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 Detectabilty (AWGN), Compression resilience
    - HVS fidelity: Contrast Sensitivity, Masking
    - QIM: WM Detectability, Compression resilience
- Experimental Results and Extensions (Optimal embedding)
- Conclusions

Conventional Watermarks

US $10

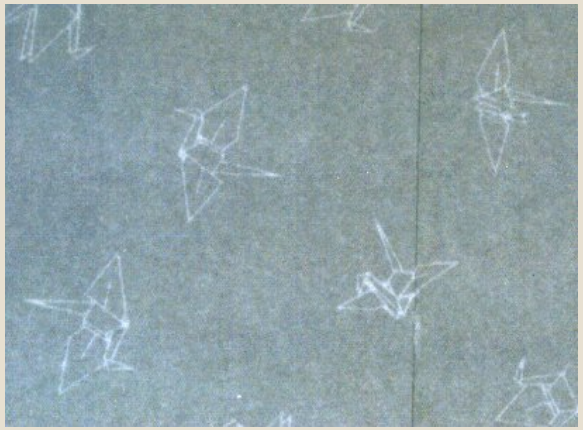
US $20

US $100

€ 20

€ 50

€ 100

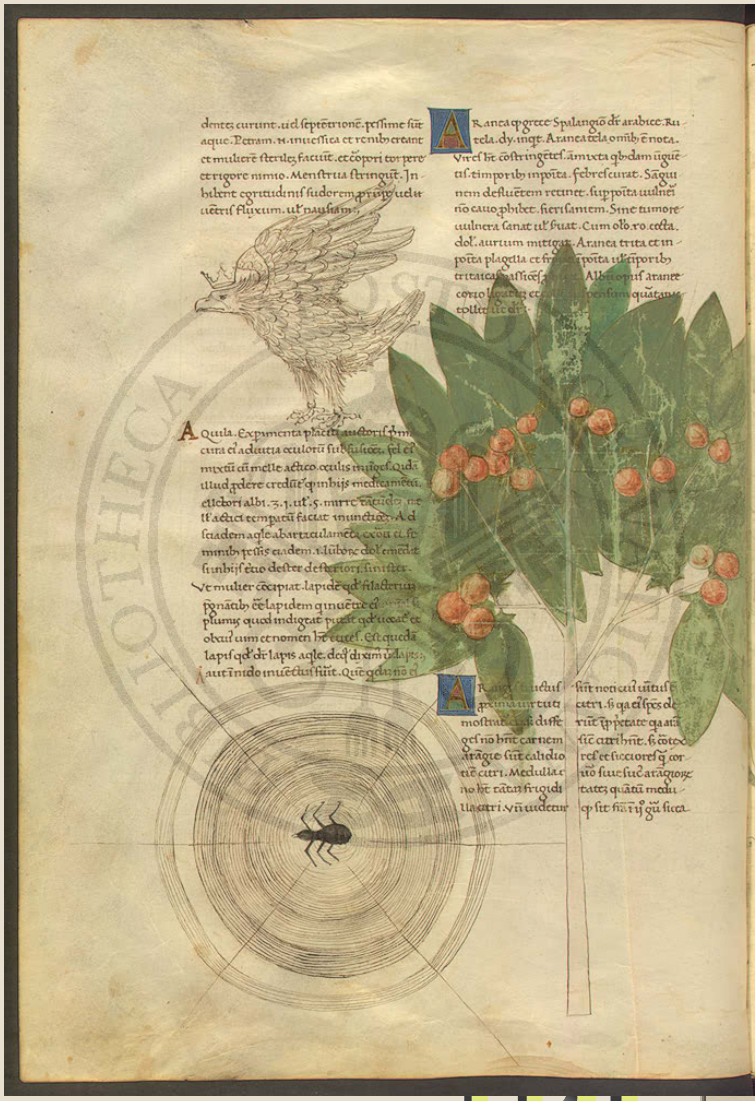


Conventional Watermarks

- 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

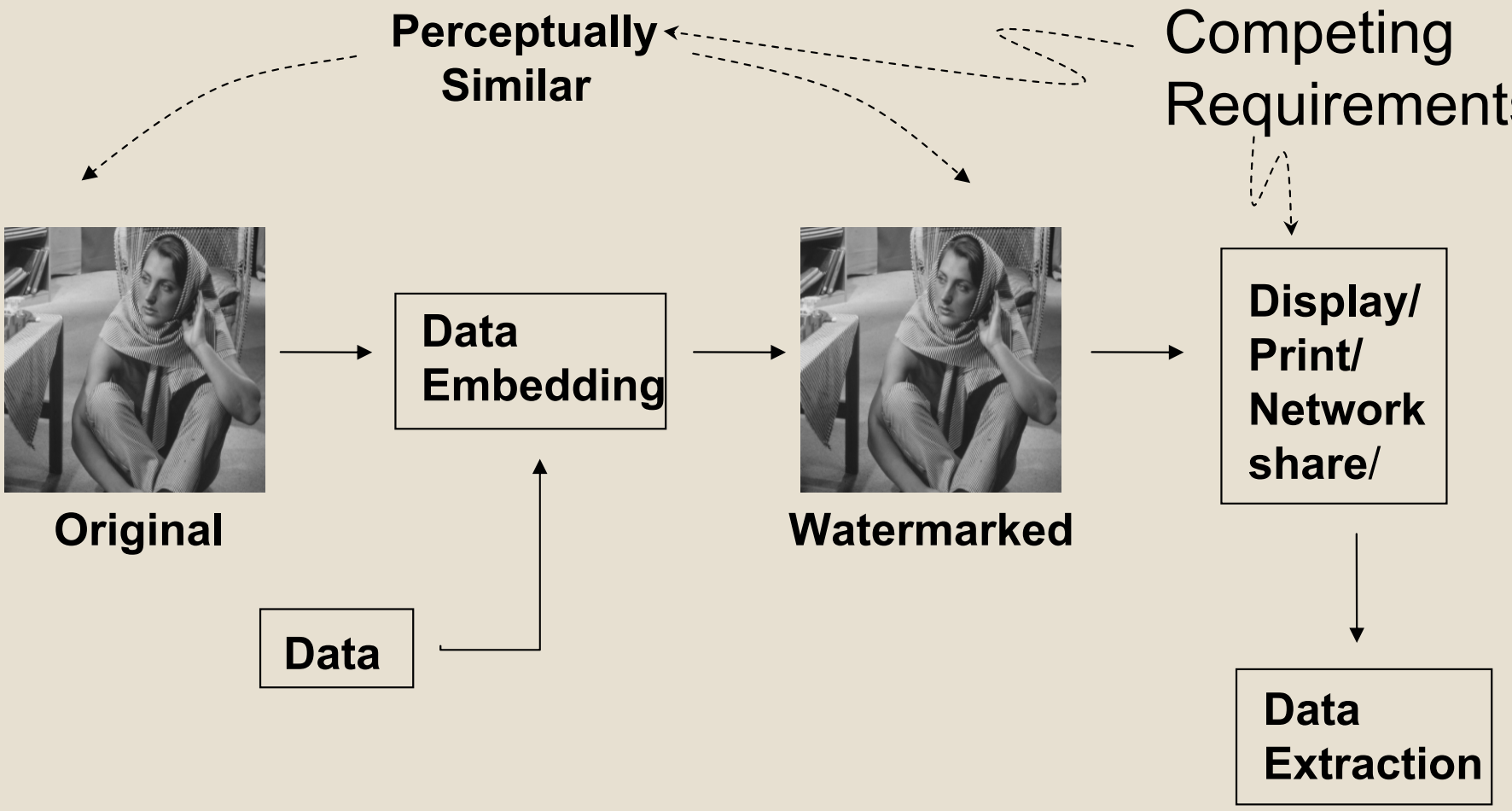
Digital Watermarks

- 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



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

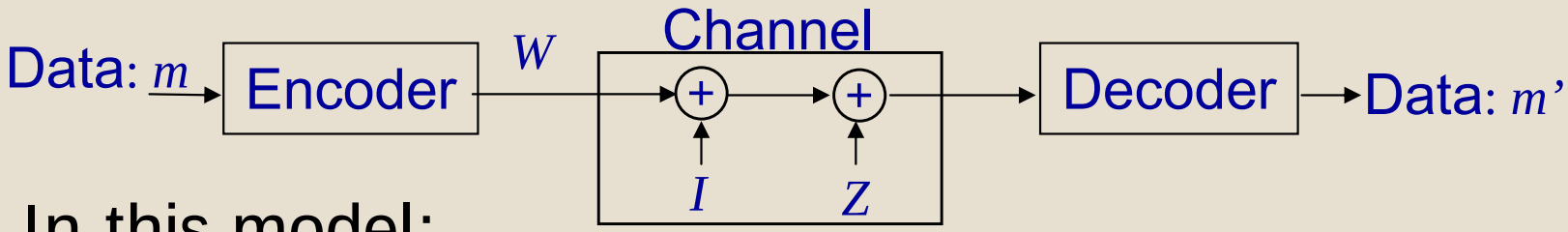
Combinations

Multiple Watermarks

Fragile	⟹	Authentication
Semi-fragile	⟹	Broadcast monitoring
Robust	⟹	Fingerprinting, copyright protection Meta-data tagging

Communications model

- 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*)

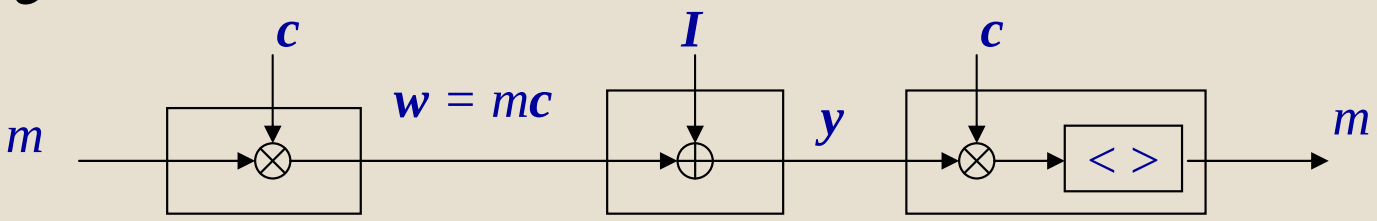
  Minimize perceptibility (power of *W)*

