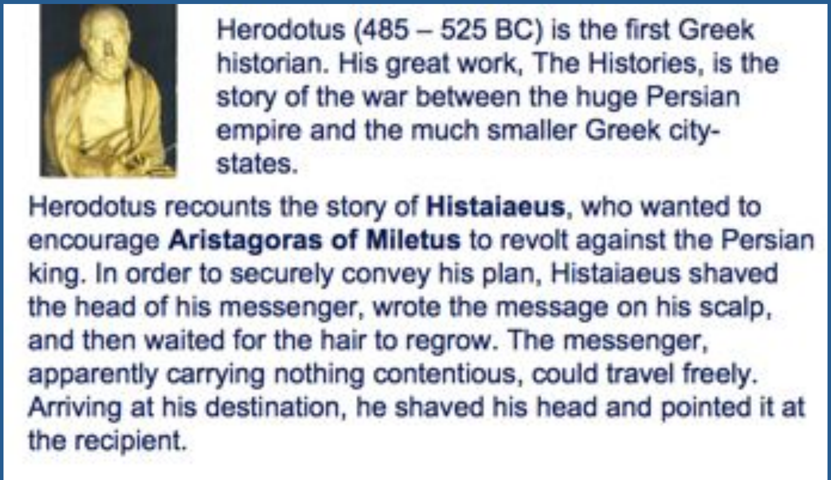
Why?

- Because you want to protect it from malicious use
  - 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





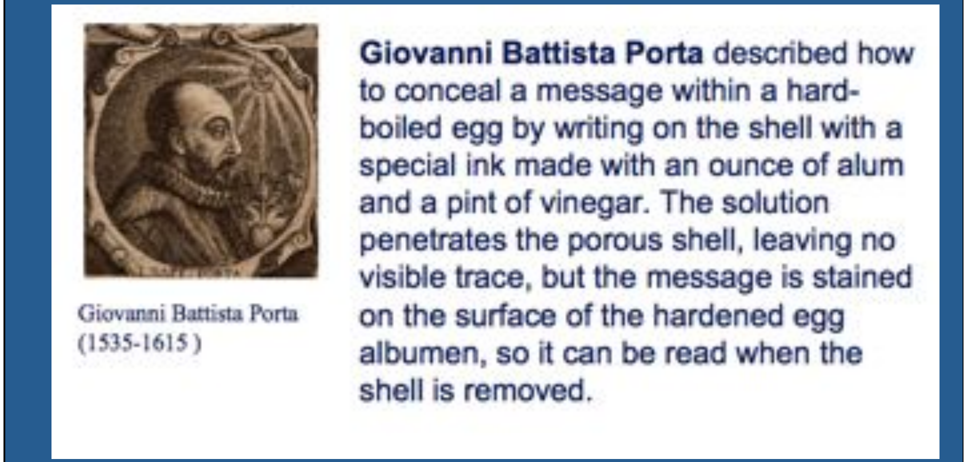
Ancient Steganography



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 regrow. The messenger, apparently carrying nothing contentious, could travel freely. Arriving at his destination, he shaved his head and pointed it at the recipient.

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.

Fundamental Issues

- **Fidelity**
  - The degree of perceptual degradation due to embedding operation.
- **Robustness**
  - The level of immunity against all forms of manipulation (intentional and non-intentional attacks).
- **Payload**
  - The amount of message signal that can be reliably embedded and extracted (subject to perceptual constraints at the designated level of robustness).
- **Security**
  - Perhaps the most misunderstood and ignored issue. Meaning of security depends on the application as we shall see later.

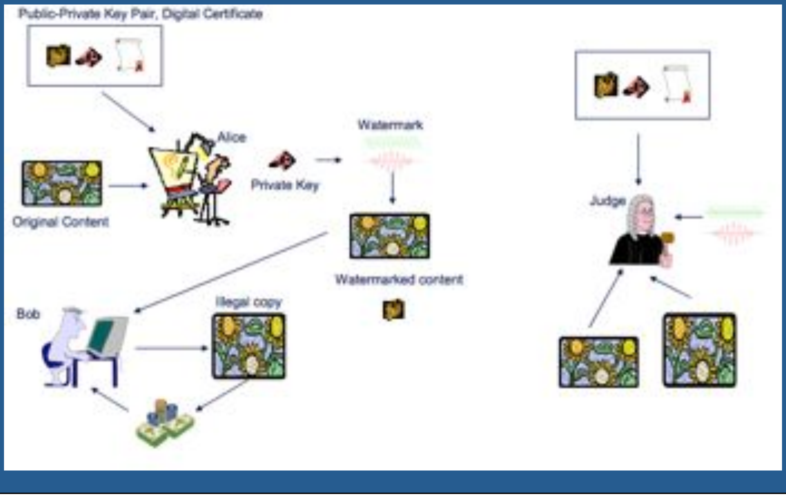
DIGITAL WATERMARKS

What is a Watermark?

