Information Embedding: From Theory to Practice

Pierre Moulin

University of Illinois at Urbana-Champaign

Electrical and Computer Engineering

IEEE Signal Processing Society Distinguished Lecturer Program

2012–2013

Outline

- Overview and applications
- Information-theoretic models and analyses
- From theory to practice

Part I:
Overview and Applications

Information Embedding

- **Imperceptibly** embed message into cover data (e.g. images, video, audio, text, computer programs) and **communicate** to receiver
- Private receiver (uses secret key) *vs* Public receiver

Public Receiver	**Private Receiver Public Communication**	**Private Receiver Secret Communication**
in-band captioning database annotation	DRM for multimedia authentication content ID transaction tracking networking	steganography timing channels

Digital Rights Management

- Watermarking is used for copyright protection of Hollywood releases
- In 2004, watermarking made it possible to trace a bootlegged DVD back to a movie screener for the Motion Picture Academy

Digital Rights Management

- Watermarking is used for copyright protection of Hollywood releases
- In 2004, watermarking made it possible to trace a bootlegged DVD back to a movie screener for the Motion Picture Academy
- Now he has plenty of time to watch DVDs

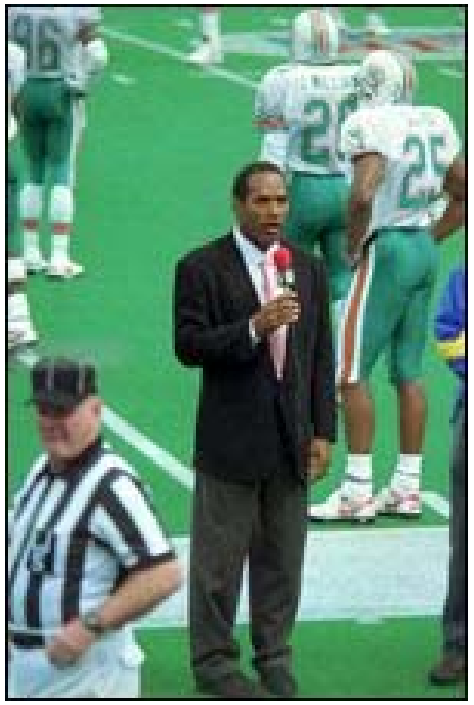
Information Embedding

- **Imperceptibly** embed message into cover data (e.g. images, video, audio, text, computer programs) and **communicate** to receiver
- Private receiver (uses secret key) *vs* Public receiver

Public Receiver	**Private Receiver Public Communication**	**Private Receiver Secret Communication**
in-band captioning database annotation	DRM for multimedia authentication content ID transaction tracking networking	steganography timing channels

Authentication

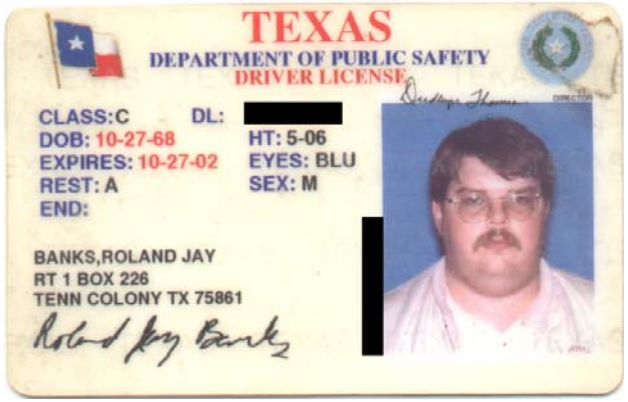
Arrest



O. J. Simpson


Pride in the Past, Progress in
911 EMERGENCY
www.StrangePolice.com

Forgery?



Authentication of driver licenses

Information Embedding

- **Imperceptibly** embed message into cover data (e.g. images, video, audio, text, computer programs) and **communicate** to receiver
- Private receiver (uses secret key) *vs* Public receiver

Public Receiver	**Private Receiver Public Communication**	**Private Receiver Secret Communication**
in-band captioning database annotation	DRM for multimedia authentication content ID transaction tracking networking	steganography timing channels