  Maximize robustness (power of noise *Z*)

  } Low SNR

Spread Spectrum Watermark [Cox97]

- Spread spectrum techniques are well known in communications for their low SNR operation
- A message bit is “spread” using a pseudo-random unit vector ***c***

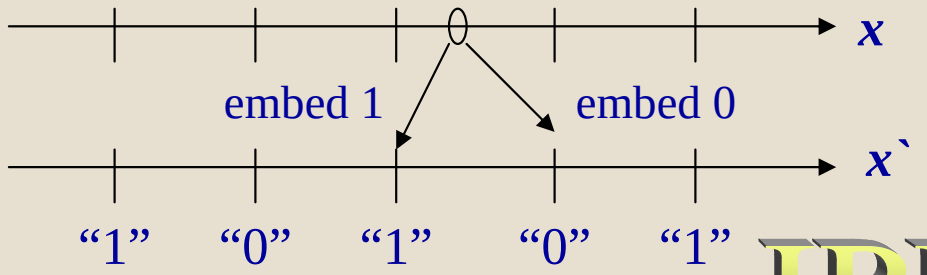


- Signals ***c, w, I, y*** of length N (N = “chip rate”)
- Decoder
  - computes correlation (scalar)
    $s = \boldsymbol{y} \cdot \boldsymbol{c} = (\boldsymbol{w} + \boldsymbol{z}) \cdot \boldsymbol{c} = (m\boldsymbol{c} + \boldsymbol{z}) \cdot \boldsymbol{c} = m + \eta$
  - Maximum likelihood decision rule
    if $s > 0$, $m = 1$, otherwise $m = -1$

Quantization Index Modulation [Chen01]

- Host known at transmitter → interference from original may be reduced/eliminated
- QIM: Generalization of LSB embedding
- Given a set of quantizers $\mathbf{Q = \{ Q_1, Q_2, \ldots , Q_n\}}$
- 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
$Q_i(x) = q(x + v_i) - v_i$

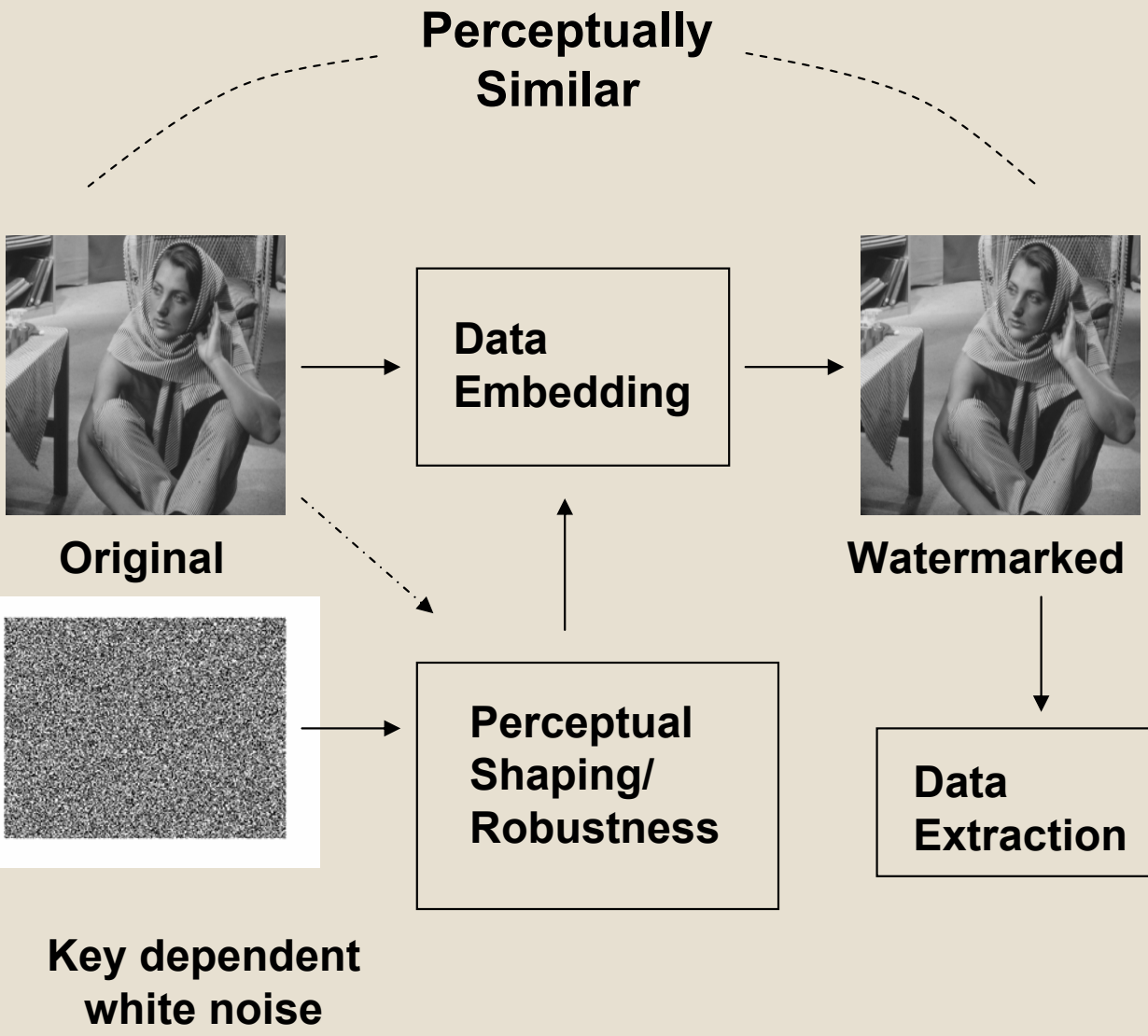


Limitation of Non-informed Embedding

Original

Watermarked

Perceptual Requirements through Ad Hoc Modifications (SS)



