Scene Adaptive Video Watermarking

Edward J. Delp

Purdue University
School of Electrical and Computer Engineering
Purdue Multimedia Testbed
Video and Image Processing Laboratory (*VIPER)*
West Lafayette, IN 47907-1285
+1 765 494 1740
+1 765 494 0880 (fax)
email: ace@ecn.purdue.edu
http://www.ece.purdue.edu/~ace

Multimedia Security

- “Everything” is digital these days - a copy of a digital media element is identical to the original
- How can an owner protect their content?
- Are images still “fossilized light”?
- What does all of this mean in terms of law?
- Does any security system really work or does it just make us feel good!

What Do We Want From a Security System?

- **Access Control**
- **Copy Control** Þ

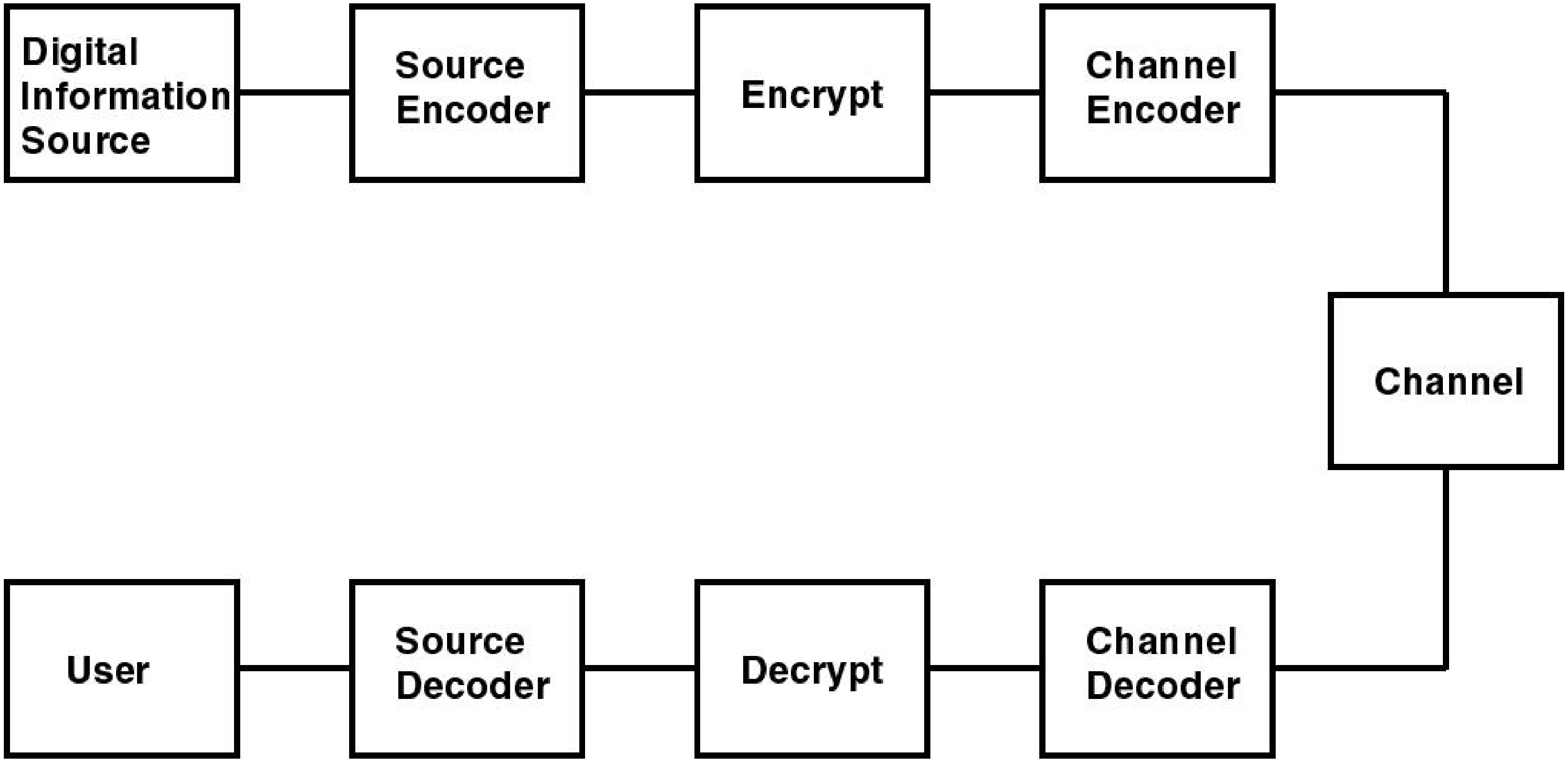
Playback Control

Record Control

Generation Control

- **Auditing (fingerprinting)**
  - **Who did what and when?**

Digital Communication System



What is Watermarking?

