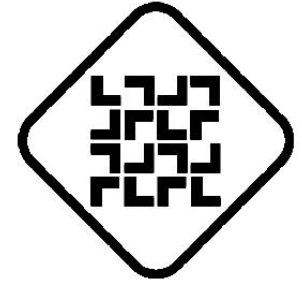




Sharif University of Technology



Iranian Society of Cryptography

Information Theoretic Analysis of Information Hiding

Hanieh Khalilian

Outline

- Introduction
- Information Theoretic Model
- Different Approaches of Capacity Evaluation
- Information Hiding Game
- Capacity Evaluation
- Gaussian Channels
- Practical Case
- Experimental Results
- Conclusion
- Future Work

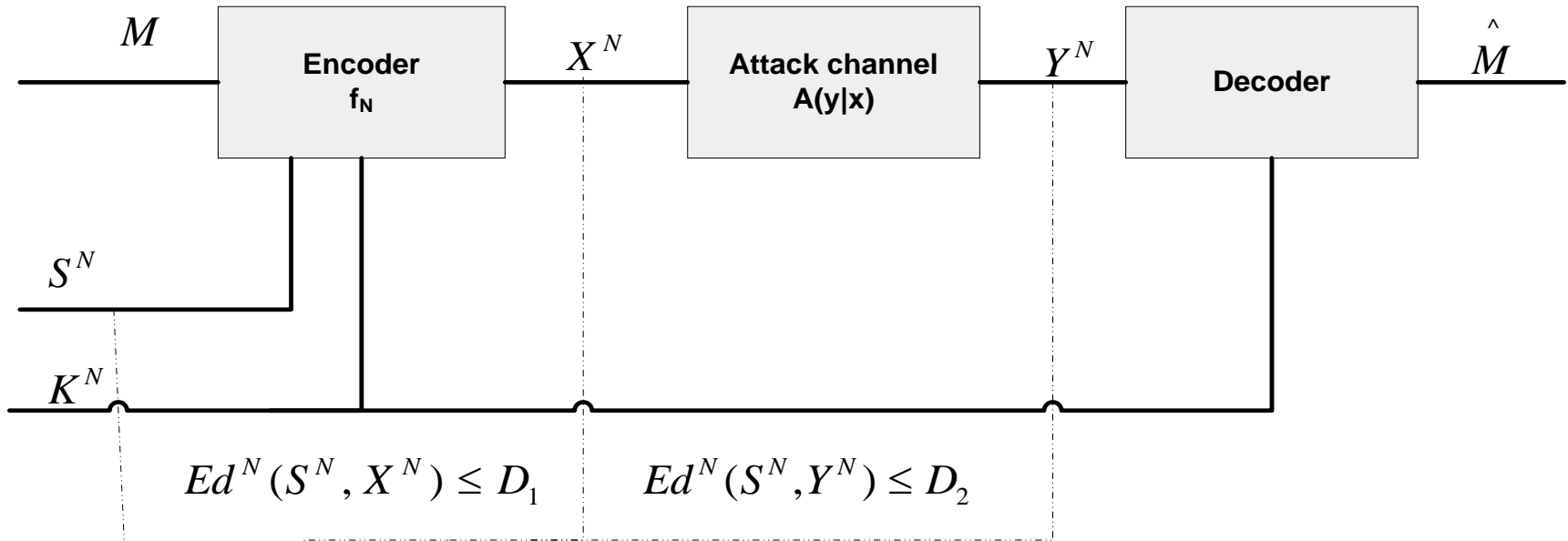
Introduction

Data hiding capacity is an evaluation of how much information can be hidden within a host signal while satisfying invisibility and robustness.