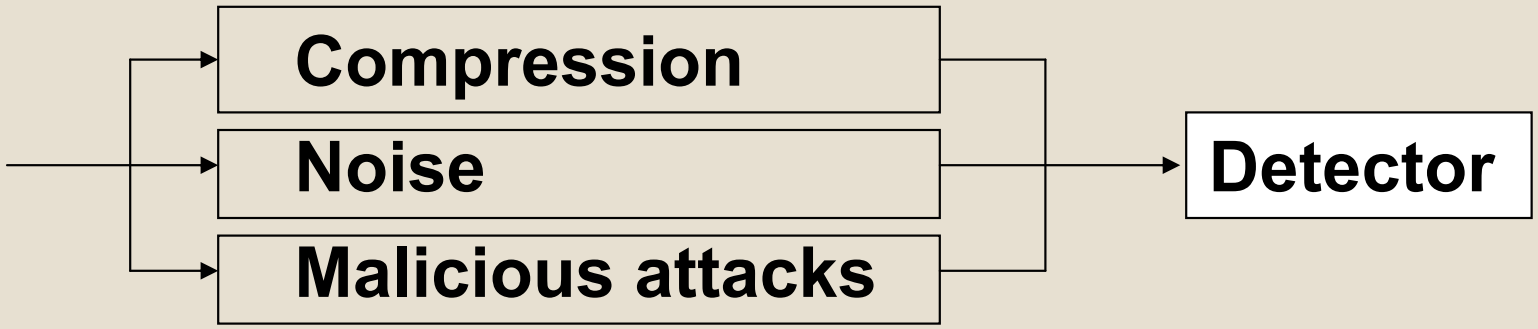
Problems

Cover interference with watermark increases: WM Power dependent on cover

Multiple Watermarking: Imperceptibility Inter-watermark interference Robustness

Set theoretic Framework for Watermarking

Feasibility Problem Noisy Channel

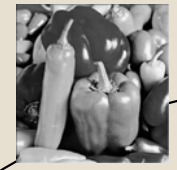


≈

Original

- **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



Original image

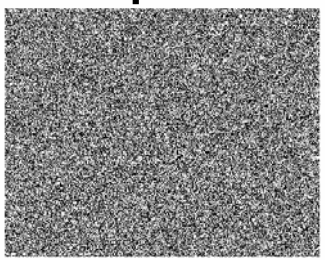
Imperceptibility

Feasible solution

Any image on intersection set meets all the criteria
Desirable

Detectability

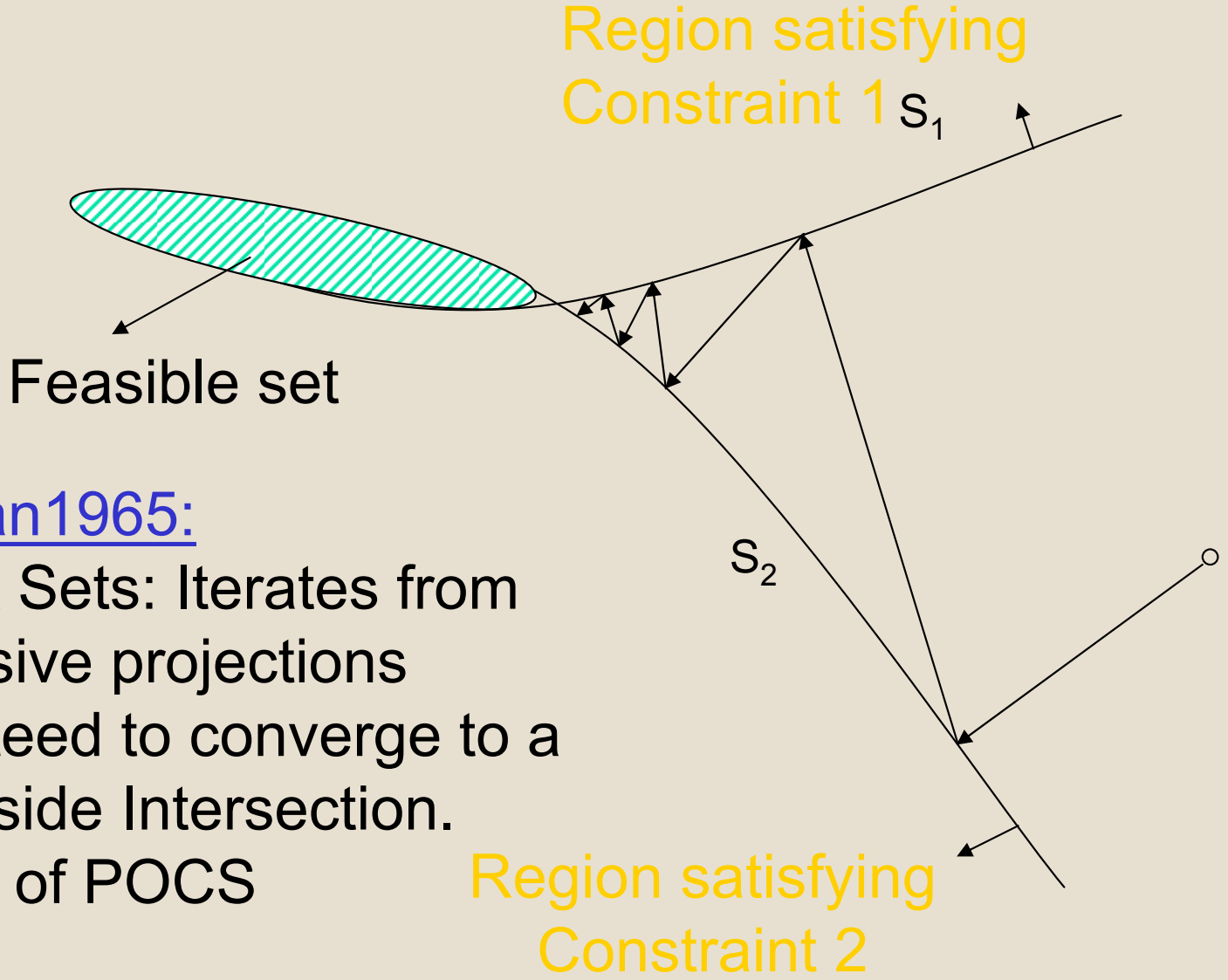
Pn-sequence
(spread spectrum)



Robustness to compression

Fragility under Malicious attacks

How to find a feasible solution?



Bregman1965:

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)

Per Watermark, WM Type dependent

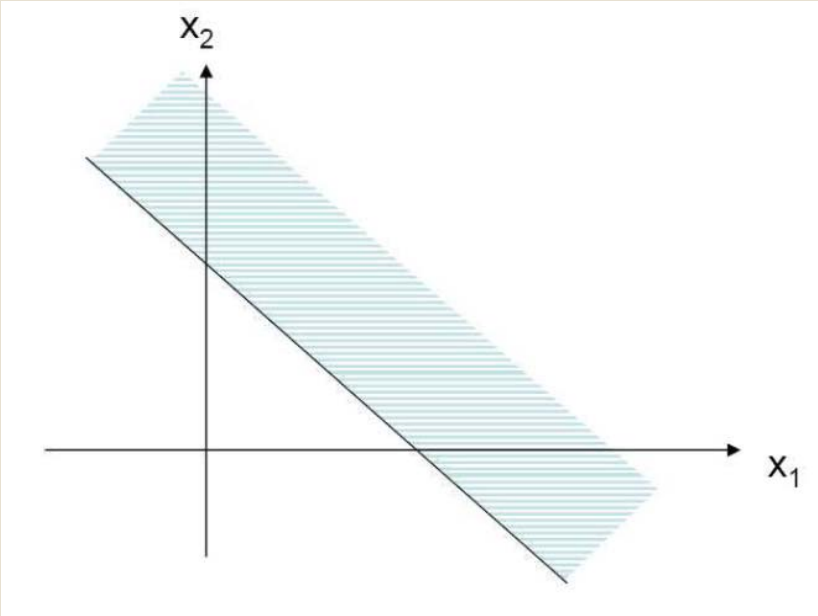
- Visual fidelity to original
  - Human contrast sensitivity [Mannos1974]
  - Texture Masking [Voloshynovskiy1999]

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

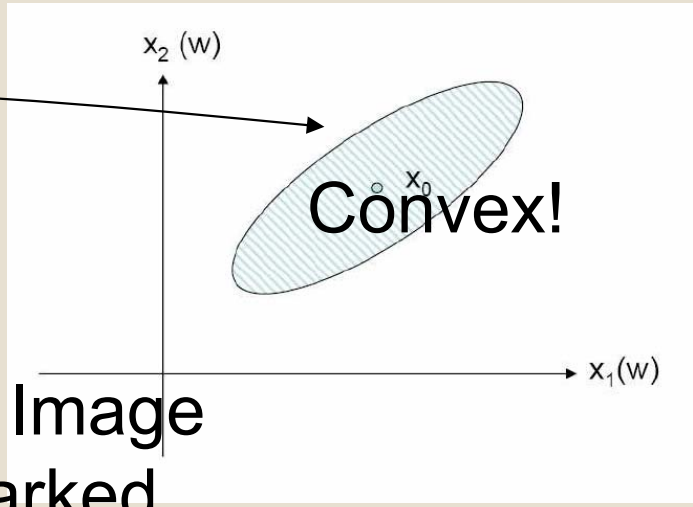
$$S_1^j \equiv \{X : W_j^T X \geq \gamma_e\}, \qquad j = 1, \ldots K$$



Visual Fidelity Constraints

Contrast Sensitivity Function:

$$S_2 \equiv \{X : \| HX - HX_0 \| \leq \theta\}$$



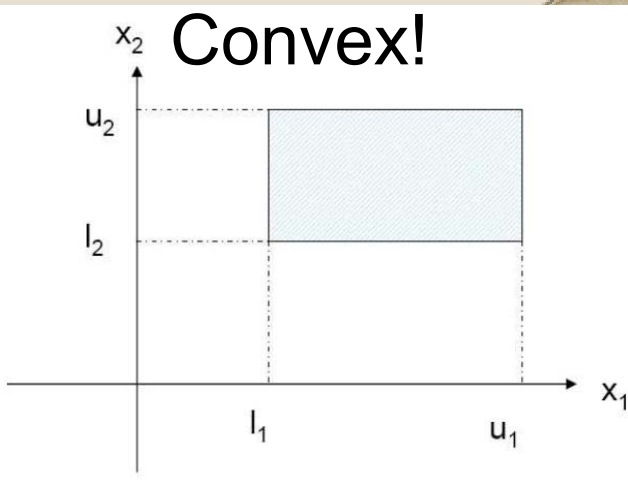
Texture Masking:

Euclidean Distance

Original Image to be marked

Human Visual Sytem

$$S_3 \equiv \{X : D_L \leq (X - X_0) \leq D_U\}$$

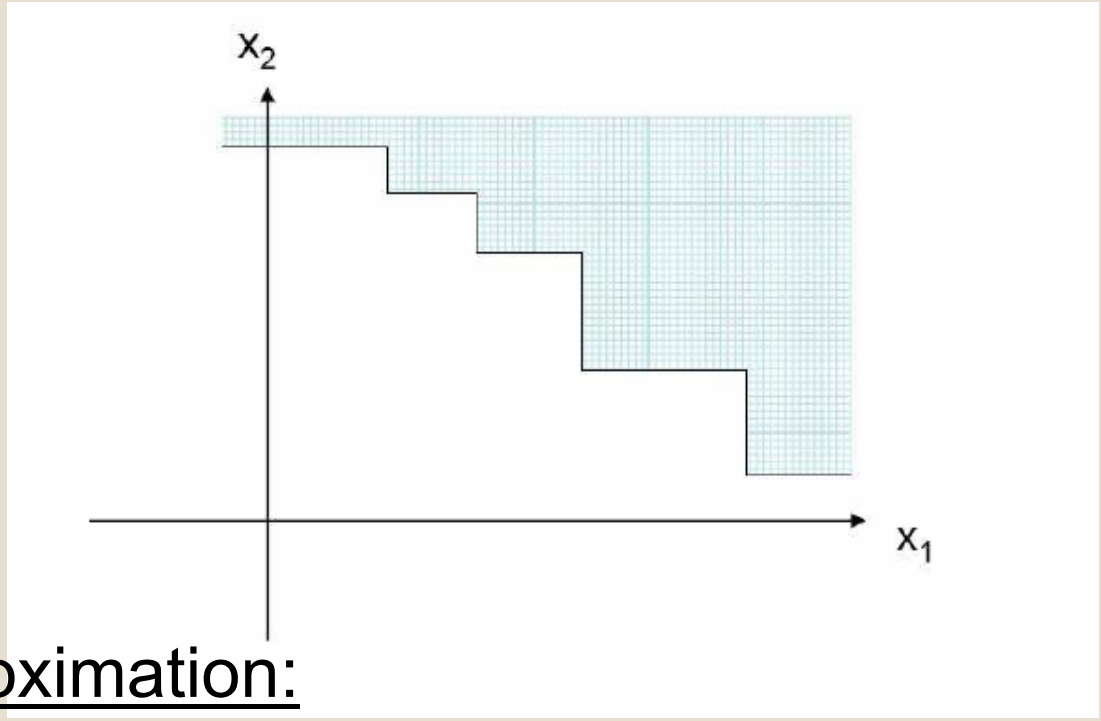


Pixel-wise lower/upper bounds of visually tolerable distortion (based on original image)