- The use of a perceptually invisible authentication technique
  - “controlled” distortion is introduced in a multimedia element
- Visible watermarks also exists

Media Elements

- Audio
- Video
- Documents (including HTML documents)
- Images
- Graphics
- Graphic or Scene Models
- Programs (executable code)

Watermarking Scenario

- Scenario
  - an owner places digital images on a network server and wants to “protect” the images
- Goals
  - verify the owner of a digital image
  - detect forgeries of an original image
  - identify illegal copies of the image
  - prevent unauthorized distribution

Where are Watermarks Used?

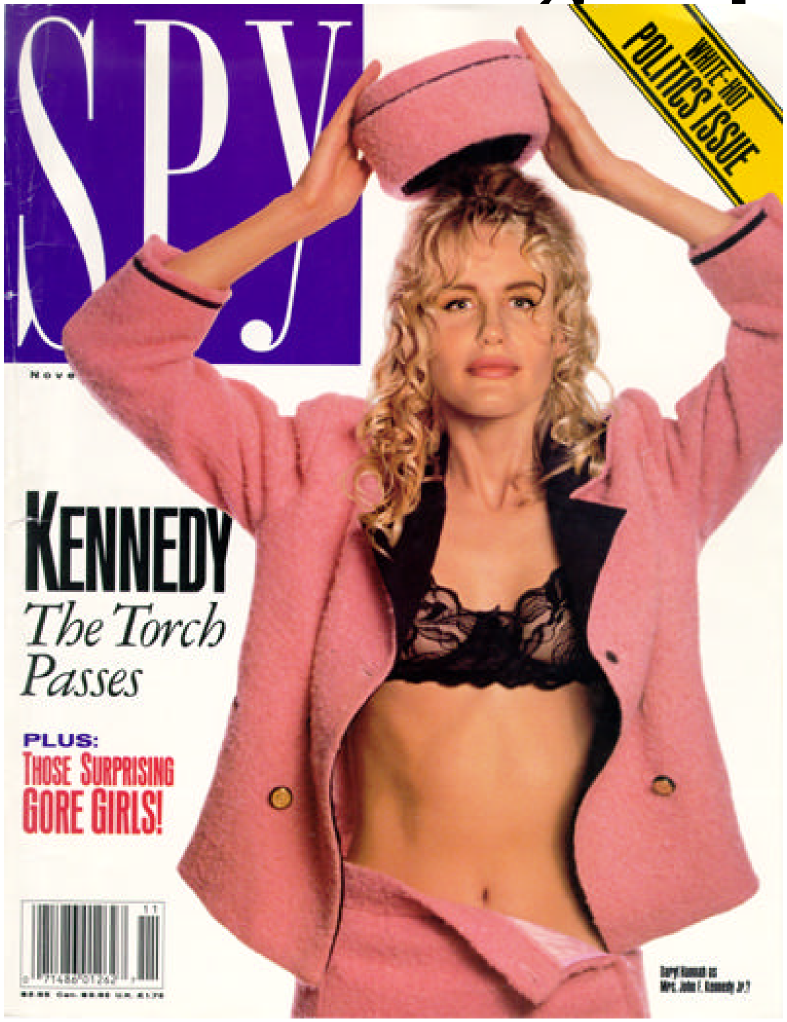
- **Watermarks have been used or proposed in:**
  - **digital cameras**
  - **DVD video**
  - **audio (SDMI)**
  - **broadcast video (in US - ATSC)**
    - **visible watermarks now used**
  - **“binding” mechanism in media databases**
  - **key distribution systems**
  - **preventing forgery of bank notes**

