Set Theoretic Watermarking: A Feasibility Framework for Data Hiding

Gaurav Sharma

Electrical and Computer Engineering Dept.,
University of Rochester

http://www.ece.rochester.edu/~gsharma/

This work is supported by the Air Force Research Laboratory and by the Air Force Office of Scientific Research (AFOSR).
Research Overview

- Imaging systems and color science
  - Color Imaging, Digital halftoning, performance evaluation and design of imaging systems, image restoration, …

- Multimedia security
  - Watermarking, steganography, steganalysis, image/video authentication, collusion resilient fingerprinting, …

- Digital image and video processing
  - Multi-camera sensor networks

- Bio-informatics/Genomic Signal Processing
  - RNA Secondary structure prediction
  - Microarrays

http://www.ece.rochester.edu/~gsharma
Acknowledgements

Colaborators

- Students
  - Oktay Altun, Adem Orsdemir
  - Mehmet Celik (currently with Philips Research Labs, Netherlands)
- Mark Bocko, ECE Dept. University of Rochester

Funding:

- Supported by
  - Airforce Office of Scientific Research (AFOSR)
  - US Air Force Research Laboratory (AFRL), Rome, NY
Outline

- Digital Watermarking (WM)
  - Problem, Applications, Communications Model
  - SS and QIM Watermarking
- Set theoretic watermarking
  - A feasible solution framework
  - Constraints
    - SS: WM Detectability (AWGN), Compression resilience
    - HVS fidelity: Contrast Sensitivity, Masking
    - QIM: WM Detectability, Compression resilience
- Experimental Results and Extensions (Optimal embedding)
- Conclusions
Conventional Watermarks

US $10  US $20  US $100

€ 20  € 50  € 100

CERTIFICATE BOND  25% COTTON FIBER

http://www.watermarks.info/
Conventional Watermarks

- Paper Watermarks
- Visual designs/patterns embedded in paper during production
  - Thinner/thicker layer of pulp while wet
- (Mostly) Imperceptible when viewing information on either side
- In use since late thirteenth century
- Commonly used today for
  - Security in bank notes, passports, legal documents
  - Ornamentation – high quality stationery
Digital Watermarks

- Electronic Multimedia Content
  - Images, audio, video, speech in digital format

- Digital Watermarking: The process of conveying information within a host [multimedia] signal without affecting the functionality of the host.

- Vatican Library Visible watermark by IBM:
  http://www.dlib.org/dlib/december97/ibm/12lotspiech.html
Digital Watermarking

Original → Data Embedding → Watermarked

Data

Perceptually Similar

Competing Requirements

Display/Print/Network share/

Data Extraction
Watermarking/Data Hiding Applications

- Authentication
  - Validation and tamper detection
- Broadcast Monitoring
  - Keep commercial statistics
- Copyright protection
  - Prove multimedia ownership
- Fingerprinting
  - Piracy tracking
- Meta data tagging
  - Web site links
Multiple Watermarks

Fragile ➔ Authentication

Semi-fragile ➔ Broadcast monitoring

Robust ➔ Fingerprinting, copyright protection, Meta-data tagging
Watermarking ≡ communications problem

In this model:
- \( W \): watermark (modulated signal)
- \( I \): original image (interference/noise)
- \( Z \): possible manipulations of the image (noise)

Aim:
- Maximize capacity (length of \( m \))
- Minimize perceptibility (power of \( W \))
- Maximize robustness (power of noise \( Z \))
Spread spectrum techniques are well known in communications for their low SNR operation.

A message bit is “spread” using a pseudo-random unit vector \( \mathbf{c} \).

Signals \( \mathbf{c}, \mathbf{w}, \mathbf{I}, \mathbf{y} \) of length N (N = “chip rate”)

Decoder

- Computes correlation (scalar)
  \[ s = \mathbf{y} \cdot \mathbf{c} = (\mathbf{w} + \mathbf{z}) \cdot \mathbf{c} = (m\mathbf{c} + \mathbf{z}) \cdot \mathbf{c} = m + \eta \]
- Maximum likelihood decision rule
  \[ \text{if } s > 0, \; m = 1, \quad \text{otherwise } m = -1 \]
Host known at transmitter → interference from original may be reduced/eliminated

QIM: Generalization of LSB embedding

Given a set of quantizers $Q = \{Q_1, Q_2, \ldots, Q_n\}$

**Embedding:**
- select $Q_i$ corresponding to the message value $m = i$
- quantize signal $x' = Q_i(x)$

**Extraction:**
- calculate $d_i = d(x', Q_i(x))$
- select $i$ s.t. $d_i$ is minimized

**Special Case:**
Coded Dither Modulation

$Q_i(x) = q(x + v_i) - v_i$
Limitation of Non-informed Embedding
Perceptual Requirements through Ad Hoc Modifications (SS)