SS Watermark Robustness To Compression

- JPEG Compression

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

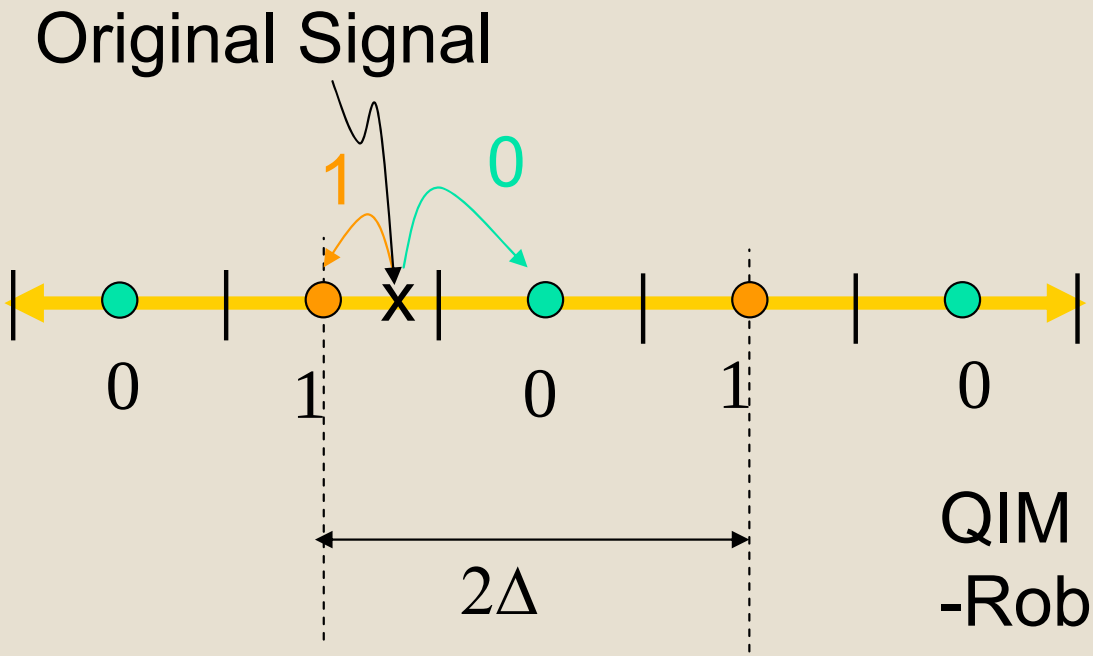


Convex Approximation:

$$\hat{S}_4 \equiv \{X : W^T IDCT\left(Q_0[DCT(X)]\right) \geq \gamma_c\}$$

Quantization Index Modulation (QIM) Watermark Embedding [Chen2001]

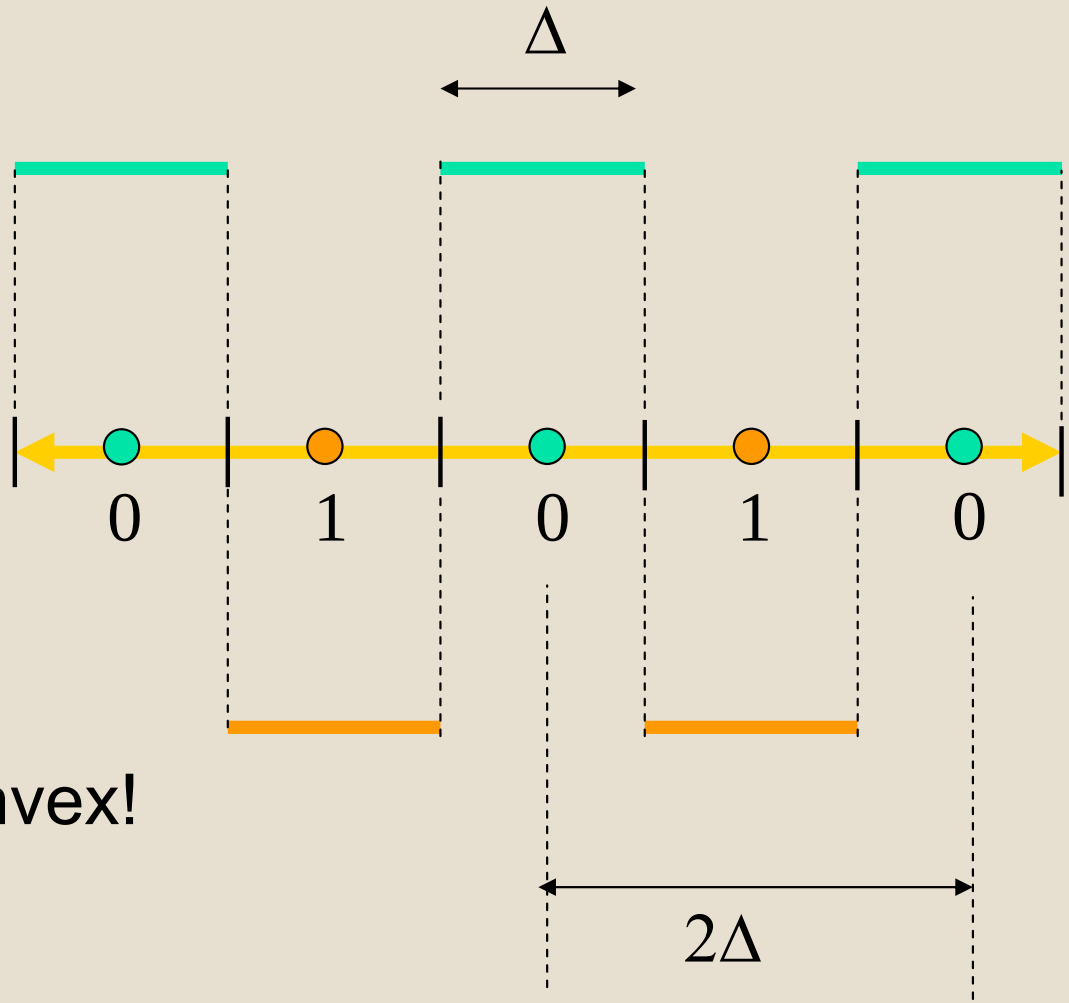
- Superior capacity-distortion properties



Scalar QIM

QIM Step size Δ
-Robustness
-Embedding Distortion

QIM Detection Regions



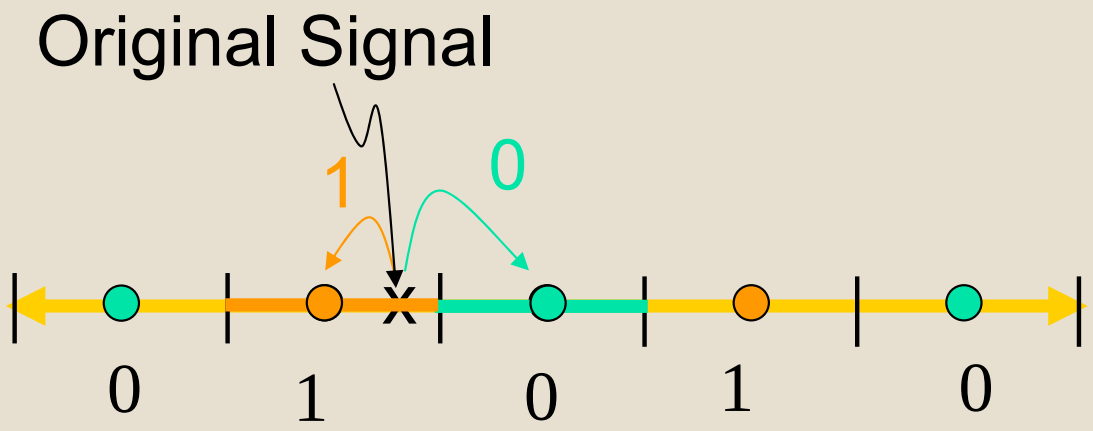
Detect
0

Detect
1

Non-convex!

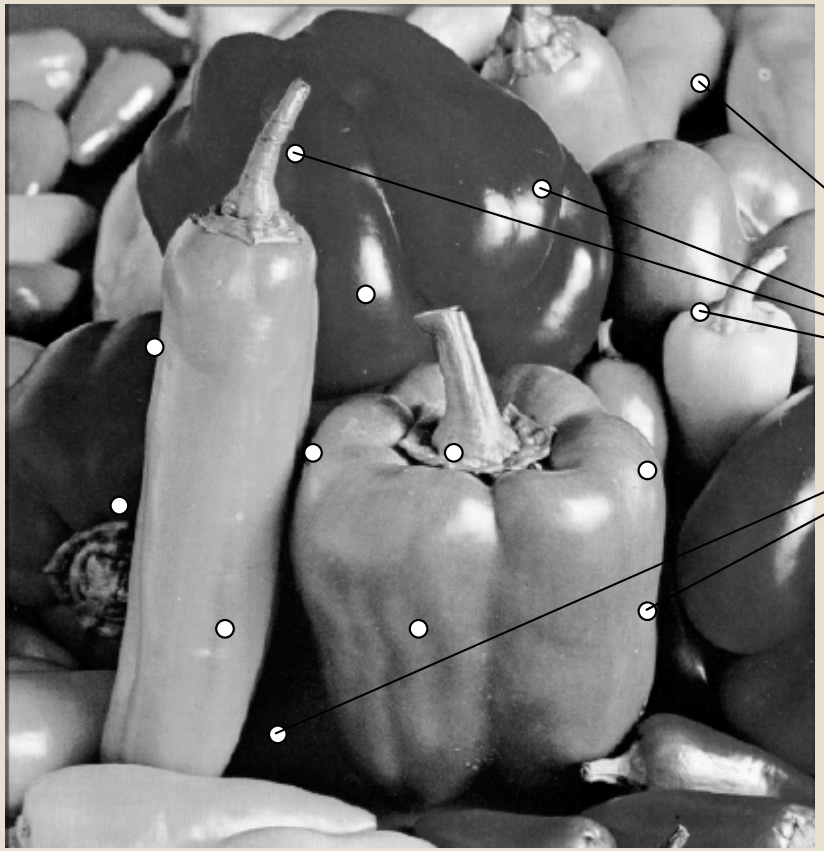
QIM Embedding Constraint Set: Convex Formulation