Usually as secondary security Þ conversion to “analog”

Multimedia Security - Tools Set

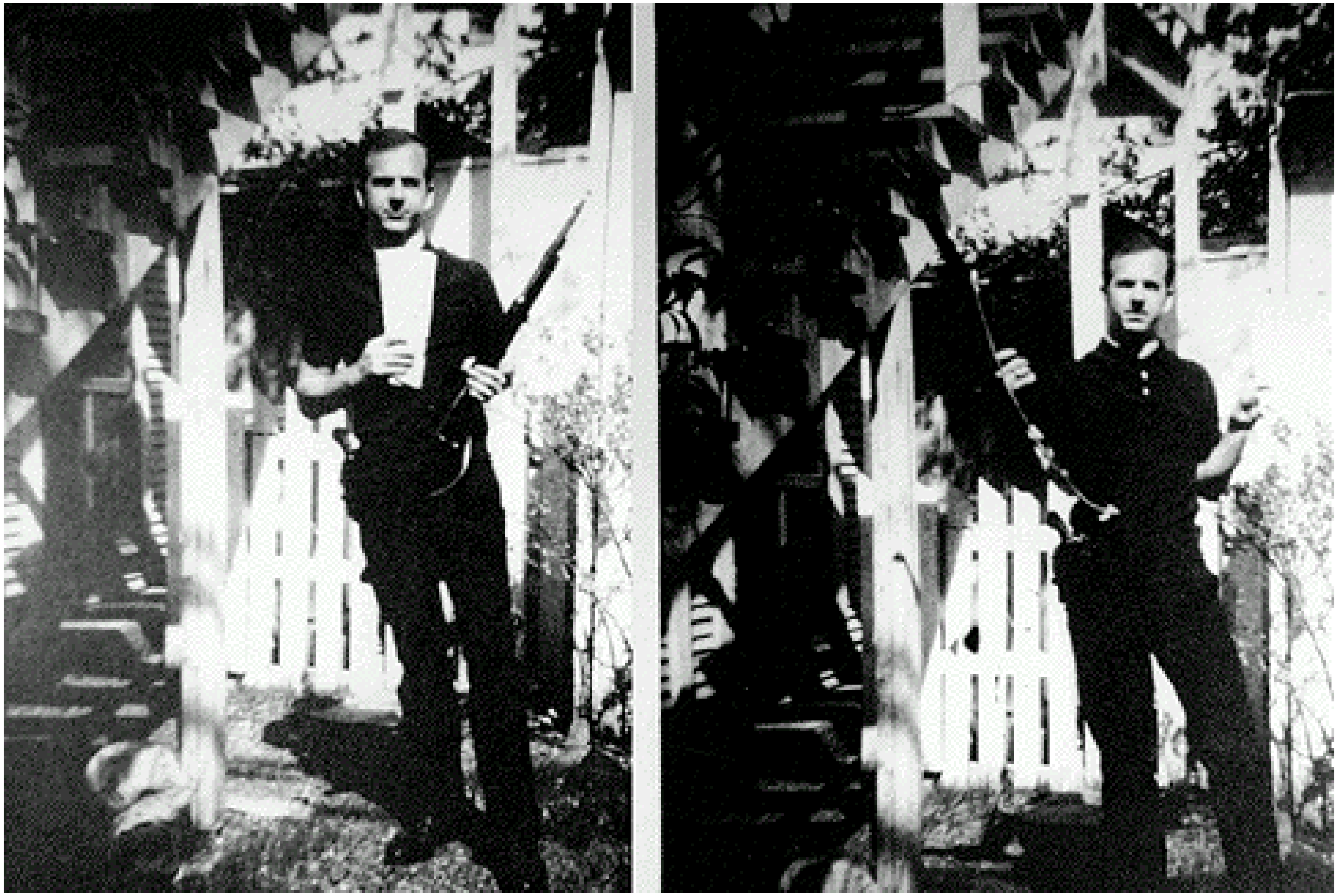
- **Encryption**
- **Authentication**
- **Hashing**
- **Time-stamping**
- **Watermarking**