Steganography

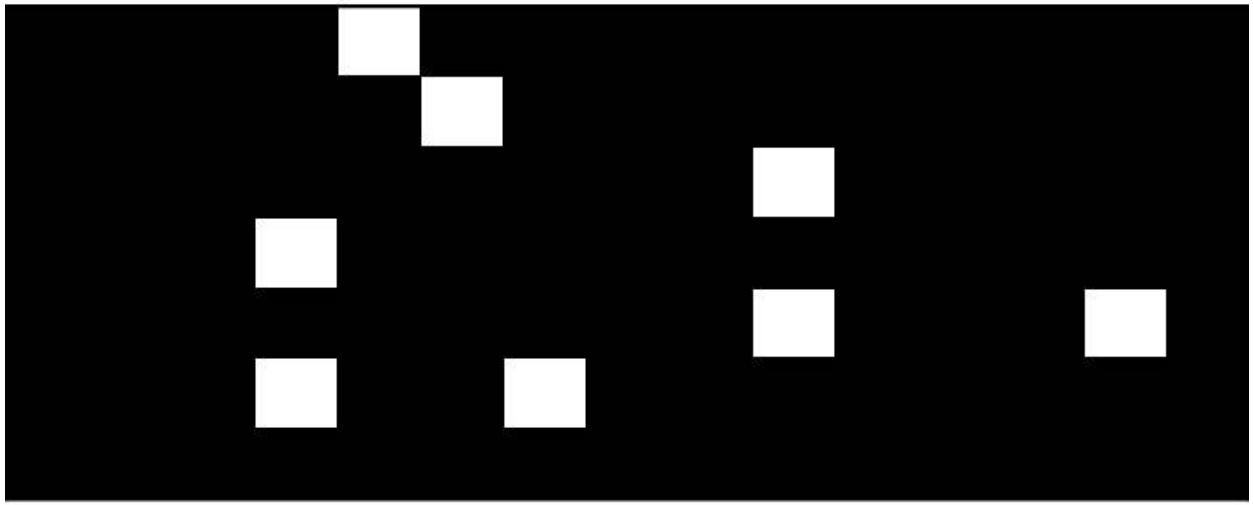
- The ultimate discreet signaling
- Must conceal existence of hidden message
- Applications: spies, military, revolutionaries, terrorists
- Name comes from ancient Greek,

$$\sigma\tau\epsilon\gamma\alpha\nu\omega \;\; \gamma\rho\alpha\phi\omega : \;\; covert\ writing$$

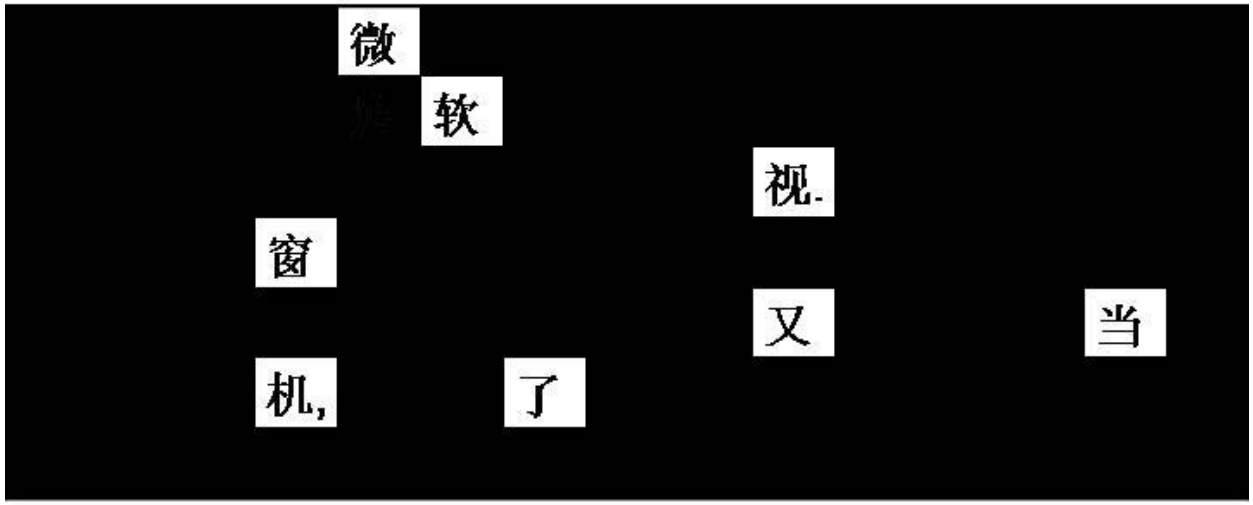
Ancient Chinese Steganography

陛	下	明	鉴:	微	臣	自	受	命	出	师,	一	刻	未	敢
懈	怠.	今	敌	疲	软	于	西,	又	务	于	东,	此	虽	进
趋	之	时	也,	臣	亦	不	敢	轻	视.	臣	本	耕	读	乡
里,	不	闻	窗	外	之	事.	然	陛	下	不	以	臣	卑	鄙,
寄	臣	以	大	事,	尔	来	二	十	又	一	年	矣.	当	此
存	亡	之	机,	唯	盼	了	敌	于	关	外,	以	不	负	陛
下	重	托.												