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



  - Noise Margin: Map to midpoint of bins

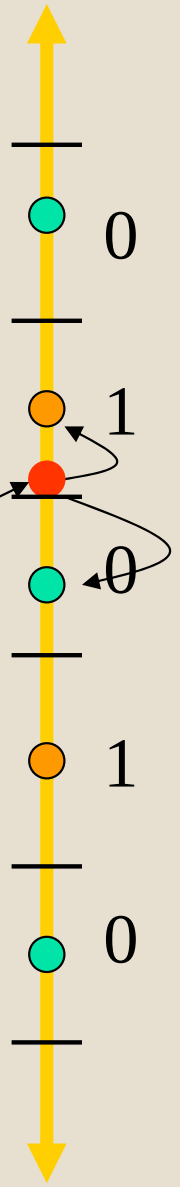
QIM embedding in Images



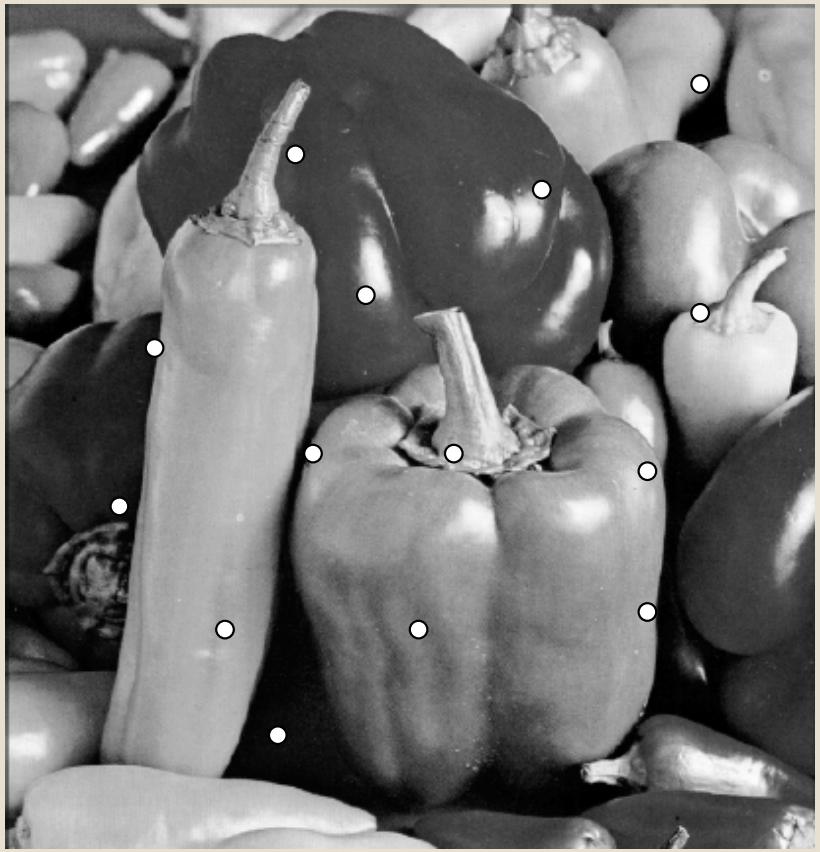
Embed information by modulation of mean of randomly selected pixels

$(\sum y_i)/L = \mu$

Embedding: Constraint on mean to match QIM value



QIM embedding II



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:

Embedded bit (+/-1)

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

Quantization modulated mean

Mean of randomly selected pixels

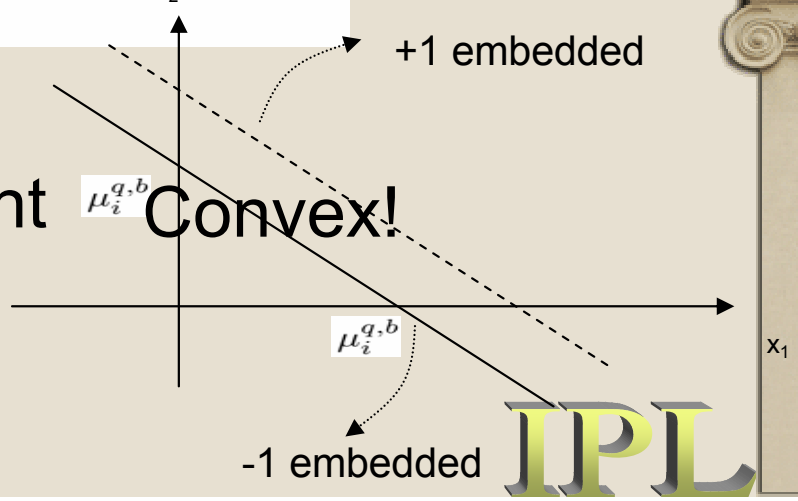
dither

Quantization step size

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

Randomly selected pixels

Interval midpoint For robustness



Robustness To JPEG Compression for QIM

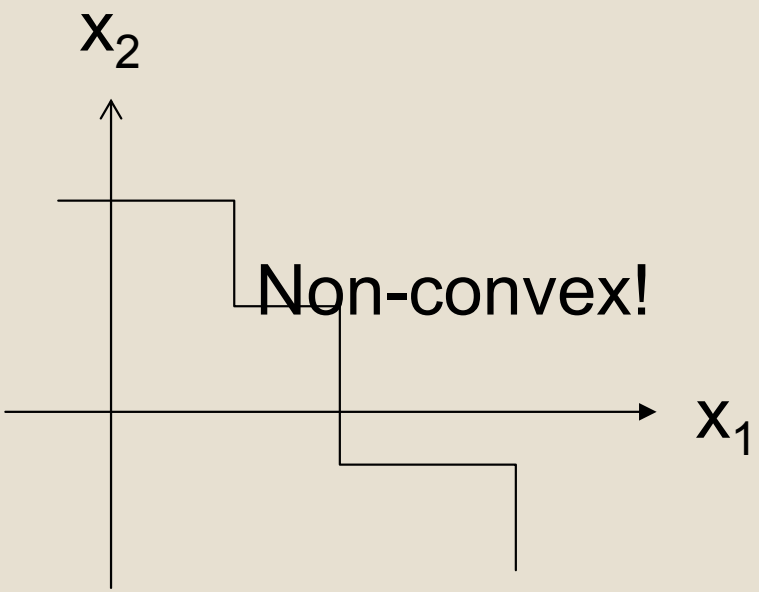
$$S_4^i \equiv \{\mathbf{X} : \overline{\mathbf{S}_i(IDCT(Q[DCT(X)]))} = \mu_i^q\}$$

Selection matrix

JPEG

Mean

Modulated mean

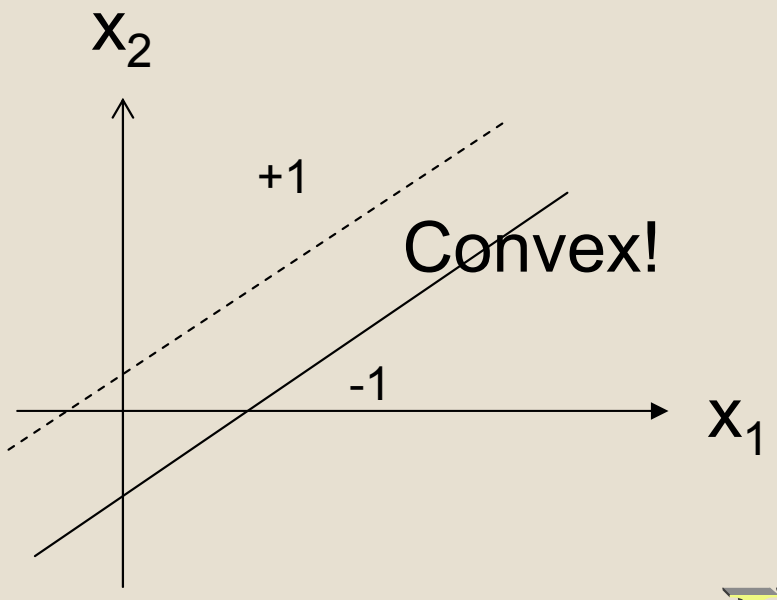


Robustness To JPEG Compression for QIM

Convex approximation:

$$\widehat{S}_4^i \equiv \{X : \overline{\mathbf{S}_i(IDCT(Q_0[DCT(X)]))} = \mu_i^q\}$$

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

$$\mathbb{S}_3 \equiv \{\mathbf{x} : LSB(\mathbf{x}) = \mathbf{T}\}$$

Non-convex

$\mathbf{T}$ 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 WMs and 4000 QIM bits + LSB WM