It depends on:

- Statistical model used for the host signal
- Distortion constraints on the data hider and attacker
- Information available to the data hider, attacker, and decoder

Information Theoretic Model

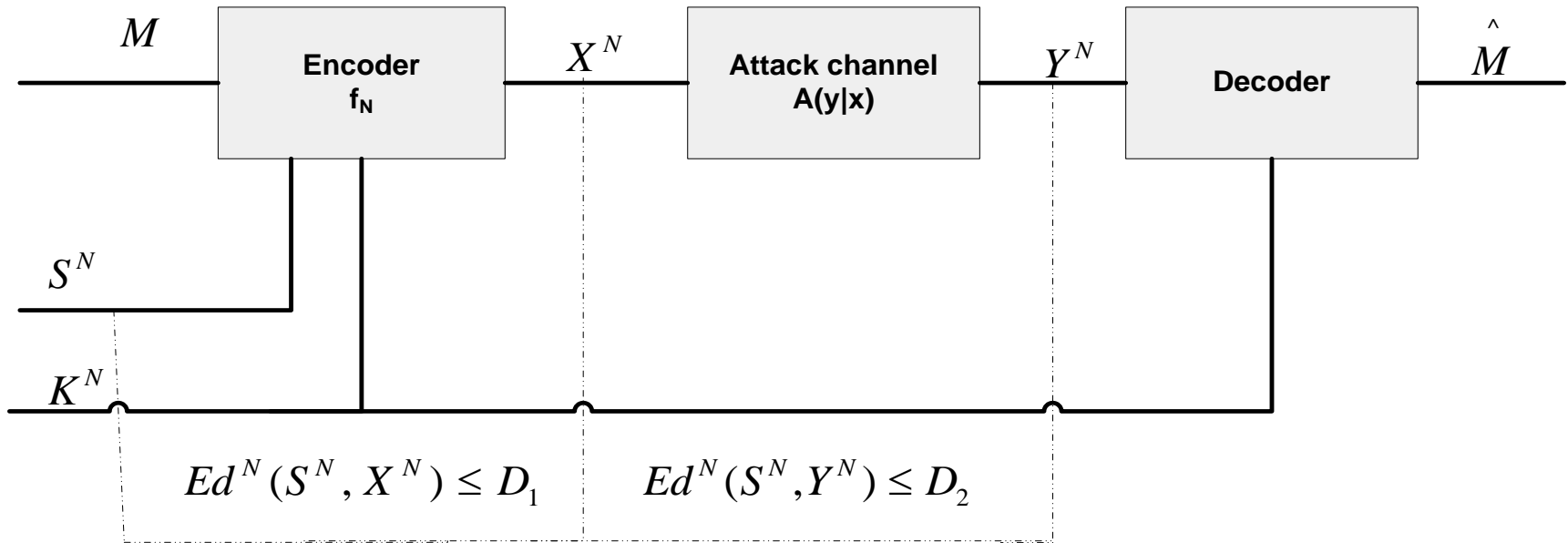


M = Hidden Data

S = Host Signal

K = Side Information

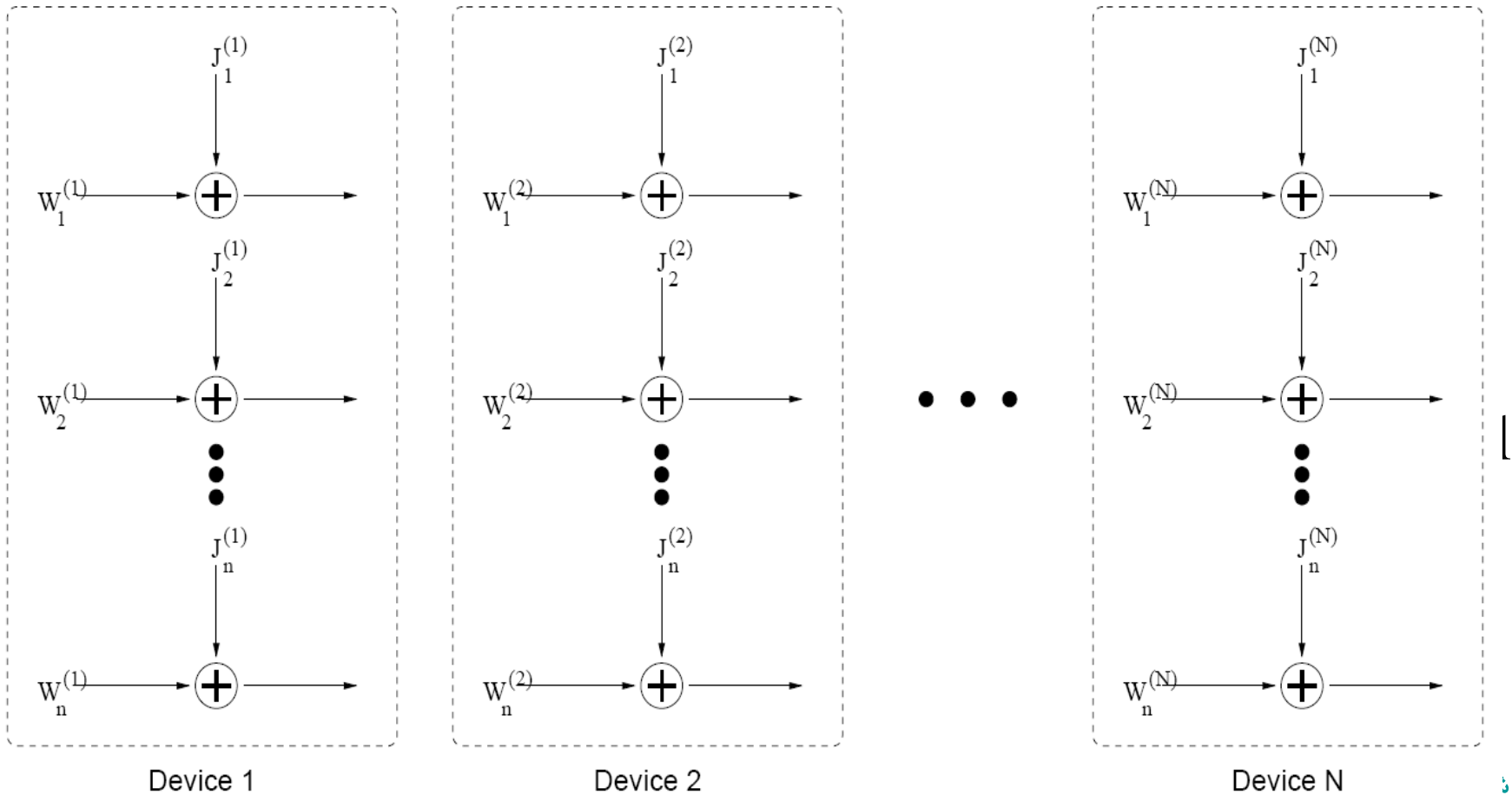
Information Theoretic Model