Why is Watermarking Important?

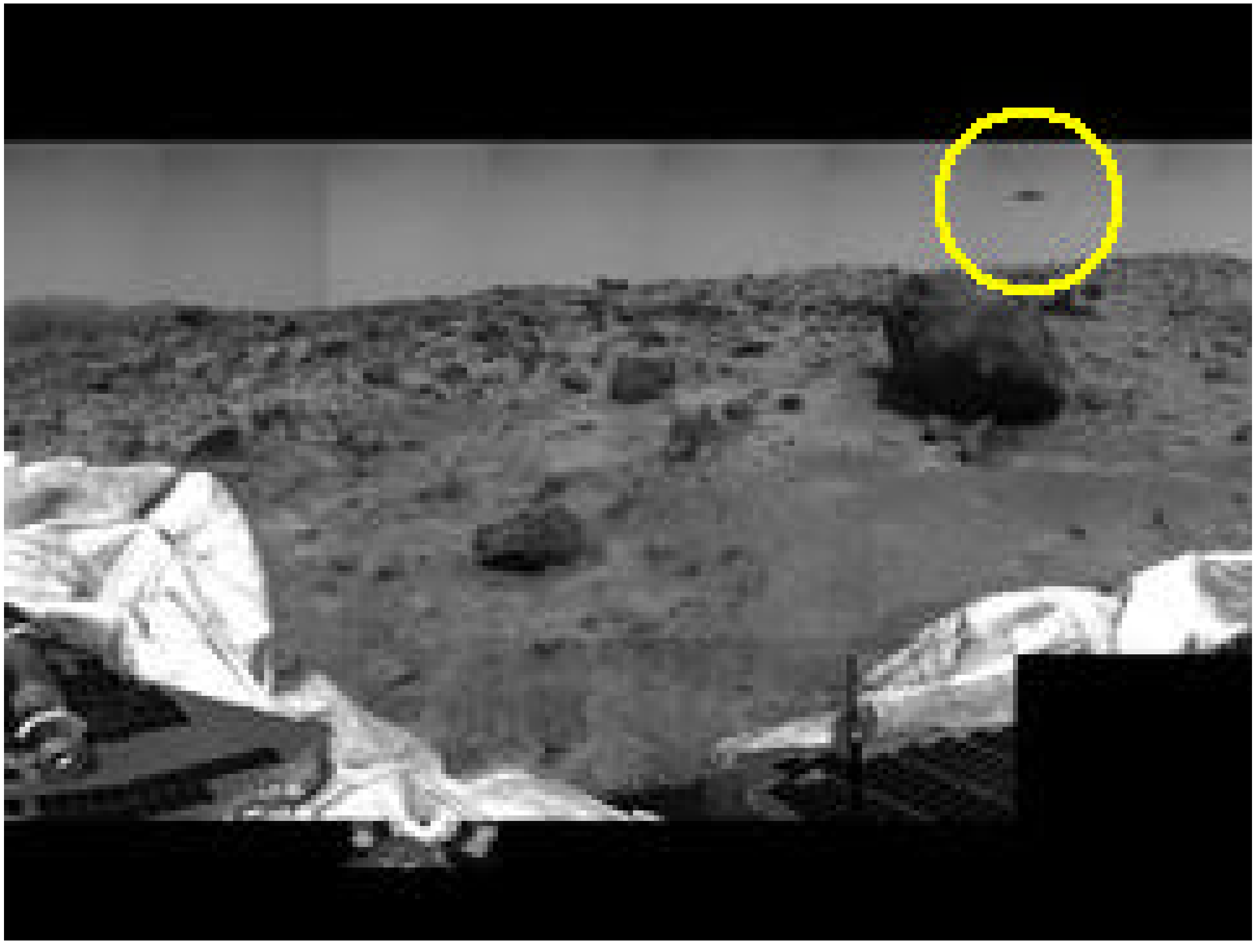


Why is Watermarking Important?