- A watermark is a “secret message” that is embedded into a “cover message”
- Usually, only the knowledge of a secret key allows us to extract the watermark.
- Has a mathematical property that allows us to argue that its presence is the result of deliberate actions.
- Effectiveness of a watermark is a function of its
  - Stealth
  - Resilience
  - Capacity

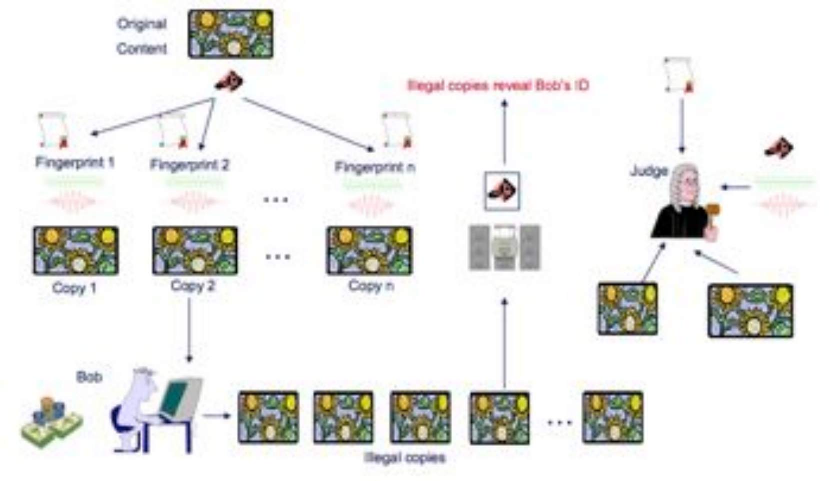
Usage Scenarios (1)

- Ownership assertion



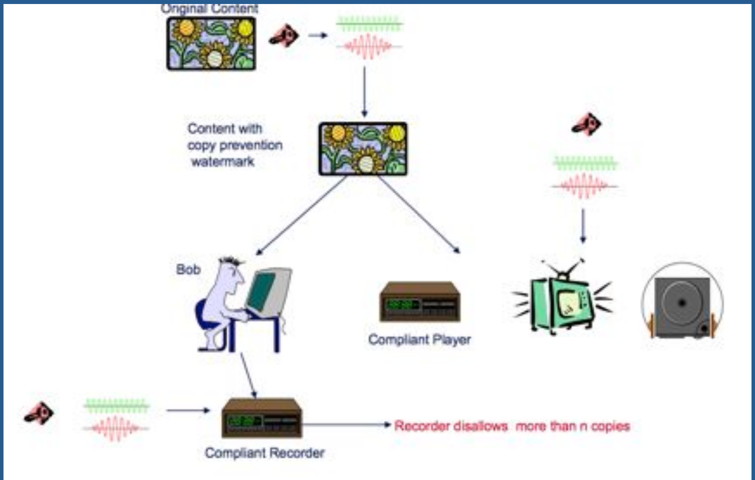
Usage Scenarios (2)

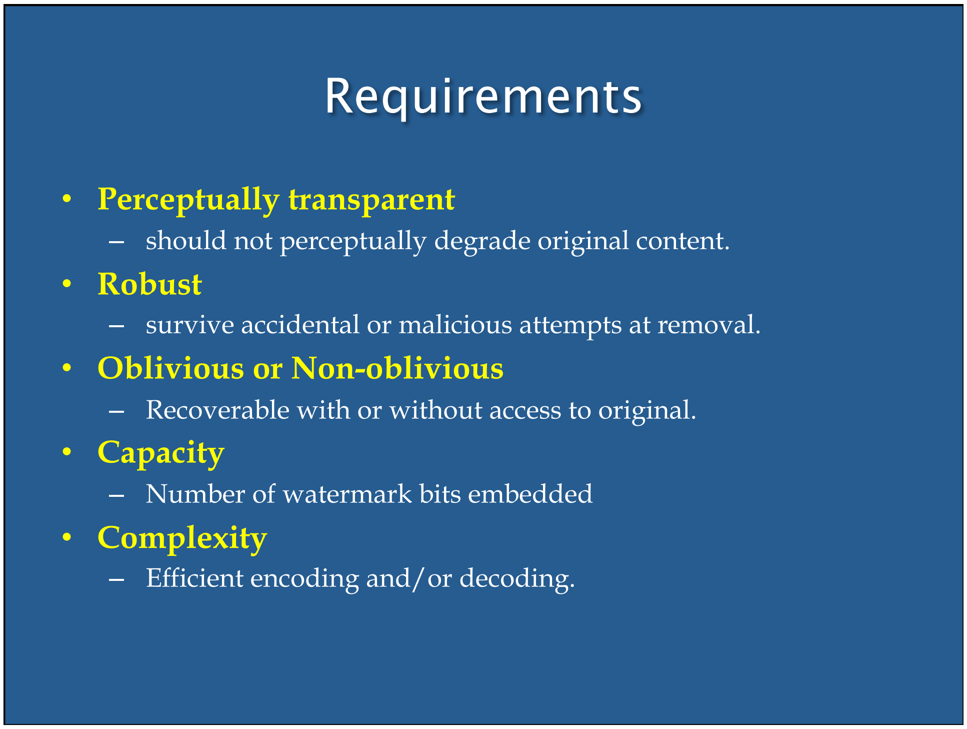
- Fingerprinting



Usage Scenario (3)