- **Data Embedding**
- **Perceptual Shaping/Robustness**
- **Watermarked**
- **Data Extraction**

**Problems**
- Cover interference with watermark increases: WM Power dependent on cover
- Multiple Watermarking: Imperceptibility
- Inter-watermark interference
- Robustness

Key dependent white noise
Set theoretic Framework for Watermarking

Feasibility Problem  Noisy Channel

- Define WM detector first (instead of embedder)
- Determine image that meets detection constraints under noisy channel.
- Looks similar to original image.
- Feasibility problem. Implicit Embedding!
Set theoretic watermarking

- Imperceptibility
- Robustness to compression
- Detectability
- Fragility under Malicious attacks
- Feasible solution
- Any image on intersection set meets all the criteria
- Desirable
- Pn-sequence (spread spectrum)

Feasible solution

Original image
How to find a feasible solution?

**Bregman 1965:**
Convex Sets: Iterates from successive projections guaranteed to converge to a point inside Intersection.
Method of POCS
Constraints for Set Theoretic Watermarking

- Watermark Detectability
  - In presence of noise
  - In presence of compression
  - In absence of any manipulations (fragile)

- Visual fidelity to original
  - Human contrast sensitivity [Mannos1974]
  - Texture Masking [Voloshynovskiy1999]

Per Watermark, WM Type dependent

Independent Of WM Type
SS WM Detectability Constraint

- Correlation receiver + Threshold Detector
  - Watermark $j$ present if $W_j^T X \geq \gamma_d$
- Constraint sets

\[ S_1^j \equiv \{ X : W_j^T X \geq \gamma_e \}, \quad j = 1, \ldots, K \]
Visual Fidelity
Constraints

Contrast Sensitivity Function:

\[ S_2 \equiv \{ X : \| H X - H X_0 \| \leq \theta \} \]

Texture Masking:

Euclidean Distance

Pixel-wise lower/upper bounds of visually tolerable distortion (based on original image)

Human Visual System

Convex!
SS Watermark Robustness To Compression

- JPEG Compression

\[ S_4 \equiv \{ X : W^T IDCT (Q[DCT(X)]) \geq \gamma_c \} \]

Convex Approximation:

\[ \hat{S}_4 \equiv \{ X : W^T IDCT (Q_0[DCT(X)]) \geq \gamma_c \} \]
Quantization Index Modulation (QIM) Watermark Embedding [Chen2001]

- Superior capacity-distortion properties

Original Signal

Scalar QIM

QIM Step size $\Delta$
- Robustness
- Embedding Distortion
QIM Detection Regions

Non-convex!

Detect 0

Detect 1

2Δ
QIM Embedding Constraint Set: Convex Formulation

- Conventional QIM embedding
  - Conditioning on original signal value restricts to individual bins
  - Individual bins are convex

Original Signal

- Noise Margin: Map to midpoint of bins
QIM embedding in Images

Embed information by modulation of mean of randomly selected pixels:

\[
\frac{\sum y_i}{L} = \mu
\]

Embedding:
Constraint on mean to match QIM value
Random Pixel Selection:
\[ y = S X \]
Selection matrix \( S \)
Could be Key-based

Analogous to Spread-transform dither modulation [Chen2001]

“Mean”?
Compression typically preserves mean
Generalizable to other weighted averages
QIM Watermark Delectability Constraint

Dithered QIM “Embedding” in Mean:

\[
\frac{1}{L} 1^T \mathbf{Y}_i = \mu_i^q = Q(\mu_i + d_i - b_i \frac{\Delta}{2}; \Delta) + b_i \frac{\Delta}{2} - d_i
\]

Embedded bit (+/-1)

Quantization modulated mean

Mean of randomly selected pixels
dither

Quantization step size

Randomly selected pixels

Interval midpoint

For robustness

Convex!

\[ S_2^i \equiv \{ X : \frac{1}{L} 1^T \mathbf{Y}_i = \mu_i^q \} \quad i = 1, \ldots, N \]

+1 embedded

-1 embedded
Robustness To JPEG Compression for QIM

\[ S_i^4 \equiv \{ X : S_i \left( IDCT \left( Q \left[ DCT \left( X \right) \right] \right) \right) = \mu_i^q \} \]
Robustness To JPEG Compression for QIM

Convex approximation:

\[
\hat{S}_i^4 \equiv \{ X : \text{S}_i(\text{IDCT}(Q_0[\text{DCT}(X)])) = \mu^q_i \}
\]

Subspace projection operation determined by original image. Assumption: Zero quantized (JPEG) coefficients cause most watermark power loss.
LSB Watermark

**LSB Plane Set to Match message**

\[ S_3 \equiv \{ \mathbf{x} : \text{LSB}(\mathbf{x}) = T \} \]