Secret Mask

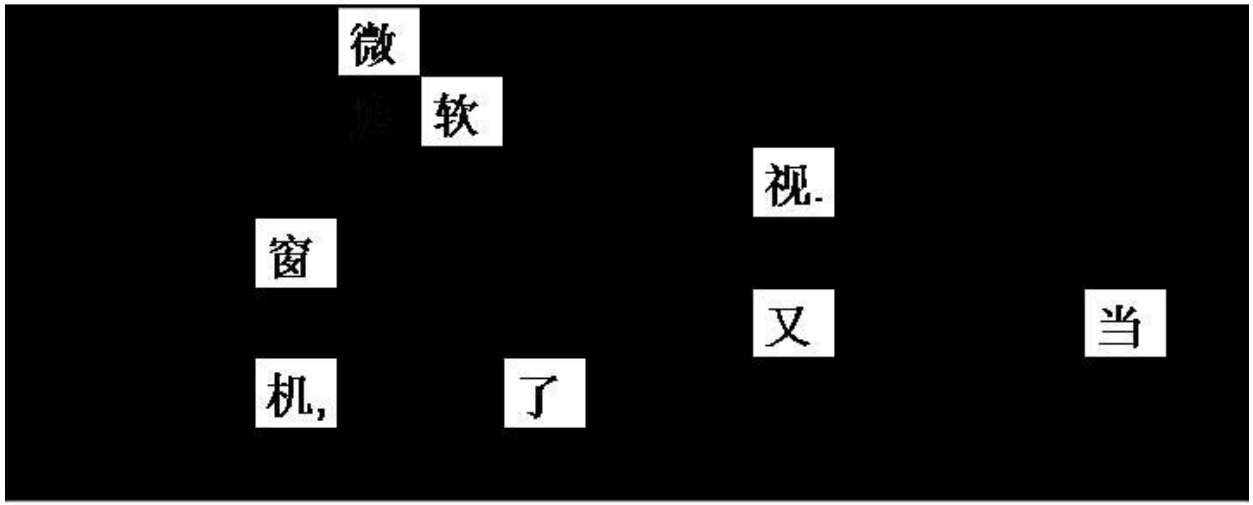


Secret Message



English Translation

Microsoft Windows crashed, again!



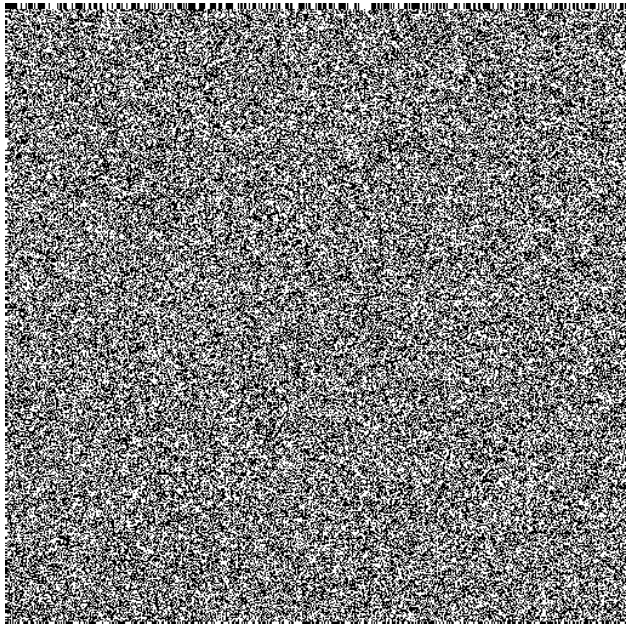
Early Internet Steganography

- **LSB embedding**: a popular image steganography method
- Cover data $\mathbf{s} = \{s_1, s_2, \cdots, s_n\}$
- Each $s_i \in \{0, 1, \cdots, 2^b - 1\}$ (b bits/sample)

$$77 = (01001101)$$

- Replace all n LSB's by hidden binary message
  $\Rightarrow$ rate $R = 1$ bit/sample