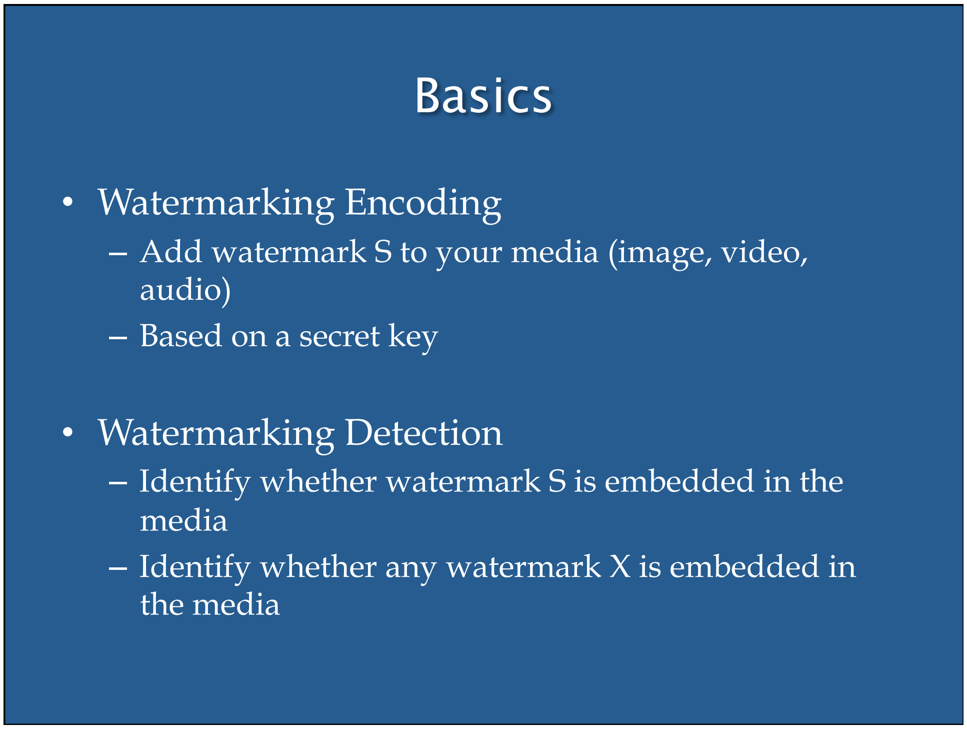
Copy Prevention or Control


Original Content
Content with copy prevention watermark
Bob
Compliant Player
Compliant Recorder
Recorder disallows more than n copies



Requirements

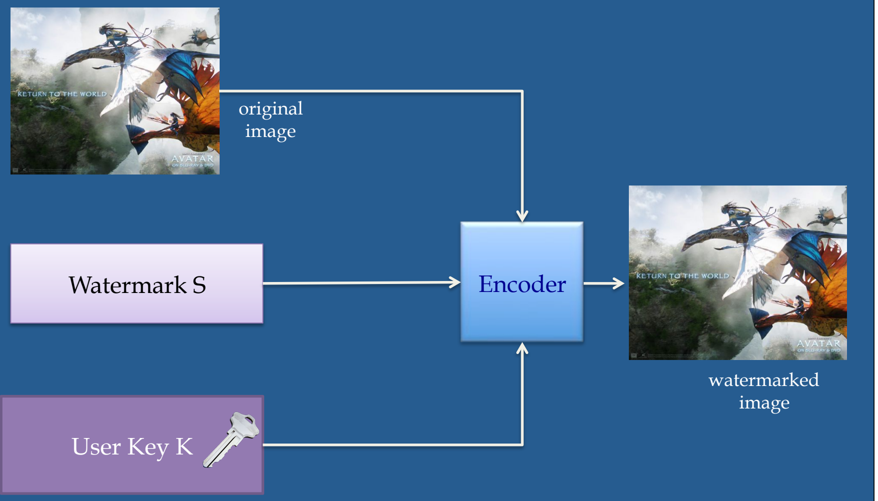
- **Perceptually transparent**
  - should not perceptually degrade original content.
- **Robust**
  - survive accidental or malicious attempts at removal.
- **Oblivious or Non-oblivious**
  - Recoverable with or without access to original.
- **Capacity**
  - Number of watermark bits embedded
- **Complexity**
  - Efficient encoding and/or decoding.