Why Watermarking is Important?

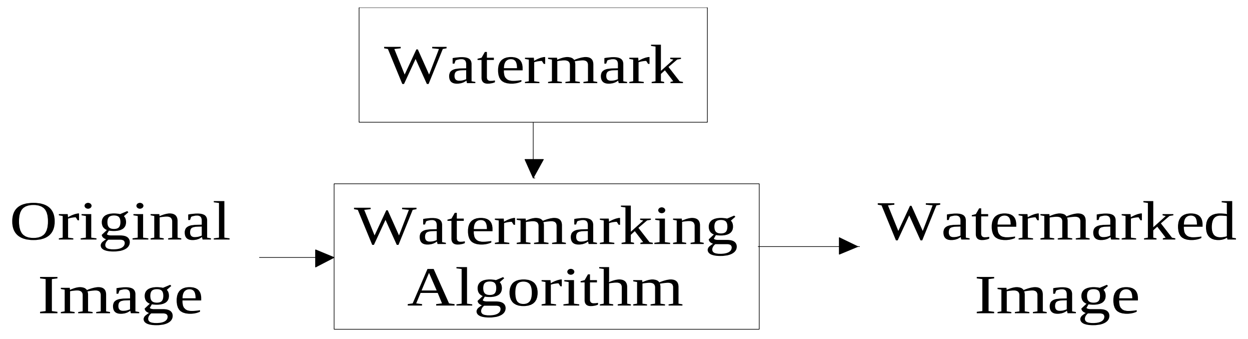


Why is Watermarking Important?



A Overview of Watermarking Techniques

- Spatial watermarking
- Spatial Frequency (DCT or wavelet) watermarking
- Visible watermarks



Components of a Watermarking Technique

- The watermark, W
  - each owner has a unique watermark
- The marking algorithm
  - incorporates the watermark into the image
- Verification algorithm
  - an authentication procedure (determines the integrity / ownership of the image)

Main Principles

- **Transparency - the watermark is not visible in the image under typical viewing conditions**

- **Robustness to attacks - the watermark can still be detected after the image has undergone linear and/or nonlinear operations (this may *not* be a good property - *fragile watermarks*)**

- **Capacity - the technique is capable of allowing multiple watermarks to be inserted into the image with each watermark being independently verifiable**

Attacks

- Compression
- Filtering
- Printing and rescanning
- Geometric attacks - cropping, resampling, rotation
- Collusion - spatial and temporal
- Conversion to analog

Current Research Issues

- Theoretical Issues
  - capacity and performance bounds
  - models of the watermarking/detection process
- Robust Watermarks
  - linear vs. nonlinear
  - scaling and other geometric attacks
  - watermarking analog representations of content
  - new detection schemes
  - what should be embedded (watermark structure)

