SESSION 6: APPLICATIONS & ADVANCED TOPICS

- Data-Hiding Codes for Images
- Desynchronization Attacks
- Authentication
- Steganography
- Fingerprinting
Data-Hiding Codes for Images

- Wavelets → approximate parallel-Gaussian model
With embedded data

\[ D_1 = 10 \]

\[ C(D_1, D_2) = 5297 \text{ bits} \]

Attacked

\[ D_2 = 50 \]
Decoding Performance for 3 QIM schemes

Operational $P_{be}$ vs $D_2/D_1$ for Lena with $D_1 = 10$.
Rate $R(D_2) = \frac{1}{10} C(D_2)$. 
Desynchronization Attacks

- Such attacks are perceptually benign but can disable basic detectors
- Delays (fixed or time-varying)
  \[ y(n) = x(n - \theta) + w(n) \]
- Amplitude scaling (valumetric attacks)
  \[ y(n) = \theta x(n) + w(n) \]
- Offsets
  \[ y(n) = \theta + x(n) \]
- Erasures and Insertions

Can you read this sentence?
Warping Attack on Lena

lena with $\rho=.995$ max shift 15
Desynchronized QIM Decoders

\[
\begin{align*}
    D'_2 &= D_2 + \theta^2 \\
    D'_2 &\sim D_2 + (\theta - 1)^2 \frac{\|x\|^2}{N} \\
    D'_2 &\sim D_2 + \theta^2 \frac{\|x\|^2}{N}
\end{align*}
\]

\[\Rightarrow \text{catastrophic performance degradation}\]
Improved QIM Decoders

- Motivation: desync attacks have *benign effect on capacity*
- Use pilot sequences for estimating desync parameters
- Use Reed-Solomon codes for coping with an equal number of insertions & deletions
- Use Davey-Mackay codes for coping with more general insertions, deletions & substitutions
Steganography

- *Existence* of hidden message should be concealed
- Can be addressed in information-theoretic framework
- Additional constraint:
  marked $X$ must be *typical* of host signal distribution
- For instance, capacity is generally *slightly lower* than without steganography constraint:

$$C(D_1, D_2) = \max_Q \min_{\mathcal{A}} \frac{1}{Q} \left( I(U; Y|K) - I(U; S|K) \right)$$

where $\max_Q$ is subject to the constraint $p_X = p_S$
Authentication

- Probability of error $P_{e,N} = Pr[\hat{M} \neq M]$
- Probability distribution $p(s^N, k^N)$ (iid symbols)
- Composite binary hypothesis test: $H_0$ vs $H_1$; $A$ viewed as a nuisance parameter
- Detection rule: $\hat{M} = \phi(y^N, k^N) \in \{0, 1\}$
Detection Rule

- Probability of false alarm $P_{FA}$ ("false positives")
  \[ P_{FA} = Pr[\hat{M} = 1|M = 0] \]
- Probability of miss $P_M$ ("false negatives")
  \[ P_M = Pr[\hat{M} = 0|M = 1] \]
- Probability of error $P_e = Pr[\hat{M} \neq M]$
Optimal Detector

• Given $A$, Likelihood Ratio Test (LRT)

\[
\frac{p(y^N, k^N | H_1)}{p(y^N, k^N | H_0)} \begin{cases} 
H_1 & > \tau \\
H_0 & < \tau
\end{cases}
\]

is optimal under classical optimality criteria (Bayes, minimax, Neyman-Pearson)

• Two approaches when $A$ is unknown:
  – Assume a prior distribution $p(A)$
    \[ \Rightarrow \phi = \text{simple hypothesis test} \]
  – In some problems, optimal $\phi$ is still a LRT designed under the worst-case $A$
The Authentication Game

- Assume information hider does not know attack channel $A$
- Assume attacker knows WM code $f$ but not secret key $k^N$
- Assume decoder knows WM code $f$ and attack channel $A$
- Constraint on encoder: $f \in \mathcal{F}$
- Constraint on attacker: $A \in \mathcal{A}$
- Solve $\min_{f \in \mathcal{F}} \max_{A \in \mathcal{A}} P_{e,N}(f, A)$
Application to Blind SSM Watermarking

Probability of error as a function of $D_w$ ($D_a = 2D_w$) using Lena and Daubechies’ 9/7 filters
Significance Map

Significance map, D9/7 3–level $D = 6e^{-05}$; $E = 3e^{-05}$

$$D_w = 10^{-5} \text{ and } D_a = 2D_w$$
An Optimal Watermark

Watermarked image D9/7 3-level $D = 0.0001$; $E = 5e-05$; psnr = 43.8936; snr = 38.2372

\[ D_w = 5 \times 10^{-5}, \quad D_a = 2D_w \]
Fingerprinting

- $L$ users collude and attempt to remove watermark
Thanks
To grad. students Mustafa Kesal, Anil Goteti, Aleksandar Ivanović, Alexia Briassouli, Tie Liu
To Dr. M. Kivanç Mihçak
To Profs. Joseph A. O’ Sullivan and Ralf Koetter
To National Science Foundation: grants CCR 00-81268 and CCR 02-08809 and infrastructure grant CDA 96-24396
To all of you for attending!