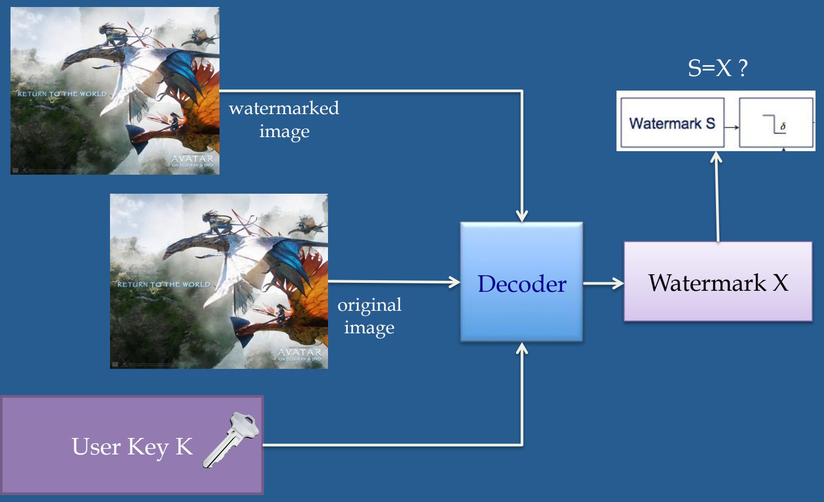
Basics

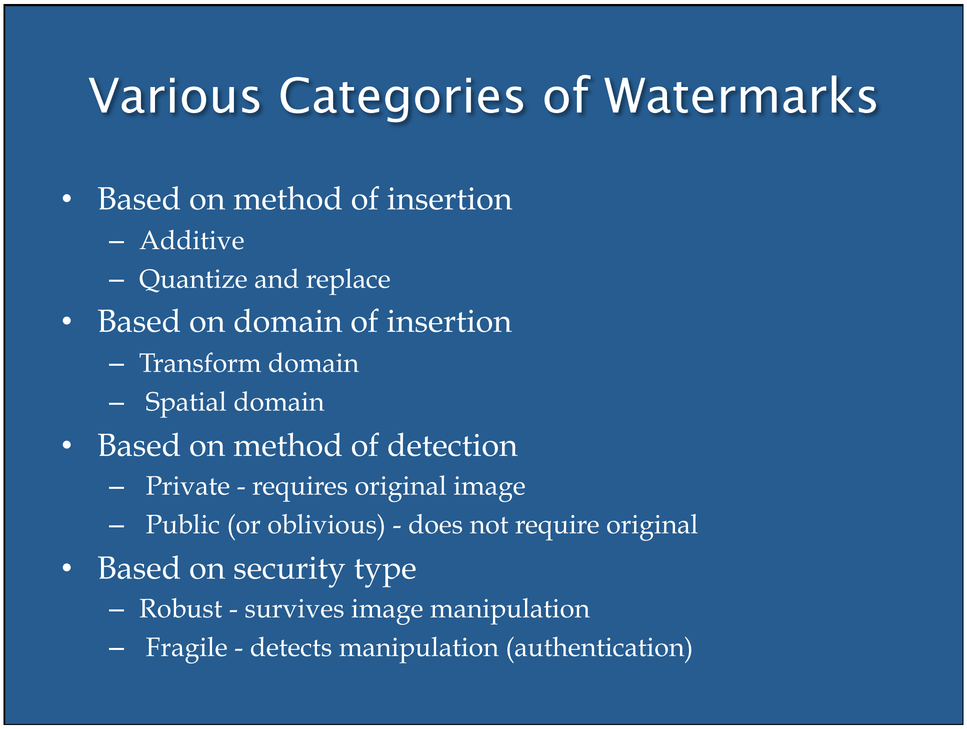
- Watermarking Encoding
  - Add watermark S to your media (image, video, audio)
  - Based on a secret key
- Watermarking Detection
  - Identify whether watermark S is embedded in the media
  - Identify whether any watermark X is embedded in the media

Watermarking Encoding



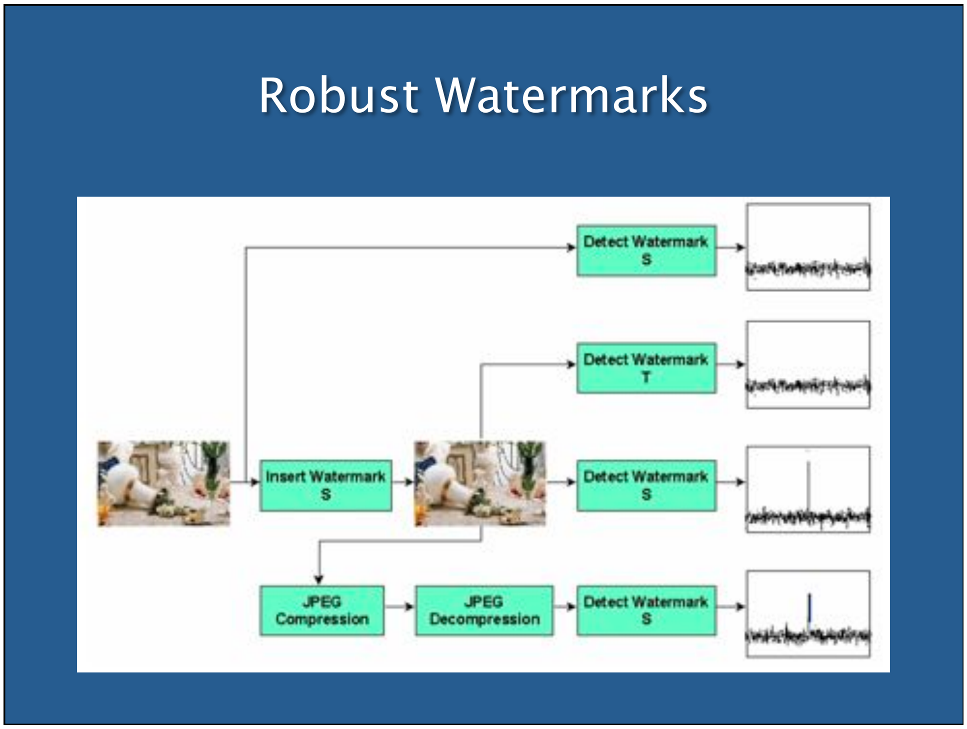
Watermarking Decoding





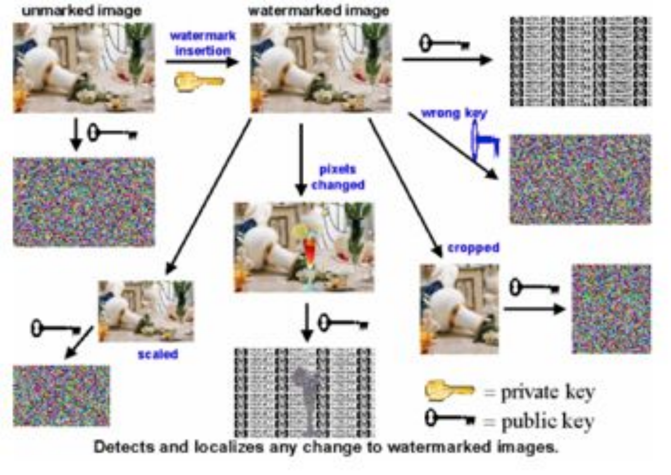
Various Categories of Watermarks

- Based on method of insertion
  - Additive
  - Quantize and replace
- Based on domain of insertion
  - Transform domain
  - Spatial domain
- Based on method of detection
  - Private - requires original image
  - Public (or oblivious) - does not require original
- Based on security type
  - Robust - survives image manipulation
  - Fragile - detects manipulation (authentication)