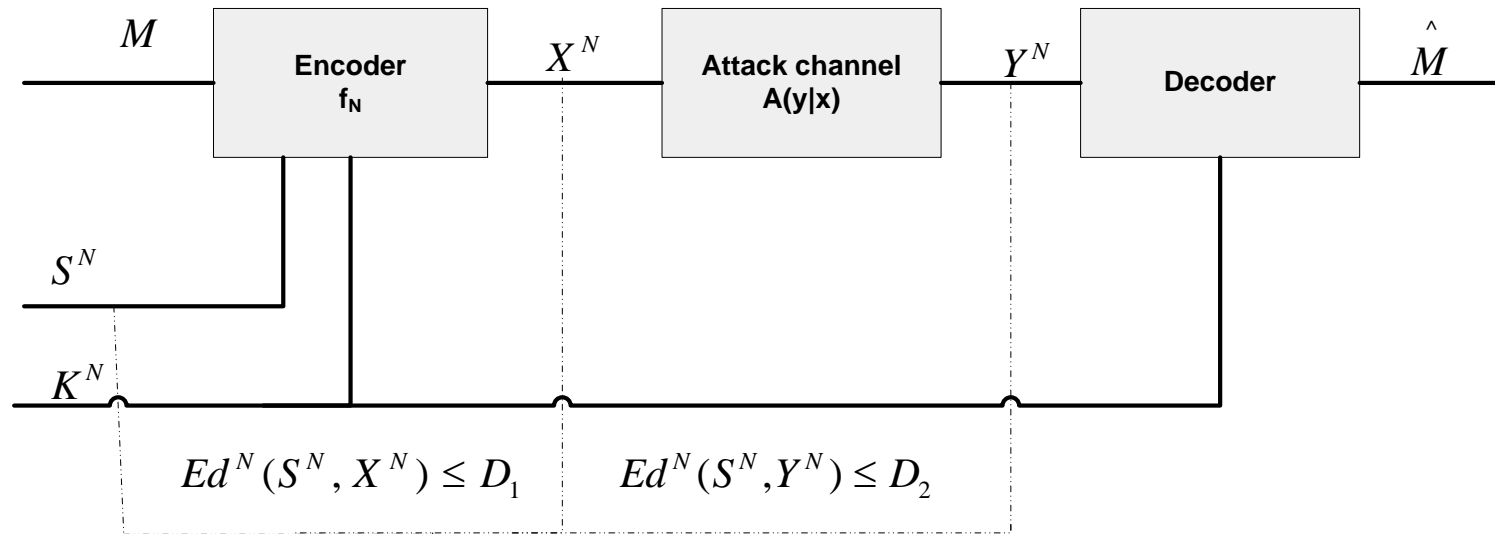
D_1 = maximum allowable distortion by information hider

D_2 = maximum allowable distortion by attacker

Different Approaches of Capacity Evaluation



The Information Hiding Game



First party: encoder and decoder

Second party: attacker

Payoff function: rate, error probability

The Information Hiding Game