Non-convex

T is the image size bit-plane carrying the information
Projection Operators for POCS based Watermarking

- Projection of $y$ onto set $S_i$

\[ P_{S_i}(f) = \arg \min_{g \in S_i} \| g - f \| \]

- Constrained optimization
  - Lagrange multiplier based analytic solution(s)
  - See publications for details
Experimental Results

1. 8 images from USC image database
Experimental Results

1. 8 images from USC image database

2. Semi-fragile scenario

3. Embedding
   - 40 SS WM$s$ and 4000 QIM bits + LSB WM
   - QIM Random pixel selection size: $L=100$
   - $\Delta = 4$, $Q_0[\ ]$ determined by JPEG quantization of original image at Q factor 50

4. Visibility and Robustness against JPEG with varying rate (Q factor)
Image Sequence from Projections
Image Sequence from Projections
Image Sequence from Projections
Image Sequence from Projections
Detection of multiple watermarks for POCS:

Results for Goldhill Image

<table>
<thead>
<tr>
<th></th>
<th># Embedded</th>
<th># Correctly Recovered</th>
</tr>
</thead>
<tbody>
<tr>
<td>$SS$</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>$QIM$</td>
<td>500</td>
<td>500</td>
</tr>
<tr>
<td>$LSB$</td>
<td>262144</td>
<td>262144</td>
</tr>
</tbody>
</table>

Successfully managed:
- Interference between watermarks
- Interference between cover file and watermarks
Impact of Visual Fidelity Constraint

Original Image

Watermarked Image

Watermarked Image w/o visual constraint (PSNR Matched)
Robustness To JPEG Compression

Detection Performance

<table>
<thead>
<tr>
<th></th>
<th>Q = 90</th>
<th>Q = 80</th>
<th>Q = 70</th>
<th>Q = 60</th>
<th>Q = 50</th>
<th>Q = 40</th>
<th>Q = 30</th>
<th>Q = 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS</td>
<td>320/320</td>
<td>320/320</td>
<td>320/320</td>
<td>320/320</td>
<td>320/320</td>
<td>318/320</td>
<td>306/320</td>
<td>281/320</td>
</tr>
<tr>
<td>QIM</td>
<td>4000/4000</td>
<td>4000/4000</td>
<td>3972/4000</td>
<td>3221/4000</td>
<td>3001/4000</td>
<td>2953/4000</td>
<td>2612/4000</td>
<td>2214/4000</td>
</tr>
</tbody>
</table>

Detection of different watermarks when watermarks are inserted with robustness to compression sets.

<table>
<thead>
<tr>
<th></th>
<th>Q = 90</th>
<th>Q = 80</th>
<th>Q = 70</th>
<th>Q = 60</th>
<th>Q = 50</th>
<th>Q = 40</th>
<th>Q = 30</th>
<th>Q = 20</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS</td>
<td>320/320</td>
<td>320/320</td>
<td>0/320</td>
<td>0/320</td>
<td>0/320</td>
<td>0/320</td>
<td>0/320</td>
<td>0/320</td>
</tr>
<tr>
<td>QIM</td>
<td>4000/4000</td>
<td>3948/4000</td>
<td>2881/4000</td>
<td>2633/4000</td>
<td>2548/4000</td>
<td>2424/4000</td>
<td>2347/4000</td>
<td>1994/4000</td>
</tr>
</tbody>
</table>

Detection of different watermarks when watermarks are inserted without robustness to compression sets.
Observations

- Framework naturally allows for combination of constraints in different domains
  - Perceptual constraints
    - Contrast sensitivity – frequency domain
    - Masking – spatial domain (can also do alternate domain)
  - Watermarks
    - Spatial domain/transform domain
  - WM Robustness to Signal Processing
    - Compression arbitrary linear transform domain
    - AWGN in Spatial domain
Assured Fragility for Semifragile WMs

- Fragility Constraint: Watermark lost under aggressive compression
  - Inverted Robustness constraint

$$\hat{S}_5 \equiv \{ X : W^T \left( T^I(Q^A_0[T^F(X)]) - \overline{T^I(Q^A_0[T^F(X)])} \right) \leq \gamma \}$$

Subspace projection operation to robust compression determined by original image.