Robust Watermarks

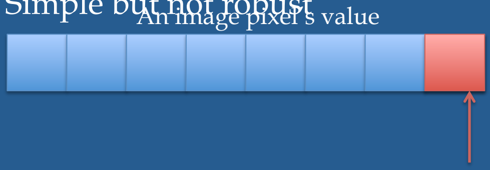
Fragile Watermarks



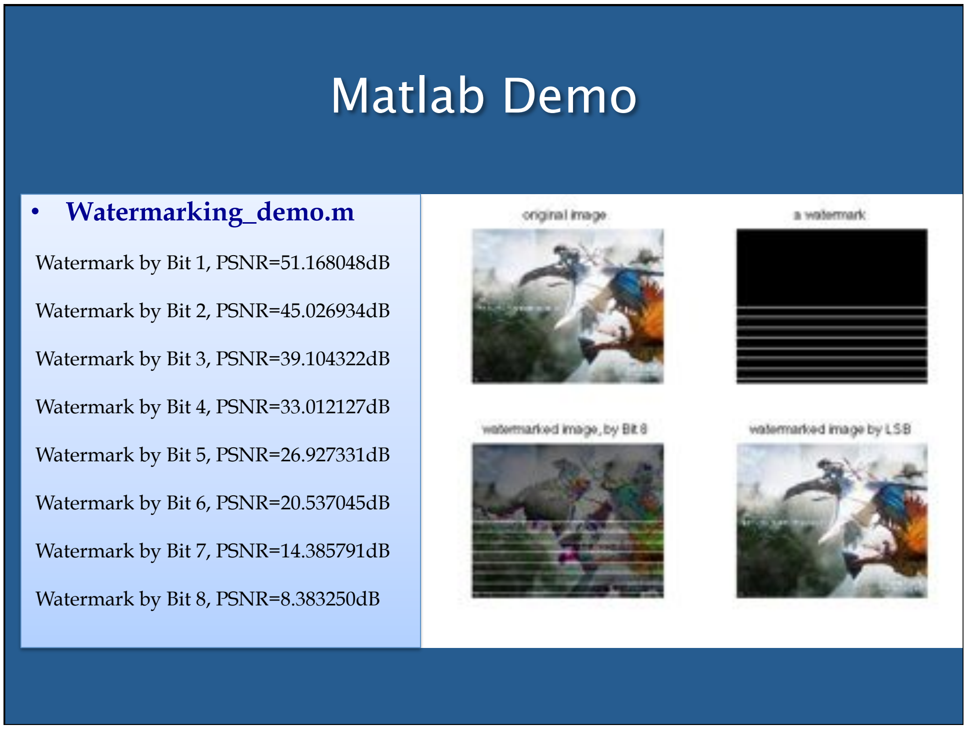
Detects and localizes any change to watermarked images.

Embedding Watermarks

- Method 1:
  - Spatial Domain Least Significant Bit (LSB) Modification
  - Simple but not robust



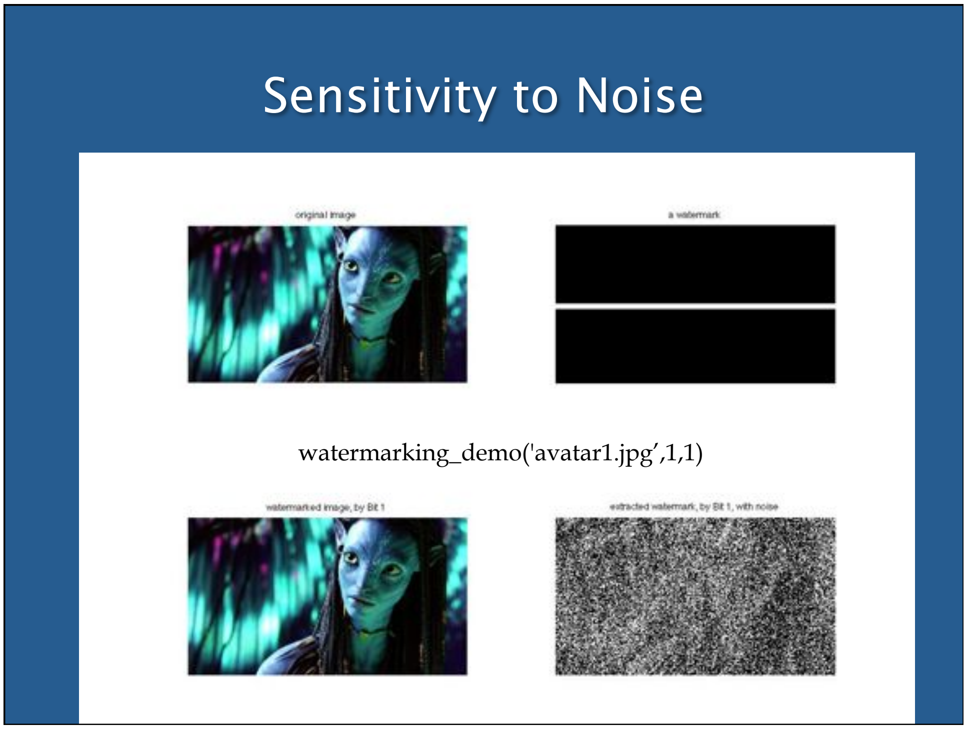
Replace the bit with your watermark pixel value (0 or 1)