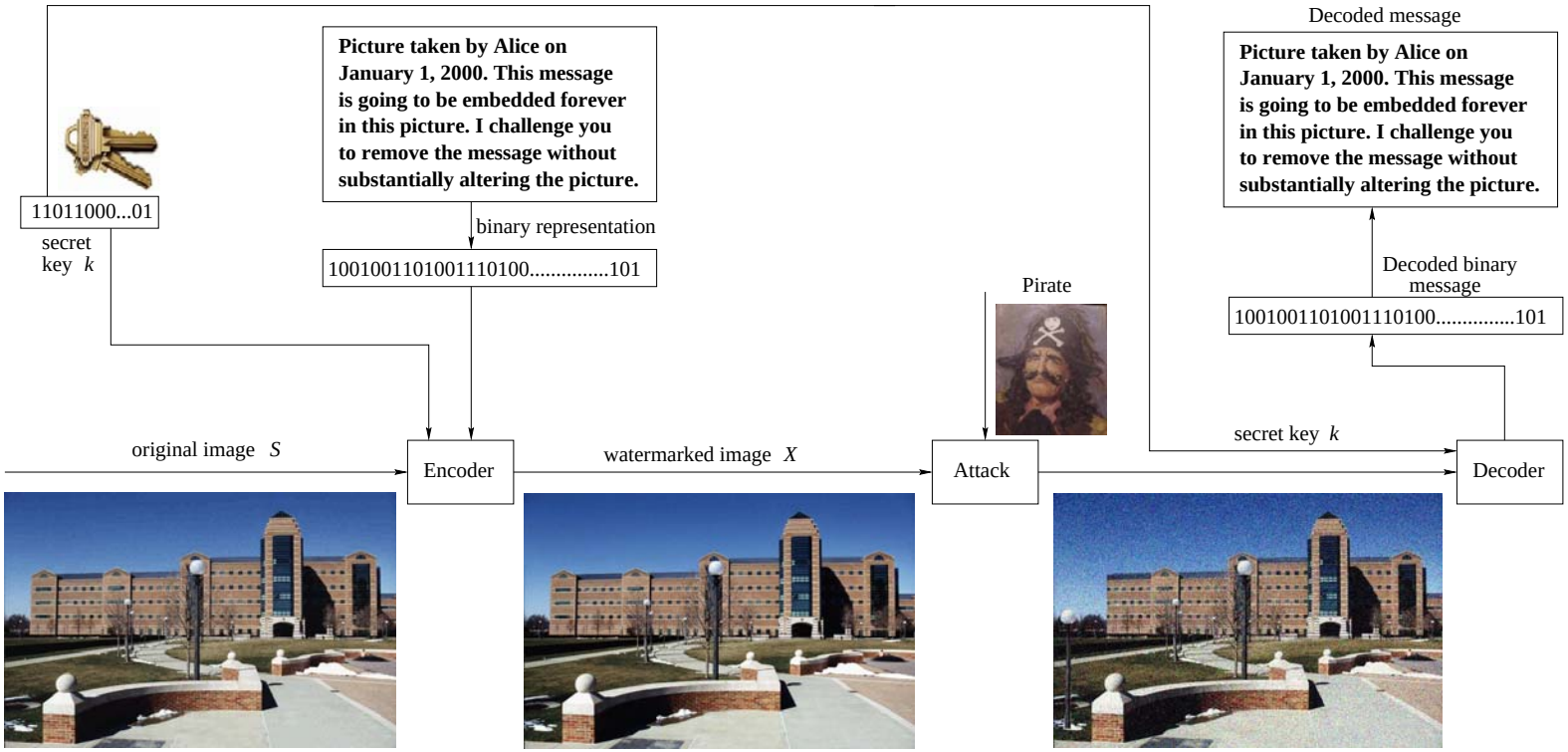
Lena LSB plane



- Invisible but statistically detectable?

Part II: Information-Theoretic Models and Analyses

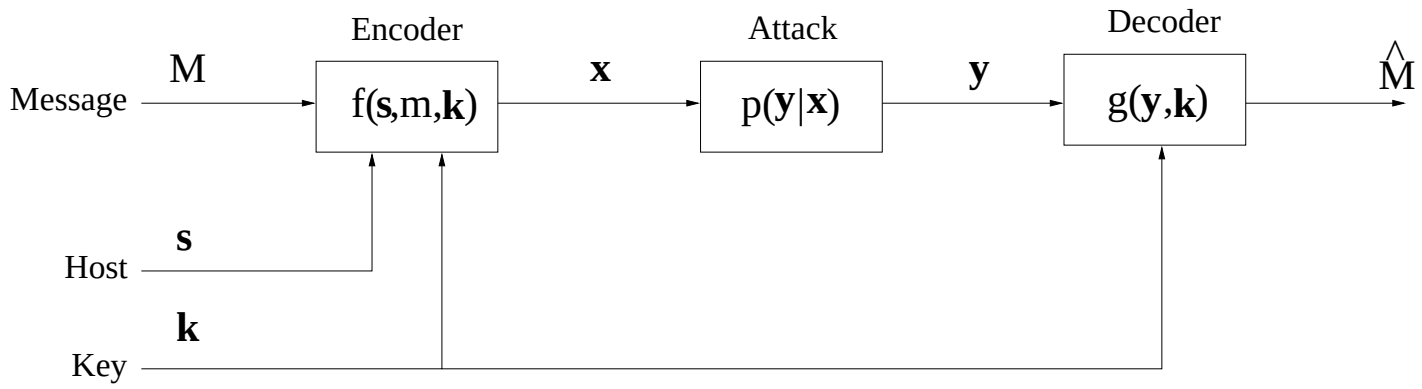
A Generic Problem: Hiding Data in Images



Basic Properties

- **Fidelity** (in terms of signal distortion metric)
  $\leftrightarrow$ discretion level
- **Payload** (number of transmitted bits)
- **Robustness/Security** (against adversary)
- **Detectability** (by steganalyzers/eavesdroppers)

Basic Communication Model



- Encoding function $\mathbf{x} = f(\mathbf{s}, m, \mathbf{k})$
- **Attack channel** $p(\mathbf{y}|\mathbf{x})$ (stochastic)
- **Distortion** constraints on f and $p(\mathbf{y}|\mathbf{x})$
- Decoding function $\hat{m} = g(\mathbf{y}, \mathbf{k})$