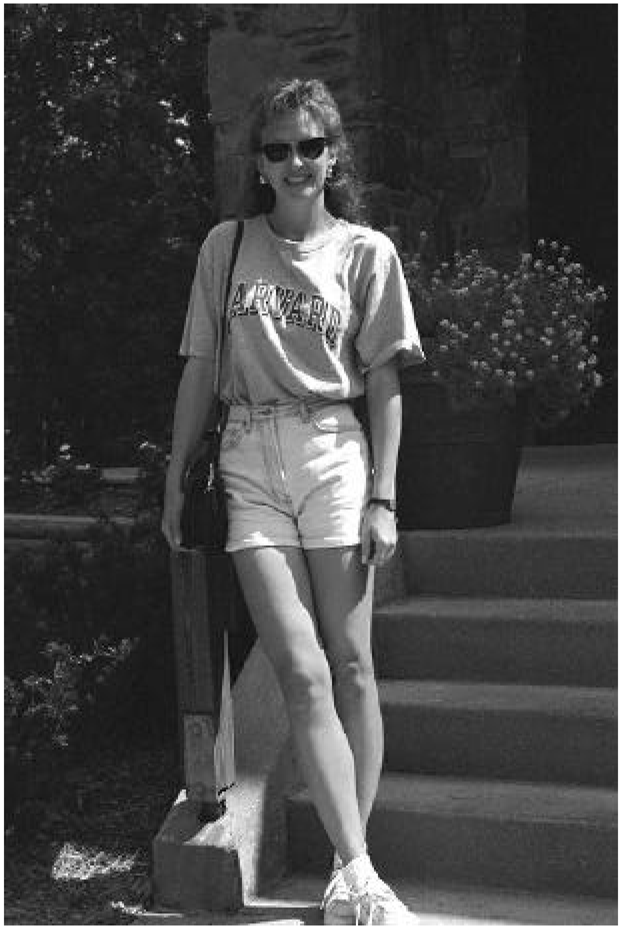
Research at Purdue

- **Fragile and semi-fragile watermarks for forensic imaging**
- **Extending concept of robust image adaptive watermarks to video**
  - **is there a temporal masking model that works?**