Matlab Demo

- **Watermarking_demo.m**

```
Watermark by Bit 1, PSNR=51.168048dB
Watermark by Bit 2, PSNR=45.026934dB
Watermark by Bit 3, PSNR=39.104322dB
Watermark by Bit 4, PSNR=33.012127dB
Watermark by Bit 5, PSNR=26.927331dB
Watermark by Bit 6, PSNR=20.537045dB
Watermark by Bit 7, PSNR=14.385791dB
Watermark by Bit 8, PSNR=8.383250dB
```

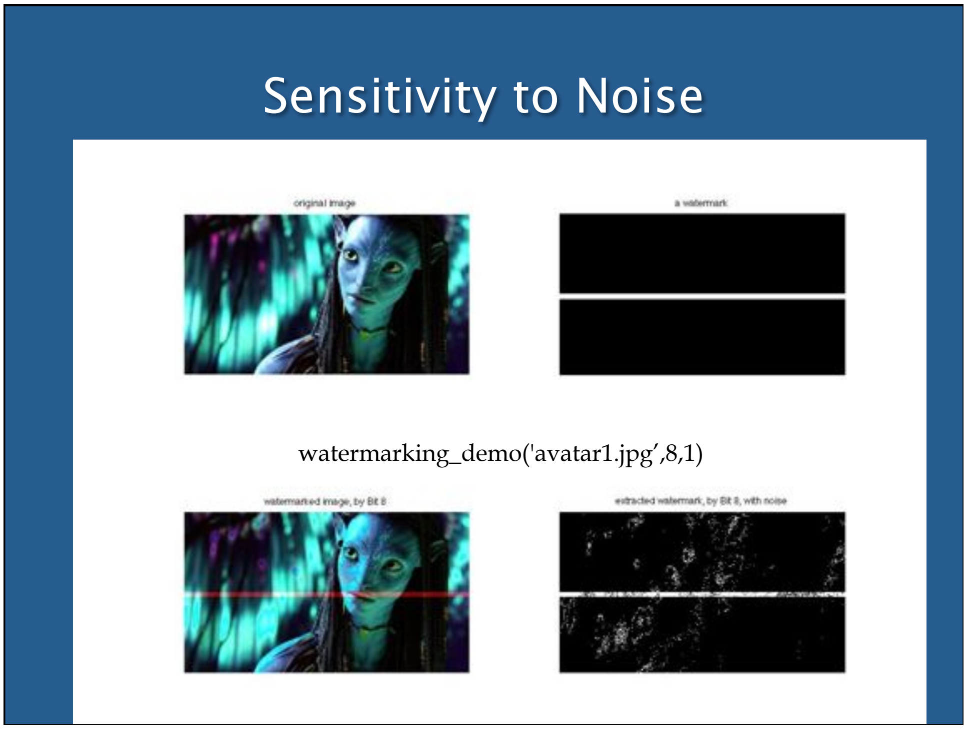


Sensitivity to Noise

original image
a watermark

```
watermarking_demo('avatar1.jpg’,1,1)
```

watermarked image, by Bit 1