   QIM Random pixel selection size: L=100

   Δ =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

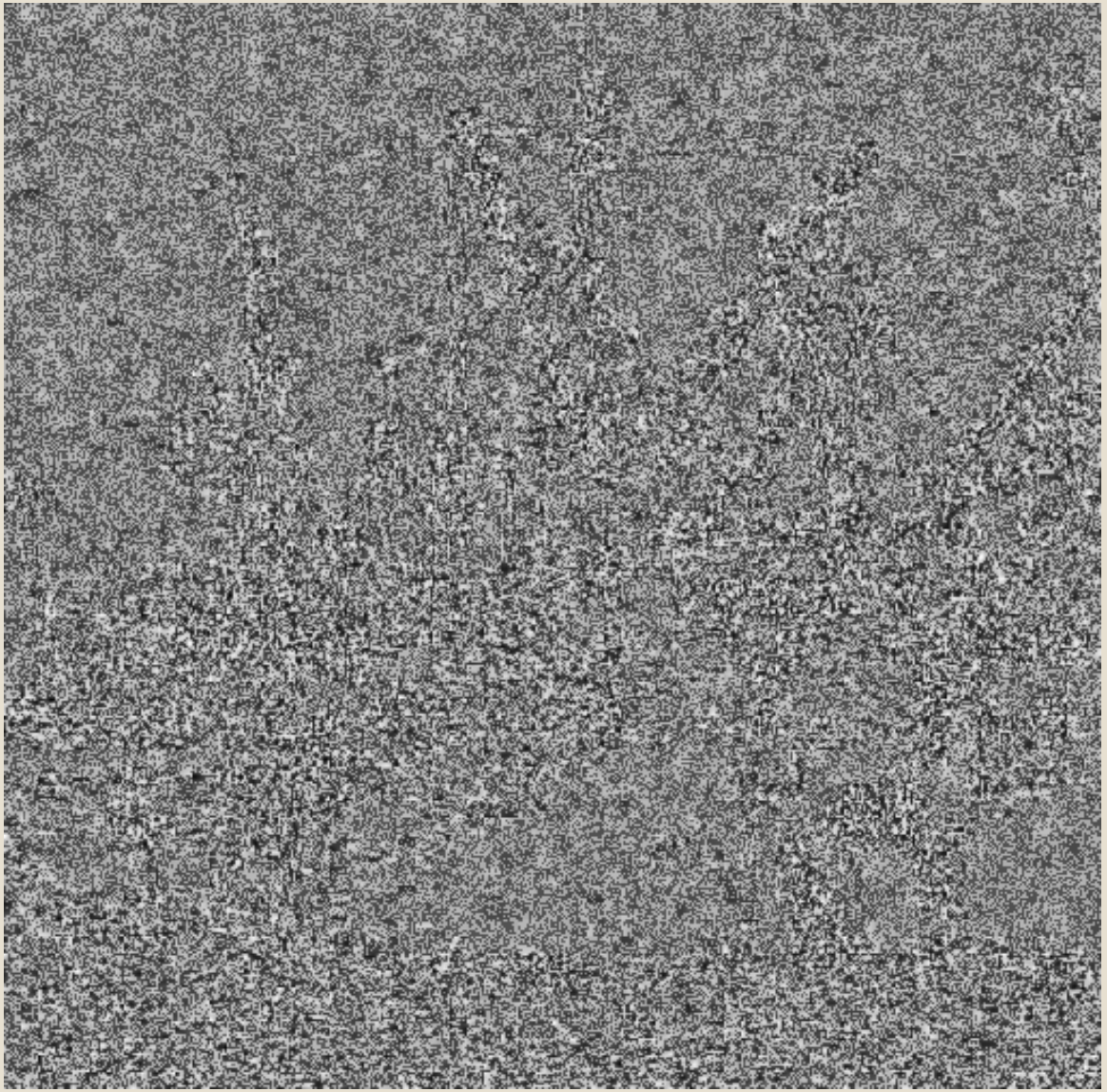
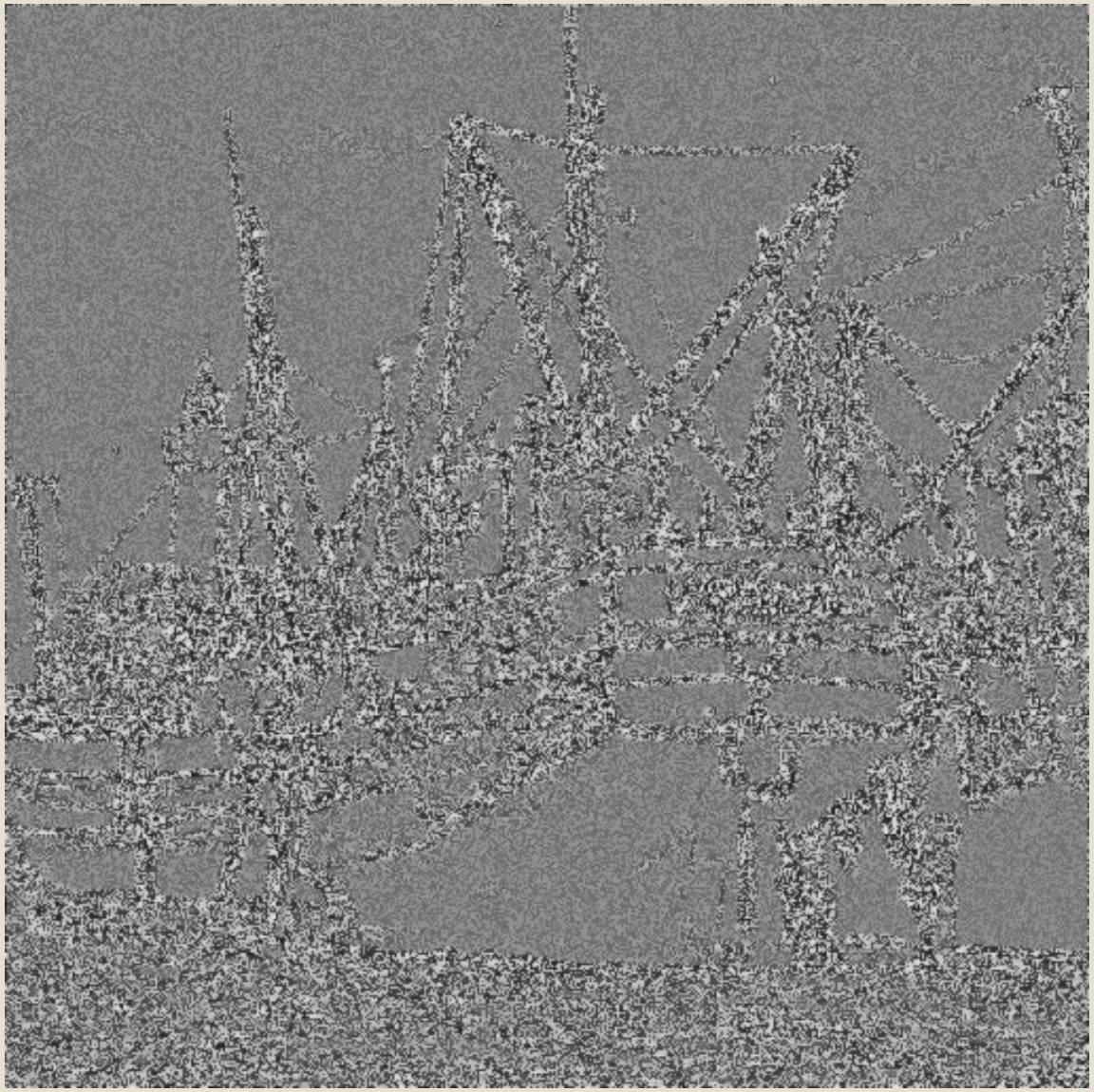


Image Sequence from Projections

Image Sequence from Projections



Experimental Results: Multiple Watermark Recovery

Detection of multiple watermarks for POCS:

Results for Goldhill Image

	# Embedded	# Correctly Recovered
SS	40	40
QIM	500	500
LSB	262144	262144

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

	$Q = 90$	$Q = 80$	$Q = 70$	$Q = 60$	$Q = 50$	$Q = 40$	$Q = 30$	$Q = 20$
SS	$320/320$	$320/320$	$320/320$	$320/320$	$320/320$	$318/320$	$306/320$	$281/320$
QIM	$4000/4000$	$4000/4000$	$3972/4000$	$3221/4000$	$3001/4000$	$2953/4000$	$2612/4000$	$2214/4000$

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

	$Q = 90$	$Q = 80$	$Q = 70$	$Q = 60$	$Q = 50$	$Q = 40$	$Q = 30$	$Q = 20$
SS	$320/320$	$320/320$	$320/320$	$0/320$	$0/320$	$0/320$	$0/320$	$0/320$
QIM	$4000/4000$	$3948/4000$	$2881/4000$	$2633/4000$	$2548/4000$	$2424/4000$	$2347/4000$	$1994/4000$

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

Observations

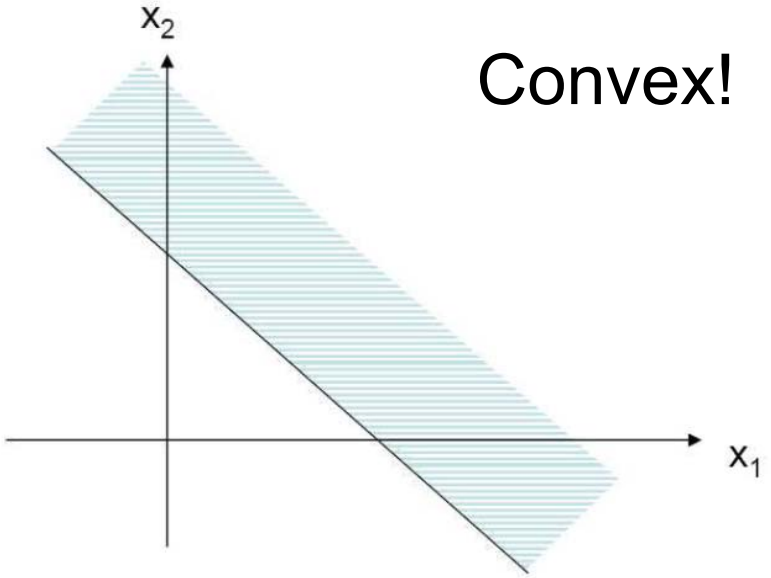
- Framework naturally allows for combination of constraints in different domains
  - Perceptual constraints
    - Contrast sensitivity – frequency domain
    - Masking – spatial domain (can also do alternate domain)
  - Watermarks
    - Spatial domain/transform domain
  - WM Robustness to Signal Processing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

Assured Fragility for Semifragile WMs

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

$$\widehat{S}_5 \equiv \{X : W^T \left(\mathcal{T}_{\mathcal{I}}(Q_0^A[\mathcal{T}_{\mathcal{F}}(X)]) - \overline{\mathcal{T}_{\mathcal{I}}(Q_0^A[\mathcal{T}_{\mathcal{F}}(X)])} \right) \leq \gamma\}$$

Subspace projection operation to robust compression determined by original image.



Convex!

Semifragility: Experimental Results

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

Repl. R	Level l	$Q=90$	$Q=80$	$Q=70$	$Q=60$	$Q=50$	$Q=40$	$Q=30$	$Q=20$	$Q=10$
1	1	107/108	105/108	102/108	98/108	84/108	77/108	64/108	5/108	0/108
	2	413/432	407/432	396/432	367/432	317/432	292/432	239/432	39/432	0/432
	3	1621/1728	1574/1728	1470/1728	1339/1728	1095/1728	965/1728	843/1728	282/1728	27/1728
	4	6526/6912	6140/6912	5578/6912	4768/6912	3914/6912	3486/6912	3064/6912	1769/6912	540/6912
2	1	107/108	103/108	99/108	97/108	94/108	91/108	87/108	74/108	2/108
	2	408/432	411/432	405/432	429/432	405/432	387/432	361/432	329/432	43/432
	3	1608/1728	1689/1728	1551/1728	1499/1728	1436/1728	1373/1728	1254/1728	1109/1728	391/1728
	4	6457/6912	6343/6912	6245/6912	5743/6912	5267/6912	4922/6912	4328/6912	3704/6912	1982/6912

Optimal Watermark Embedding

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

$$\min_{X} \quad \| HX - HX_0 \|$$

$$\text{subject to} \quad D_L(X_0) \leq (X - X_0) \leq D_U(X_0)$$

$$W^T(X - \overline{X}) \geq \gamma_e$$

$$W^T\left(\mathcal{T}_{\mathcal{I}}(Q[\mathcal{T}_{\mathcal{F}}(X)]) - \overline{\mathcal{T}_{\mathcal{I}}(Q[\mathcal{T}_{\mathcal{F}}(X)])}\right) \geq \gamma_c$$

  - Other "Optimal Embeddings"
    - Max embedding strength, Max compression robustnes, ….