Original Image

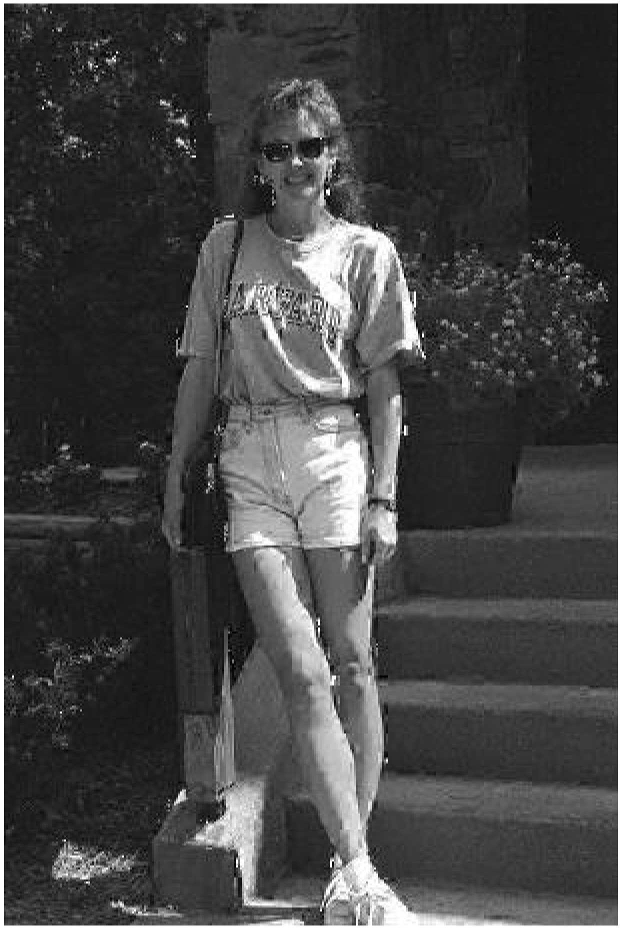
Fixed-length DCT Watermark

a = 0.1



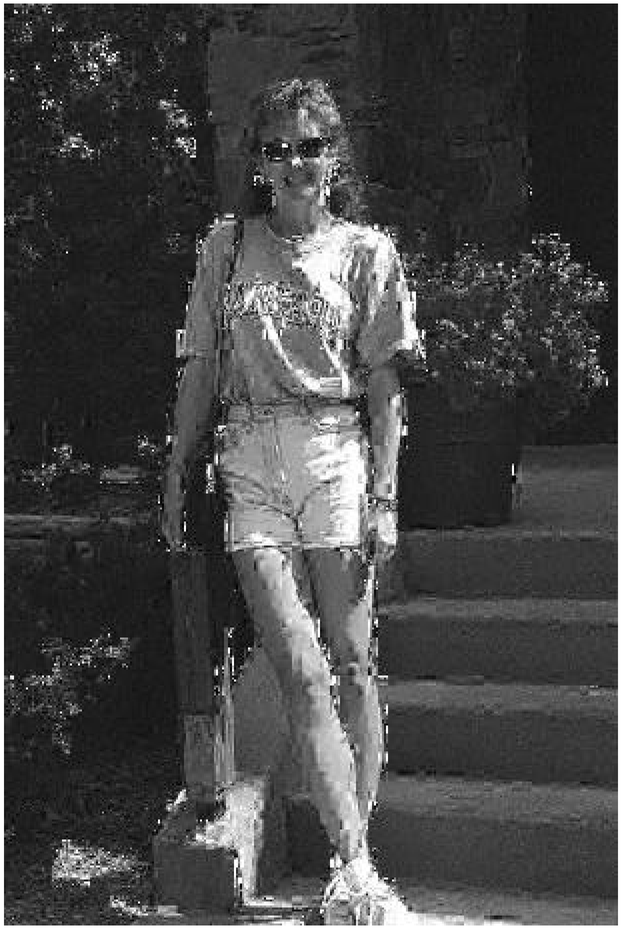
Fixed-length DCT Watermark

a = 0.5



Fixed-length DCT Watermark

a = 1.0



Fixed-length DCT Watermark

a = 5.0

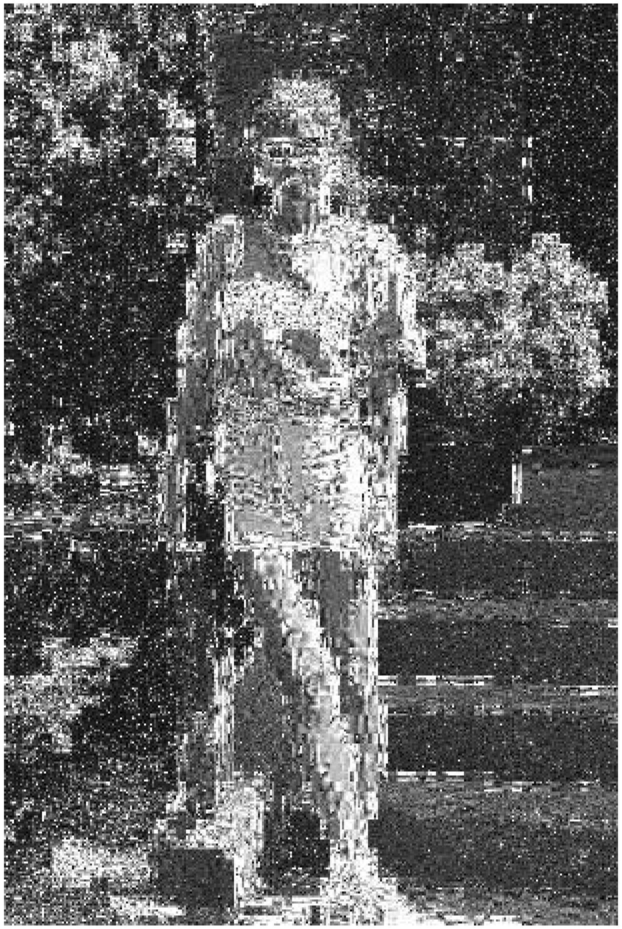


Image Adaptive Watermarks (DCT)