extracted watermark, by Bit 1, with noise

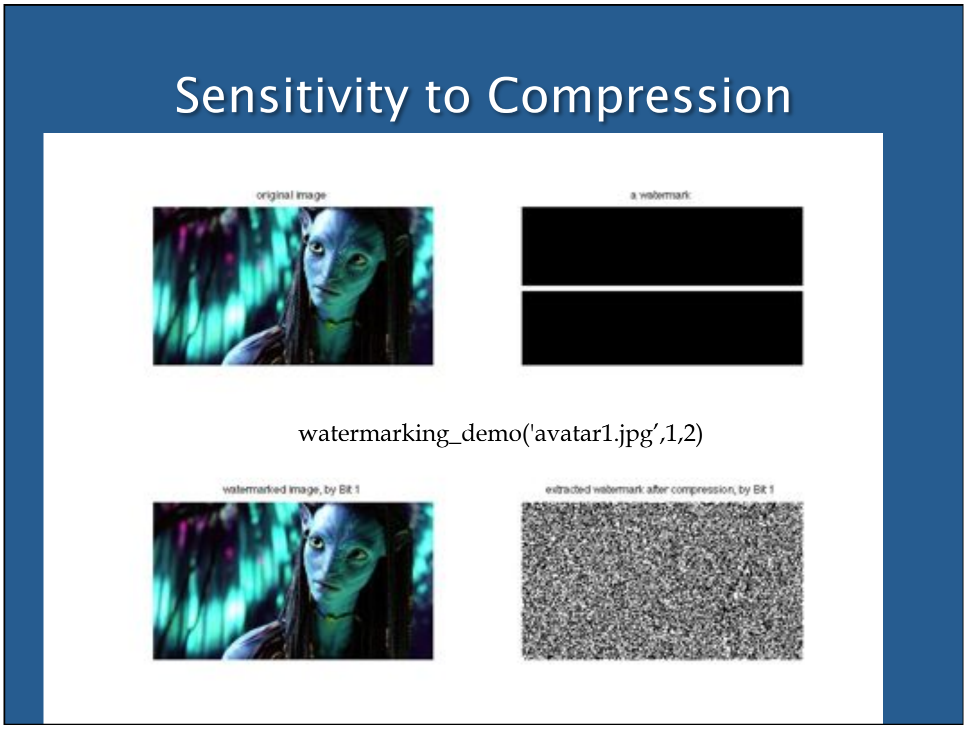


Sensitivity to Noise

original image
a watermark

```
watermarking_demo('avatar1.jpg',8,1)
```

watermarked image, by Bit 8
extracted watermark, by Bit 8, with noise

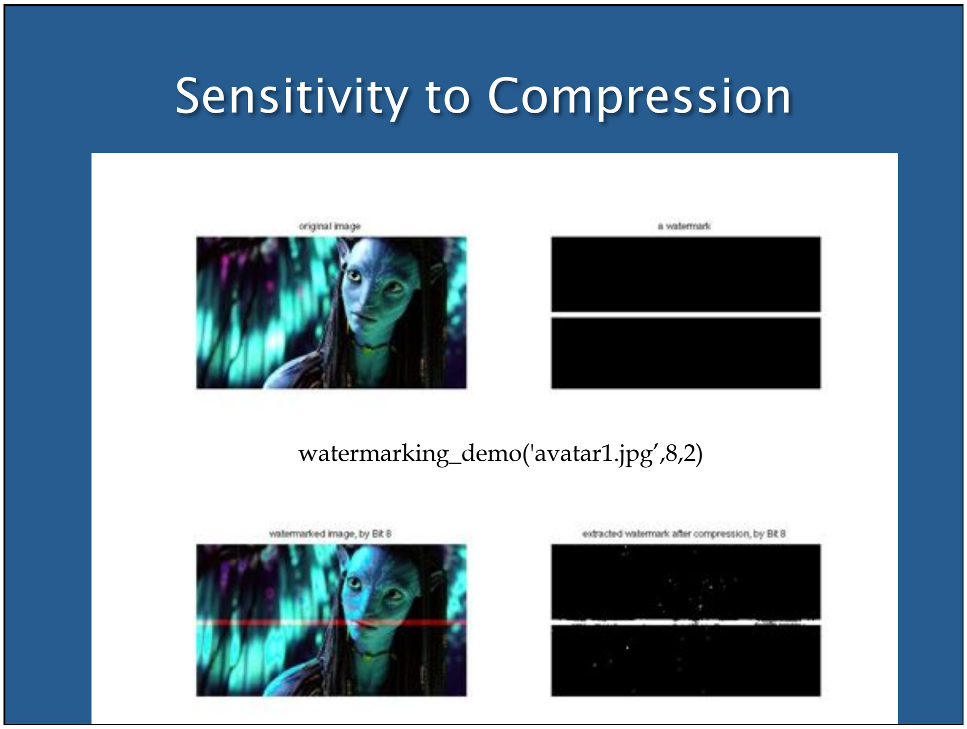


Sensitivity to Compression

original image
a watermark

```
watermarking_demo('avatar1.jpg',1,2)
```

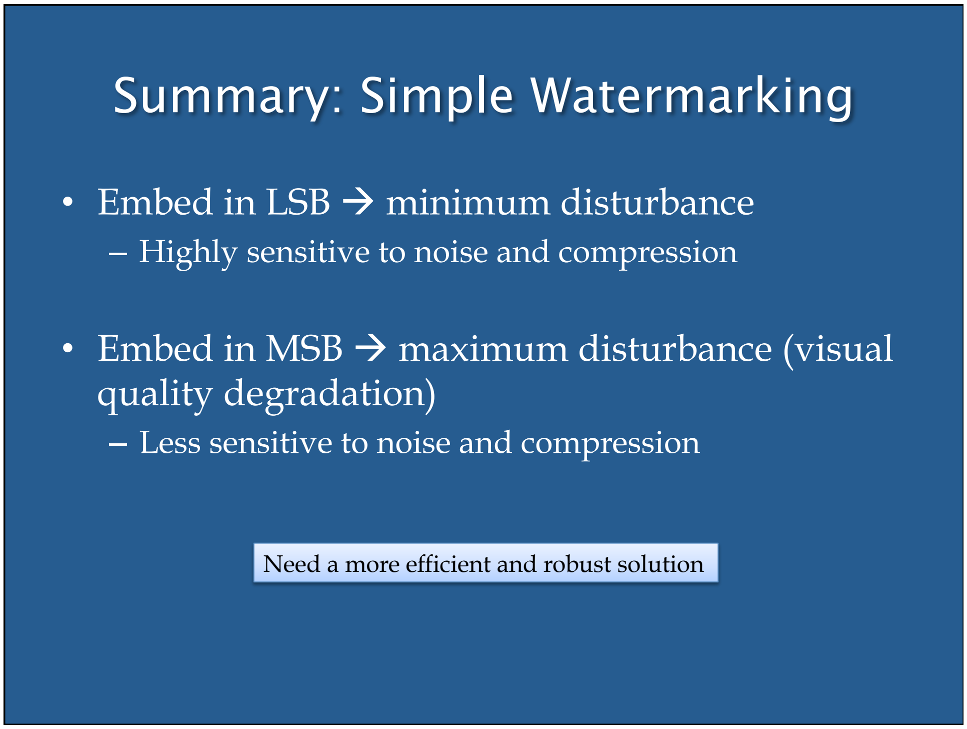
watermarked image, by Bit 1
extracted watermark after compression, by Bit 1