Convex!
Semifragility: Experimental Results

- Robust up to JPEG Q60, Fragile under JPEG Q40
  - Hierarchical scheme, shaping by replication factor R

<table>
<thead>
<tr>
<th>Repl. R</th>
<th>Level l</th>
<th>Q = 90</th>
<th>Q = 80</th>
<th>Q = 70</th>
<th>Q = 60</th>
<th>Q = 50</th>
<th>Q = 40</th>
<th>Q = 30</th>
<th>Q = 20</th>
<th>Q = 10</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>413/432</td>
<td>407/432</td>
<td>396/432</td>
<td>367/432</td>
<td>317/432</td>
<td>292/432</td>
<td>239/432</td>
<td>30/432</td>
<td>0/432</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1621/1728</td>
<td>1574/1728</td>
<td>1470/1728</td>
<td>1339/1728</td>
<td>1095/1728</td>
<td>965/1728</td>
<td>843/1728</td>
<td>282/1728</td>
<td>27/1728</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>6526/6912</td>
<td>6140/6912</td>
<td>5578/6912</td>
<td>4768/6912</td>
<td>3914/6912</td>
<td>3486/6912</td>
<td>3064/6912</td>
<td>1760/6912</td>
<td>540/6912</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>408/432</td>
<td>411/432</td>
<td>405/432</td>
<td>420/432</td>
<td>405/432</td>
<td>387/432</td>
<td>361/432</td>
<td>320/432</td>
<td>43/432</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1608/1728</td>
<td>1689/1728</td>
<td>1551/1728</td>
<td>1409/1728</td>
<td>1436/1728</td>
<td>1373/1728</td>
<td>1254/1728</td>
<td>1109/1728</td>
<td>391/1728</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>6457/6912</td>
<td>6343/6912</td>
<td>6245/6912</td>
<td>5743/6912</td>
<td>5267/6912</td>
<td>4922/6912</td>
<td>4328/6912</td>
<td>3704/6912</td>
<td>1982/6912</td>
</tr>
</tbody>
</table>
Optimal Watermark Embedding

- Least Perceptual (Freq. Weighted MSE) Distortion subject to other Constraints

\[
\min_X \quad \| HX - HX_0 \| \\
\text{subject to} \quad D_L(X_0) \leq (X - X_0) \leq D_U(X_0) \\
W^T(X - \overline{X}) \geq \gamma_e \\
W^T \left( T_T(\tilde{Q}[T_F(X)]) - \overline{T_T(\tilde{Q}[T_F(X)])} \right) \geq \gamma_e
\]

- Other “Optimal Embeddings”
  - Max embedding strength, Max compression robustnes, ....
  - Each subject to other constraints
Optimization via Feasibility

- Optimization problem

\[
\begin{align*}
\text{min} & \quad \phi_0(X) \\
\text{subject to} & \quad \phi_i(X) \leq 0, \quad i = 1, 2, \ldots, 4
\end{align*}
\]

- Closely related feasibility problem

Find \( X \)

subject to \( \phi_i(X) \leq 0, \quad i = 1, \ldots, 4 \)

\( \phi_0(X) \leq \tau \)
Optimization from Feasibility

\[ \varphi_0(X) = u_j \]

\[ \varphi_0(X) = t_j = \frac{u_j + l_j}{2} \]

\[ \varphi_k(X) \leq 0 \]

Optimal Point

Level curves of objective function
Max Embedding Strength

Min Freq Wt Percep. Dist.

Max Compression Robust.

Min Texture Visibility
Max Embedding Strength

Min Freq Wt Percep. Dist.

Max Compression Robust.

Min Texture Visibility
Conclusions

- Set-theoretic watermarking framework
  - Watermarking = Feasibility problem
    - Constraints posed by detection and WM imperceptibility
    - Models for some signal processing attacks
  - Incorporates visual adaptation for WM embedding in formulation rather than through ad hoc modifications

- Convex formulation for set theoretic watermarking
  - Implicitly embeds watermark by successive projection onto convex constraints

- General:
  - Multiple watermarking: SS, QIM, LSB (EI 2006)
  - Applicable for “embedding” in any other linear transform domain
  - Color images- multi-channel (linear) visual models
  - Other multi-media signals

- Extensions:
  - Optimal Embeddings
  - Min visibility subject to detectability and other constraints
    - Max robustness subject to visibility tolerance + other constraints
Watermark embedding formulations

- Non-informed watermark insertion
  - [Cox1997]
  - [Chen2001]

- Lower
  - Ad-hoc modifications
    - Computational complexity
    - Visual Adaptability
    - Interference cancellation
    - Systematic vs. Ad hoc
    - Informed vs. Blind

- Feasibility Formulation (Set theoretic Watermarking)
  - Higher
  - Optimization formulation
    - [AltunICIP2005],
    - [AltunICASSP2006]
    - [AltunTIFS2006]
    - [Cox1997]
    - [Chen2001]
    - [Pereira2001]
    - [Mihcak2005],
    - [AltunICIP2006]
Recent Extensions

- **Fingerprinting for Collusion (ICIP 2007)**
  - Tracing the source of a leak, identify group working together

- **Steganalysis Aware Steganography (EI 2008)**
  - Incorporate constraints to preserve statistics of original (cover) image
  - Counters statistical steganalysis
References


References


Thank you!