    Each subject to other constraints

Optimization via Feasibility[Boyd]

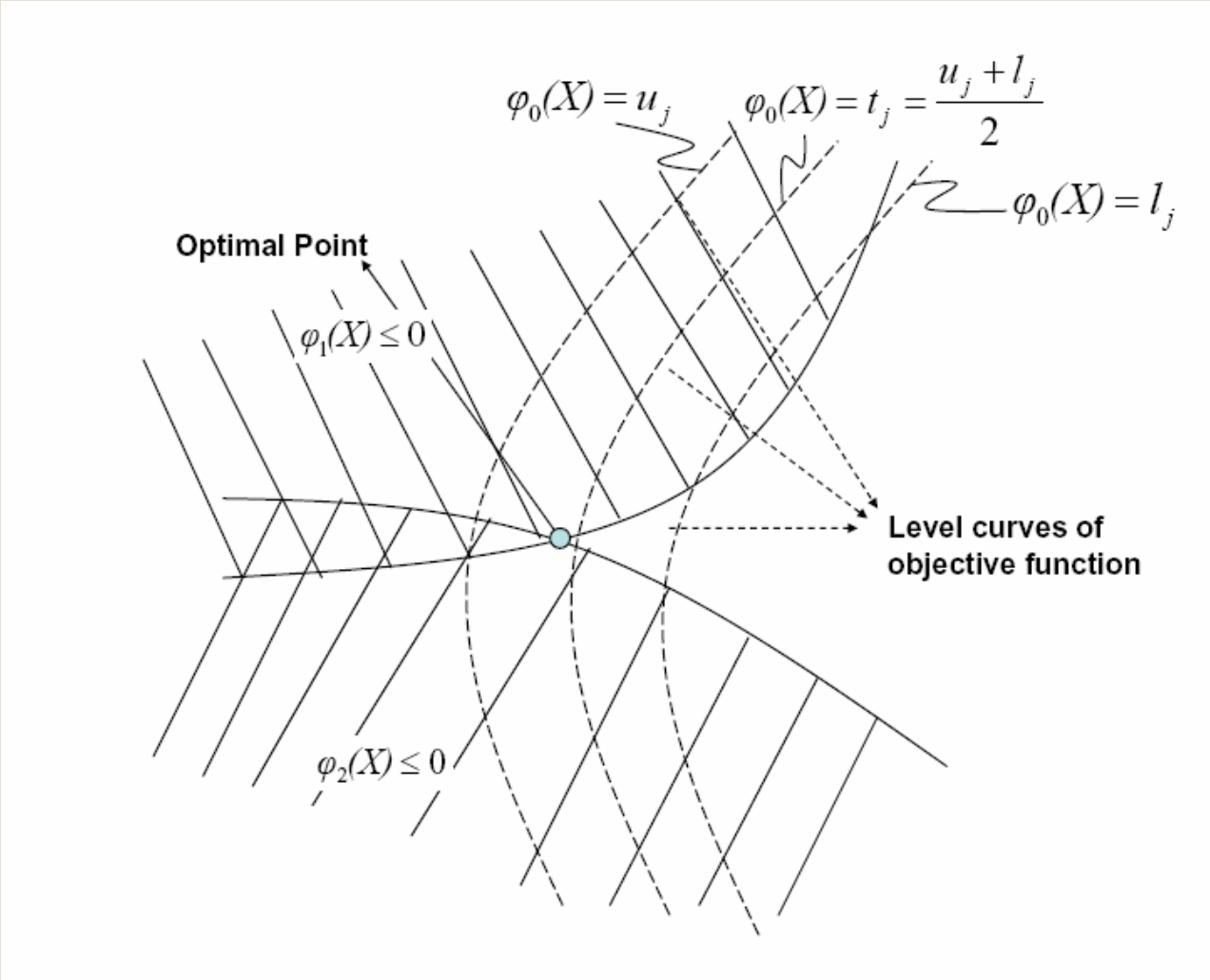
- Optimization problem

$$\begin{array}{ll} \min & \phi_0(X) \\ \text{subject to} & \phi_i(X) \leq 0, \quad i = 1, 2, .., 4 \end{array}$$

- Closely related feasibility Problem

$$\begin{array}{ll} \text{Find} & X \\ \text{subject to} & \phi_i(X) \leq 0, \quad i = 1, .., 4 \\ & \phi_0(X) \leq \tau \end{array}$$

Optimization from Feasibility

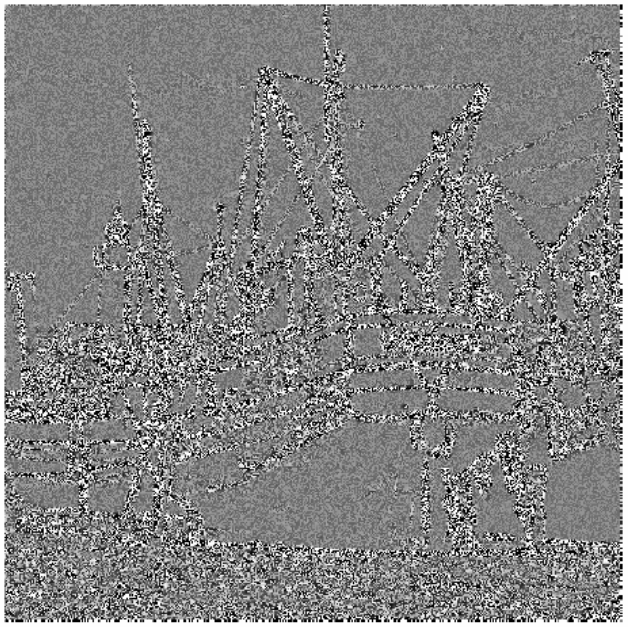


Max Embedding Strength

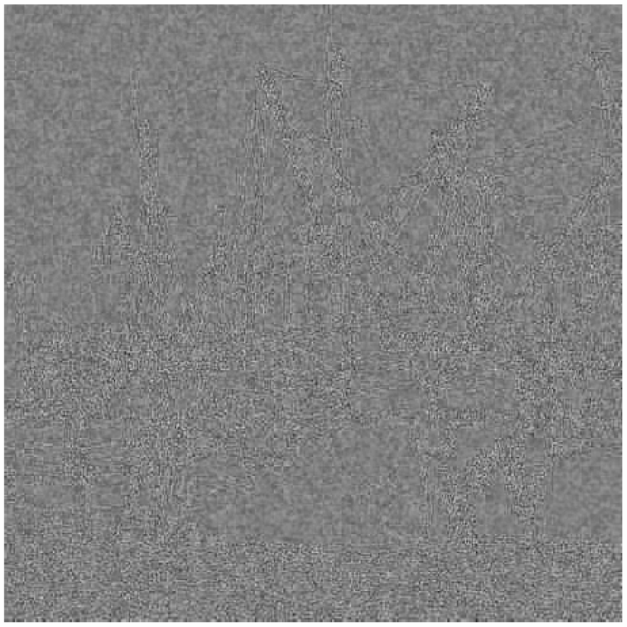
Min Freq Wt Percep. Dist.

Max Compression Robust.

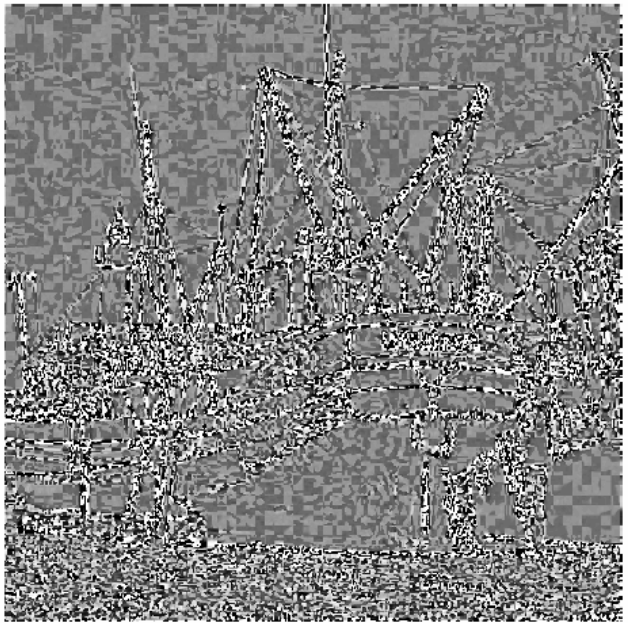
Min Texture Visibility



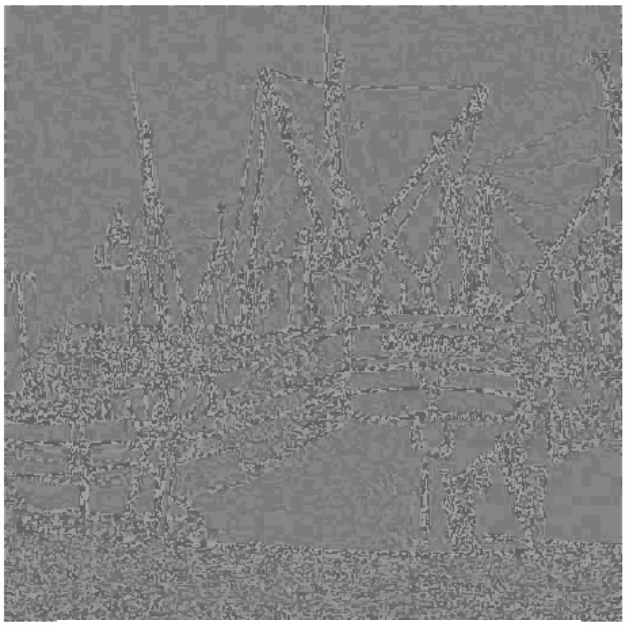
Max Embedding Strength



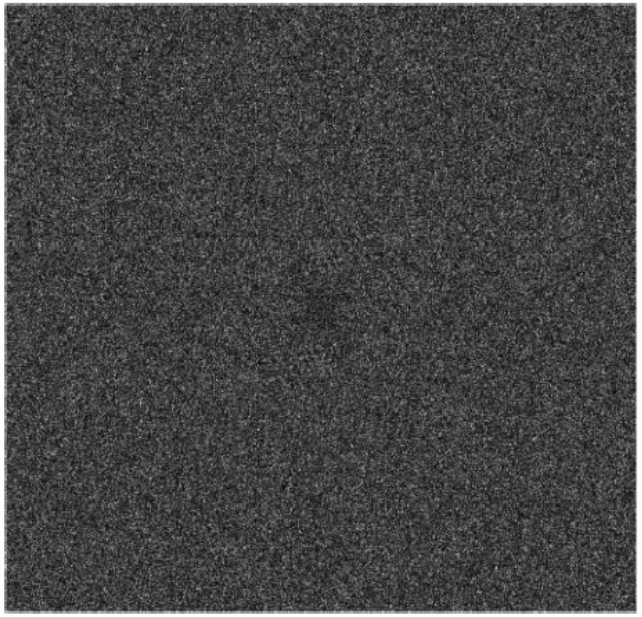
Min Freq Wt Percep. Dist.