Sensitivity to Compression

original image
a watermark
watermarked image, by Bit 8
extracted watermark after compression, by Bit 8

```
watermarking_demo('avatar1.jpg’,8,2)
```

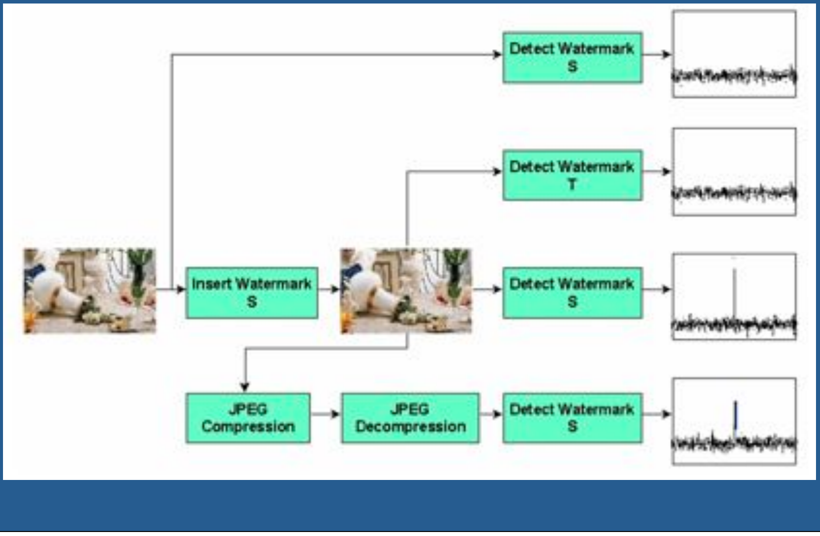


Summary: Simple Watermarking

- Embed in LSB → minimum disturbance
  - Highly sensitive to noise and compression
- Embed in MSB → maximum disturbance (visual quality degradation)
  - Less sensitive to noise and compression

Need a more efficient and robust solution

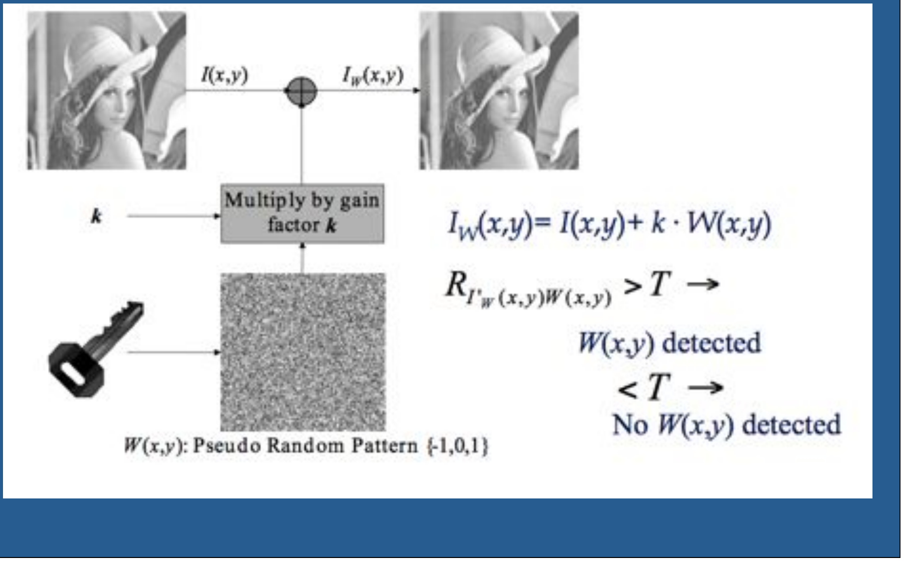
Robust Watermarks



Spatial Domain Robust Watermarking

- Pseudo-randomly (based on secret key) select n pairs of pixels:
  - pair i: a_i, b_i are the values of the pixels in the pair
  - The expected value of $\text{sum}_i\ (a_i - b_i) == 0$
- Increase a_i by 1, Decrease b_i by 1
  - The expected value of $\text{sum}_i\ (a_i - b_i)$ now →2n
- To detect watermark, check $\text{sum}_i\ (a_i - b_i)$ on the watermarked image

Spatial with Correlation (Chapter 13, 2.4.2)


$I(x,y)$
$I_W(x,y)$
k
Multiply by gain factor k
$W(x,y)$: Pseudo Random Pattern {-1,0,1}

$I_W(x,y) = I(x,y) + k \cdot W(x,y)$

$R_{I'_W(x,y)W(x,y)} > T \rightarrow$ $W(x,y)$ detected

$< T \rightarrow$ No $W(x,y)$ detected

Matlab Demo (robust_watermarking_demo.m)

```
--------------------------------------------
After embedding the watermark, PSNR=68.342274dB
--------------------------------------------

original image, sum (a-b)/n=5.76467

watermarked image, sum (a-b)/n=8.22100

watermarked image with noise, sum (a-b)/n=29.77467

watermarked image with compression, sum (a-b)/n=7.57200

--------------------------------------------
watermarked image, with a different k sum (a-b)/n=5.23767
```

What You Should Know

- The basic concept of data hiding
- What is a watermark
  - Types of watermark
  - Usage scenarios of watermark
- How to embed a watermark, and extract a watermark

Lab2 Demo

Csil

Monday: May 24, 1 – 4pm
Optional (9:30 – 11am)

10 minutes per Group

5 Minutes Presentation
5 Minutes Demo

Sign-up Sheet available today after class
After that, it is posted outside of my office HFH 1121