System Issues

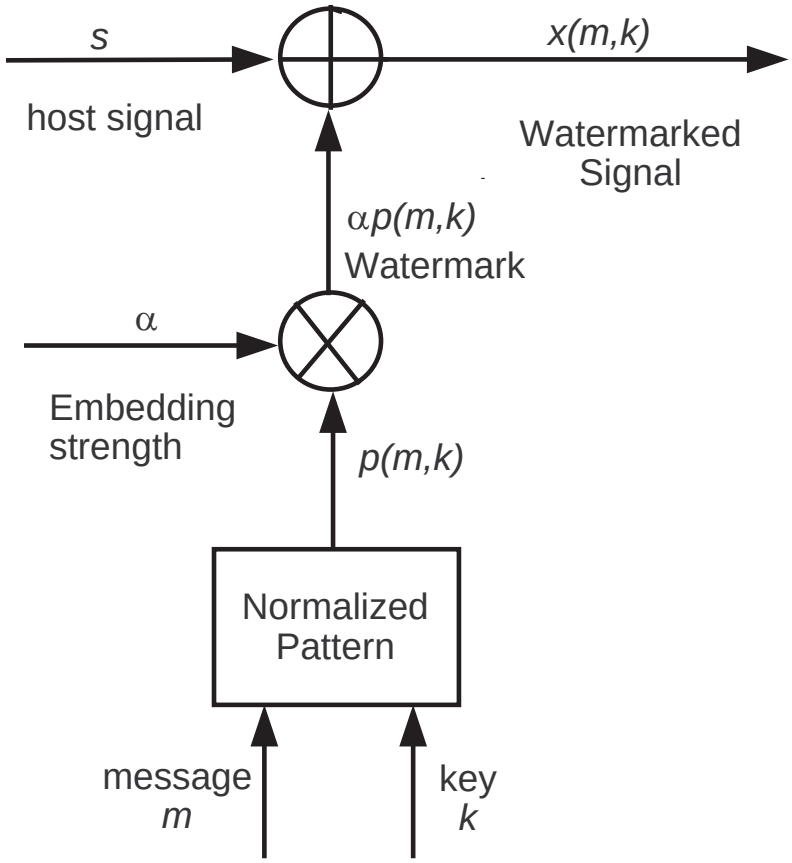
(only partially covered by basic communication model)

- Does receiver know host signal? ($\mathbf{k}$ correlated with $\mathbf{s}$)
  (*blind* vs *nonblind* decoding)
- Communication protocol
- Security level
- Private or public cryptographic system?

Attack Models

- No attack
- "Signal processing" attacks
- Cryptanalysis
- System-level attacks
  (e.g., mosaicing, ambiguity, chosen-plaintext)

The 1990's: Spread-Spectrum Codes



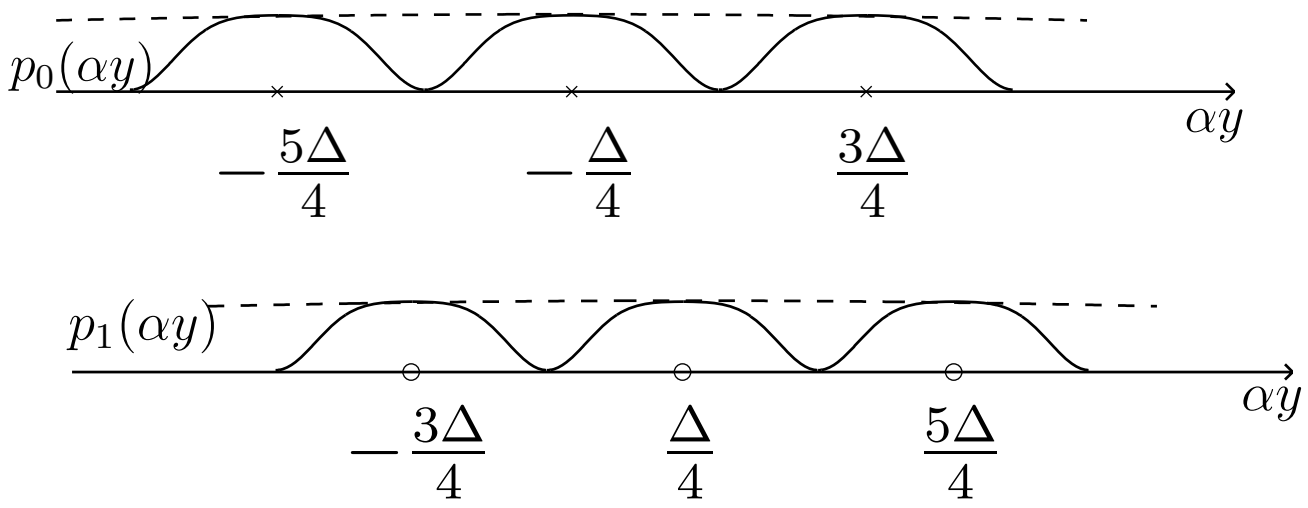
- OK if host **S** is known to receiver
- Weak performance otherwise (**S** is treated as noise)

The 21st Century: Binning Codes

- Fundamental information-theoretic technique
  (Slepian-Wolf 1975; Gel'fand-Pinsker 1980; Costa 1983)
- Host **S** is a **known interference** to encoder
- Can't cancel **S** due to fidelity constraints
- But can "optimally adapt" to **S**
- Natural framework for blind data hiding