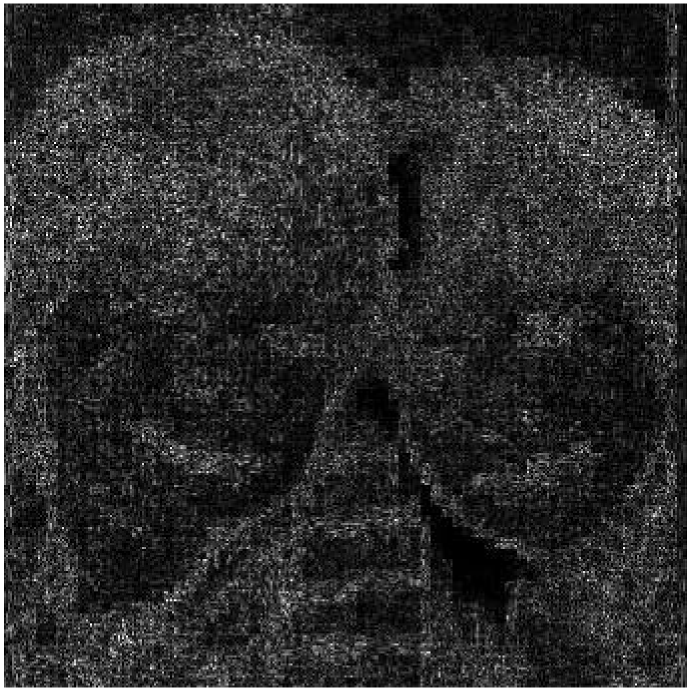
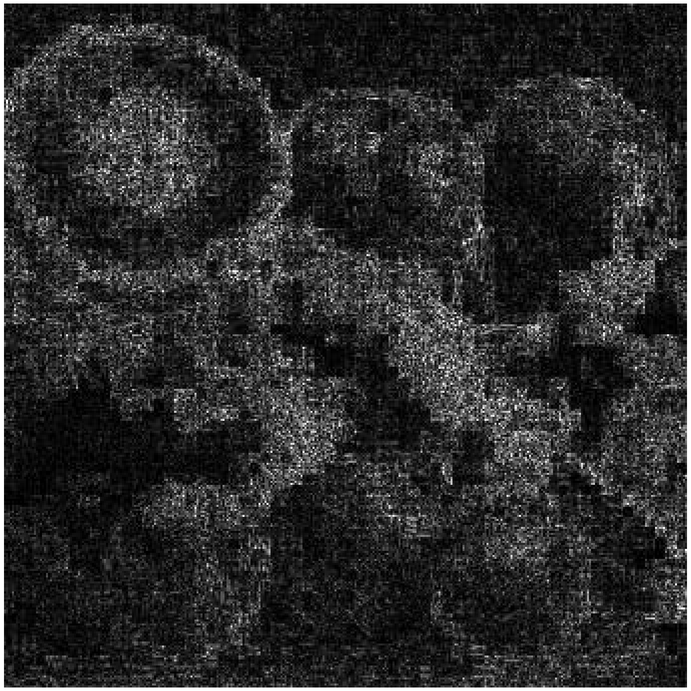


Image Adaptive Watermarks (DCT)



Project Goal

Development techniques for watermarking compressed and uncompressed video sequences that exploit the human vision system

Video Watermarking Issues

- A video sequence cannot simply be treated as an ordered collection of images:
  - – visibility issues in the use of “still” image watermarks
  - – visibility issues in stop frames
  - – human perception of motion is not accounted for in visual models for still images
  - – embedding the same watermark in all the frames of a video sequence is not secure, an attacker can correlate across the entire sequence to estimate the watermark (temporal collusion)

Video Watermarking Issues

- embedding completely different watermarks in successive frames of a video sequence is not secure
- successive video frames are highly correlated, an attacker can exploit this to estimate and remove a watermark
- the techniques for compressing video do not necessarily encode each frame of the sequence identically
- the synchronization of the audio with the video sequence may be a consideration for watermark protection

Preliminary Results

Conclusions

- We have lots of work to do!
  - How robust is the embedding model?
  - Investigate the use of non-parametric dectection

How I Spent My Summer