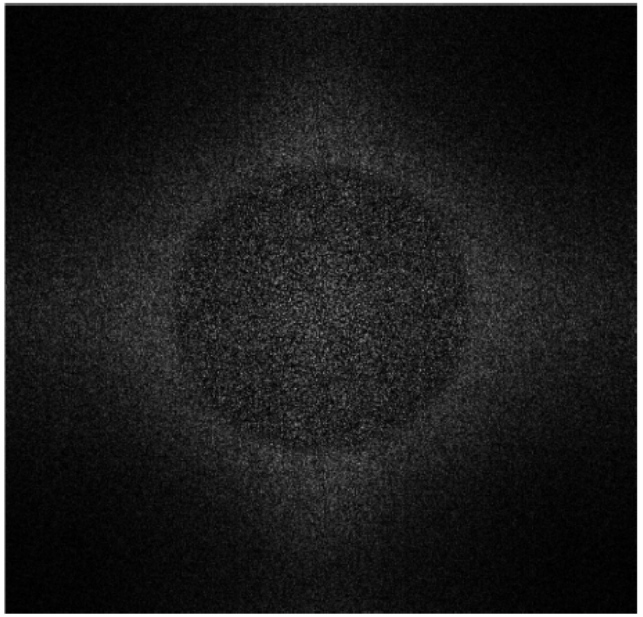
Max Compression Robust.



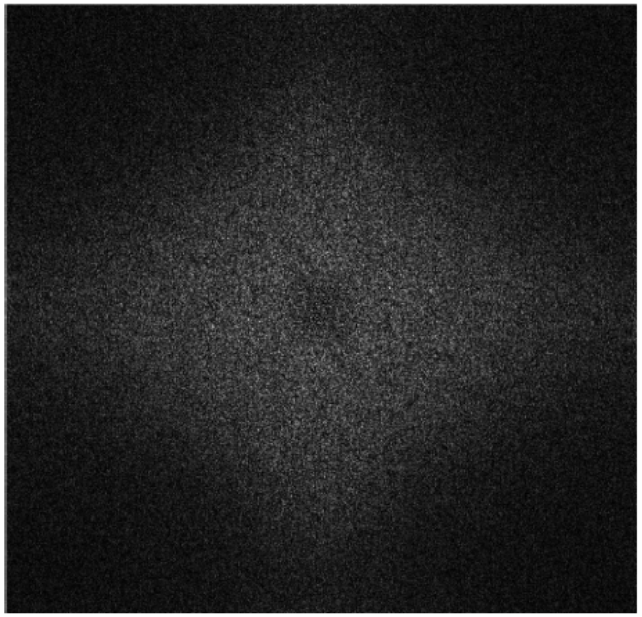
Min Texture Visibility



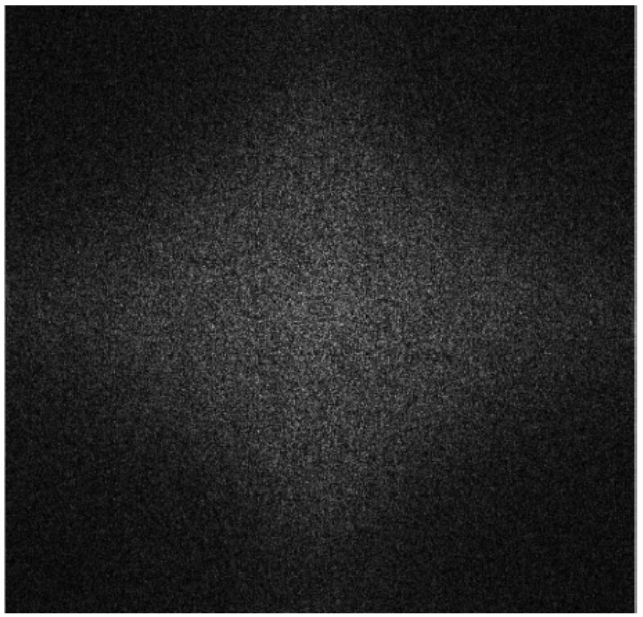
Max Embedding Strength



Min Freq Wt Percep. Dist.



Max Compression Robust.

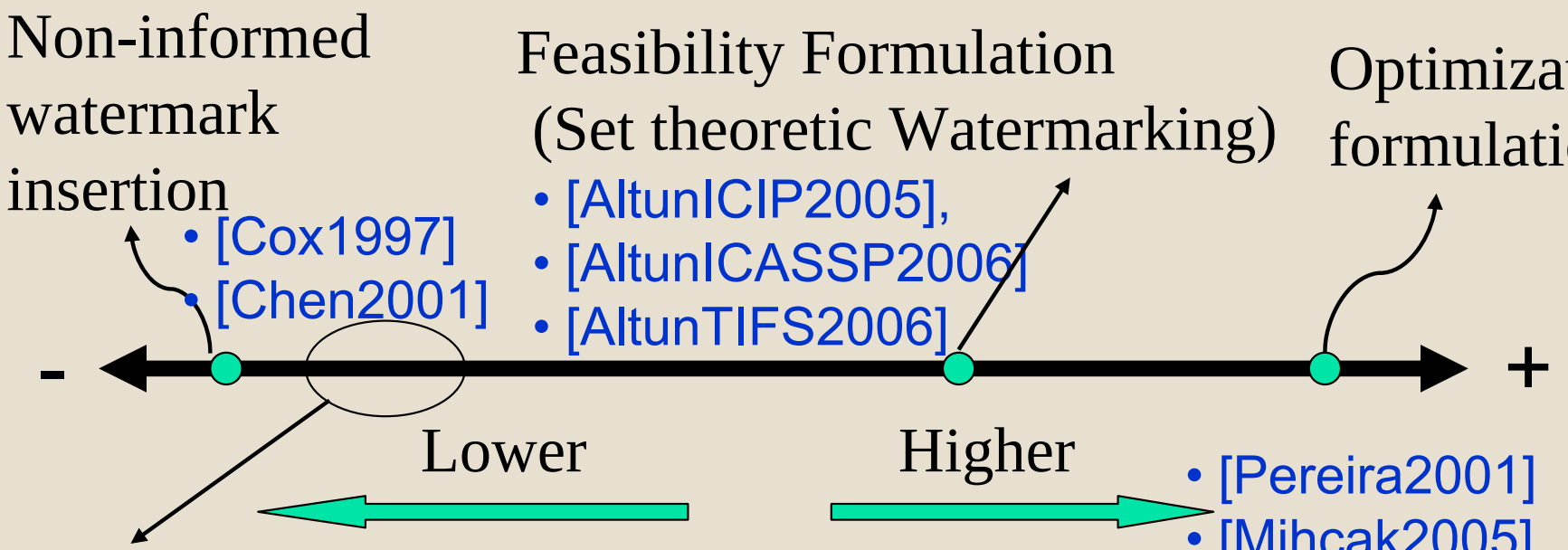


Min Texture Visibility

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



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

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

- [AltunICIP2005]: O.Altun, G.Sharma, M.Celik and M.Bocko, “Semifragile Hierarchical Watermarking In A Set Theoretic Framework,” ICIP, Genoa, Italy, Sep.2005.
- [AltunTIFS2006] O. Altun, G. Sharma, M. Celik and M. Bocko, “Set Theoretical Watermarking And Its Application To Semi-fragile Tamper Detection,” *IEEE Trans. Information Forensics And Security*, vol. 1, no. 4, Dec. 2006, pp. 479-492.
- [AltunICIP2006] O. Altun, G. Sharma, and M. Bocko, “Optimum Watermark Embedding by Vector Space Projections ” *IEEE ICIP,* Sep.2006, Atlanta, Georgia, USA.
- [Cox1997]: I. J. Cox, J. Killian, F. T. Leighton, T. Shamoon, “Secure spread spectrum watermarking for multimedia,” *IEEE Trans. Image Processing,* vol.6, pp. 16731687, Dec. 1997.
- [Chen2001]: B. Chen and G. W. Wornell, “Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding” IEEE Trans. Information Theory,, vol.47, no. 4, pp. 1423-1443, May. 2001.

References

- [Mannos1974]: J. L. Mannos and D. L. Sakrison, “The effects of a visual fidelity criterion on the encoding of images, IEEE Transactions on Information Theory, vol. 20, no. 4, pp. 525–536, Jul. 1974.

- [Mihcak2005]: M. K. Mihcak, R. Venkatesan, and T. Liu, ``Watermarking via Optimization Algorithms for Quantizing Randomized Semi-Global Image Features,'' *ACM Multimedia Systems Journal*, July 2005

- [Pereira2001]:, S. Pereira, S. Voloshynoskiy, and T. Pun “Optimal transform domain watermark embedding via linear programming,” *Signal Processing*, vol. 81, no. 6, pp. 1251–1260, Jun. 2001.

Thank you!

UNIVERSITY of ROCHESTER

IPL