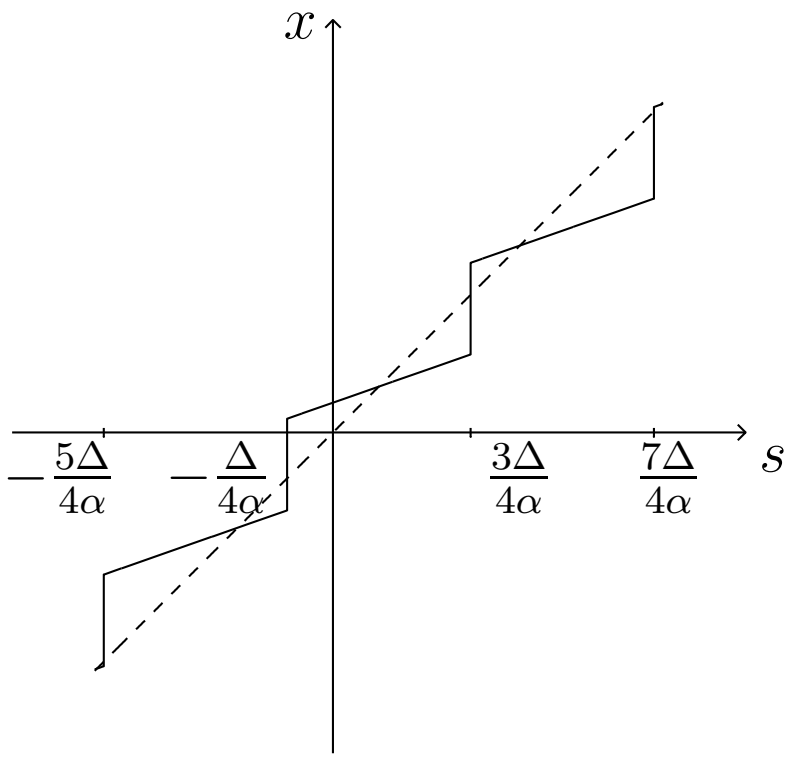
Binning $\leftrightarrow$ pdf shaping

- Embed 1 bit in signal feature $\mathbf{s}$
- Decoder performs statistical test: $Y \sim p_0$ vs $Y \sim p_1$
- Can shape p_0 and p_1 to concentrate information and maximize reliability of test

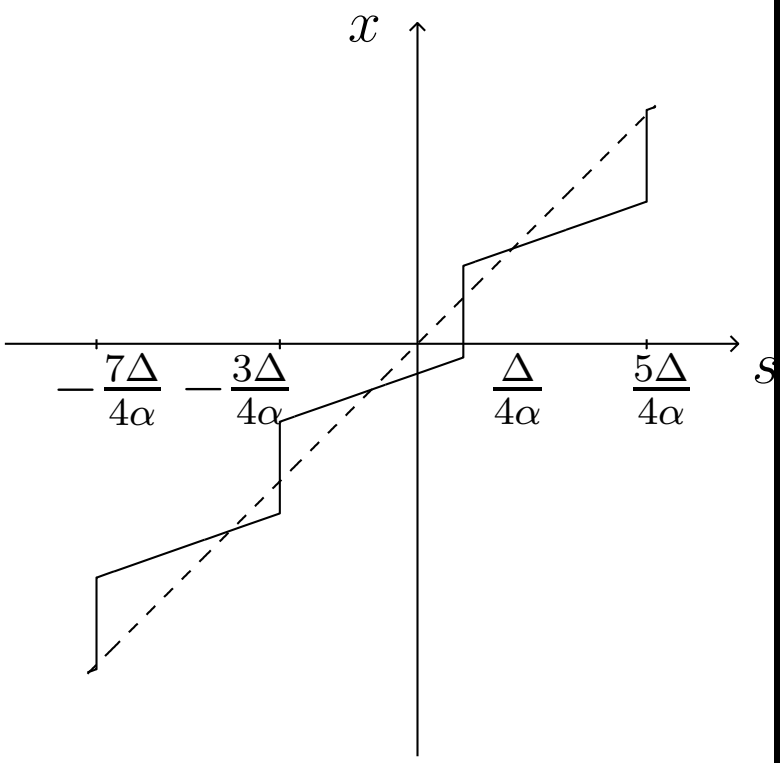


- Can shape p_0 and p_1 using quantization scheme

- Quantization embedding

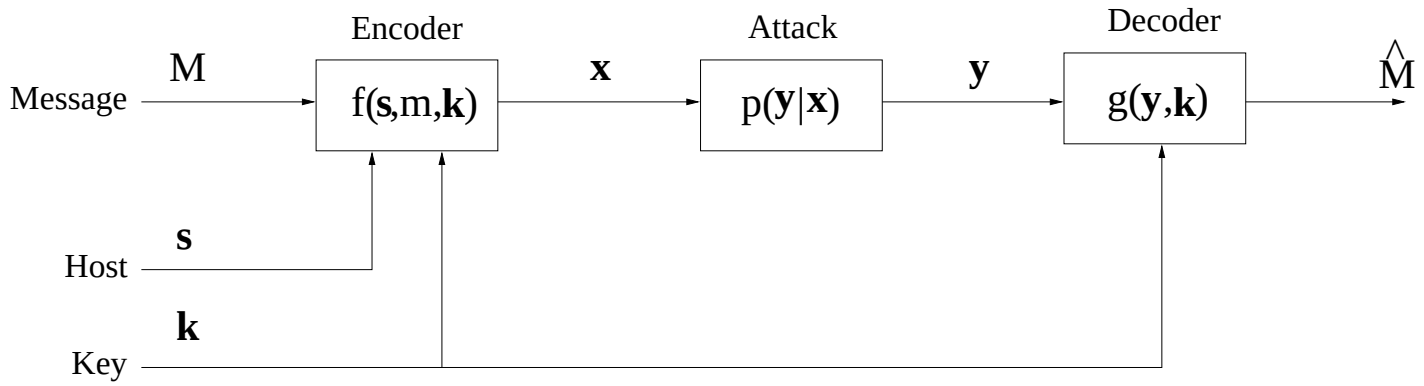


$m = 0$



$m = 1$

Information-Theoretic Limits



- Probability of error $P_{e,N} = Pr[\hat{M} \neq M]$
- Probability mass function $p_S(s)$ (i.i.d. symbols)
- Additive distortion function $d^N(\mathbf{S}, \mathbf{X}) = \frac{1}{N} \sum_{i=1}^{N} d(S_i, X_i)$
- Constraint on encoder: $d^N(\mathbf{S}, \mathbf{X}) \leq D_1$
- Constraint on attacker : $d^N(\mathbf{X}, \mathbf{Y}) \leq D_2$

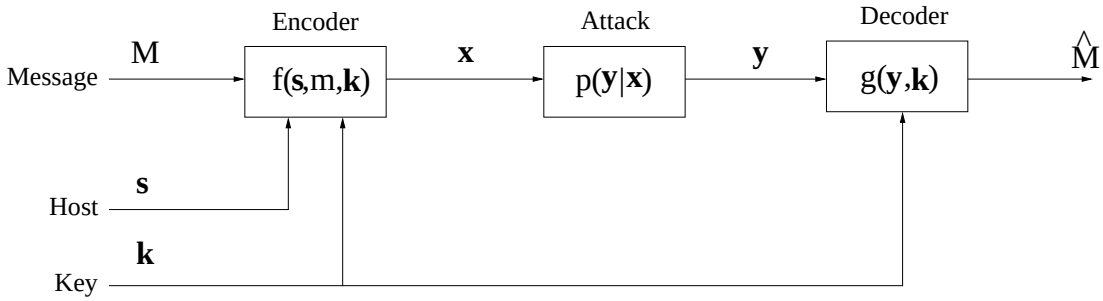
Capacity and Reliability Function

- **Goal**: make $P_{e,N} \to 0$ as $N \to \infty$
- Coding problem with side information (Gel'fand-Pinsker type)
- What is the maximum rate C such that this is possible?

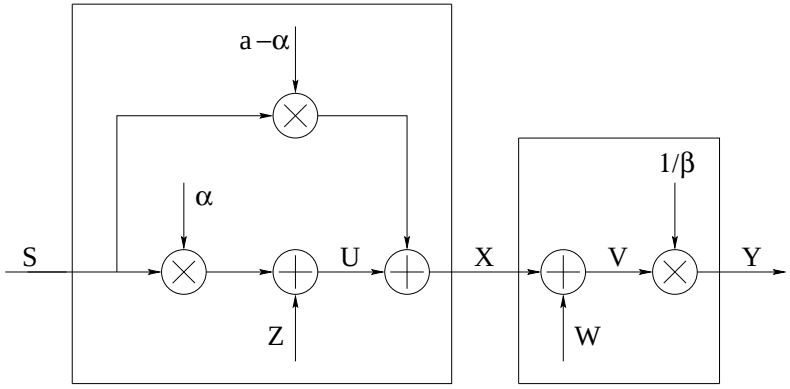
$$C = \max_{Q(x,u|s,k)} \min_{A(y|x)} [I(U;Y,K) - I(U;S,K)]$$

- Mathematical expressions for capacity can be derived and evaluated numerically
- The capacity limit is achievable by random binning

Gaussian Case

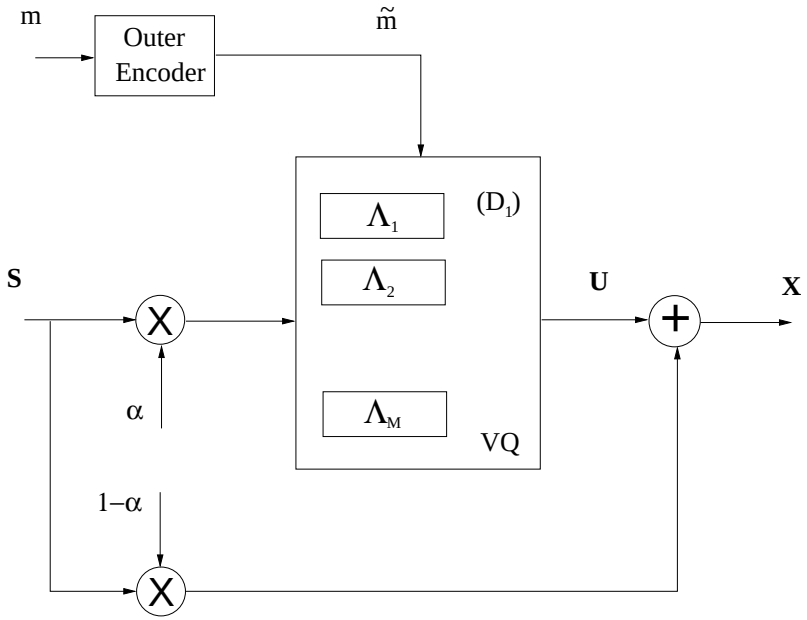


- Host $\mathbf{S}$ is i.i.d. Gaussian, MSE distortion constraints D_1, D_2
- $\sigma_S^2 \gg D_1$ (large interference) $\Rightarrow \quad C \sim \frac{1}{2}\log\left(1+\frac{D_1}{D_2}\right)$
- Perfect interference cancellation!
- C-achieving distributions are Gaussian:

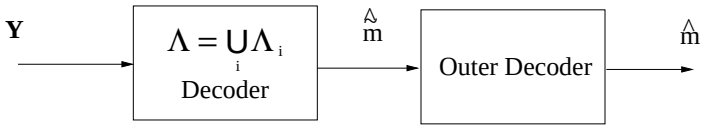


Lattice VQ Based Binning Codes

- Decompose lattice Λ into cosets $\Lambda_1, \Lambda_2, \cdots, \Lambda_M$



Encoder



Decoder

- Capacity-achieving family!
- Outperforms Spread Spectrum codes

Part III:
From Theory to Practice

Hiding Data in Images

Lena

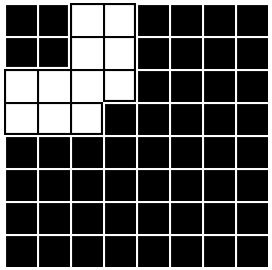
Block-DCT coefficients

- Parallel-Gaussian model for host
- Weighted MSE metric
- $D_2 = 5D_1 \quad \Rightarrow C \approx 0.01$ bpp

Practical IT-Based Codes

(Solanki et al. 2004)

Active Blocks



Selected DCT coefficients

- Order selected DCT coefficients into a sequence
- Interleave information bits, concatenate Reed-Solomon code with quantization code

- Embed 14,336 bits ($R = 0.055$ bpp)
- Withstands erasures and deletions

- Error-free recovery of the information bits

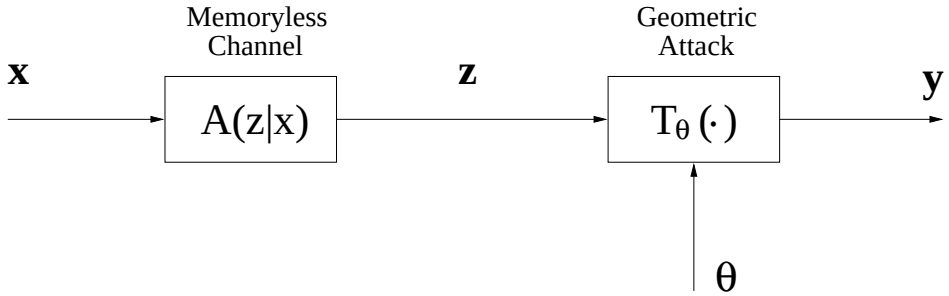
Simple Geometric Attacks

Shifted Lena

Lena

Rotated Lena

- General model: parametric class $\{T_\theta, \theta \in \Theta\}$ of attacks



- No loss in capacity relative to coherent case

Complex Geometric Attacks

Lena Warped Lena

- The "noncoherent penalty" can be severe when θ is time-varying, e.g., warping or random bending
- There exist good binning codes, but constructing practical ones is difficult!

Steganography

- Data hiding with undetectability requirement
- Assume steganalyzer knows f and statistics of $\mathbf{S}$ and tests

$$\begin{cases} \text{hypothesis } H_0 \;:\; \mathbf{X} \sim p_{\mathbf{s}} & \text{no hidden data} \\ \text{hypothesis } H_1 \;:\; \mathbf{X} \sim p_{\mathbf{x}} & \text{hidden data} \end{cases}$$

- *Perfect Secrecy* condition: $p_{\mathbf{x}} = p_{\mathbf{s}}$
- Randomized codes

Conclusion

- Specify communication model, including distortion and robustness levels
- Information Theory
  - provides fundamental performance bounds
  - guides the development of good practical schemes

For more details, see Moulin and Koetter, "Data-Hiding Codes," *Proceedings of the IEEE*, December 2005.