Three scenarios:

$$1 \quad J^* = \max_{f_N} \min_{A^N} \max_{\phi_N} J(f_N, A^N, \phi_N)$$

$$2 \quad \underline{J} = \max_{f, \phi} \min_A J(f_N, A^N, \phi_N)$$

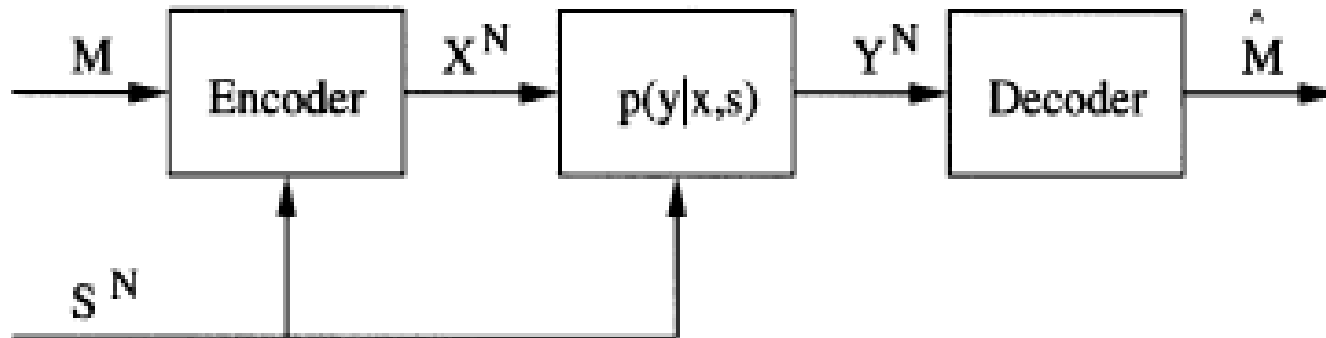
$$3 \quad \bar{J} = \min_A \max_{f, \phi} J(f_N, A^N, \phi_N)$$

Channel Identification: (1)=(2)

The Information Hiding Game

Payoff function

Channel with random parameter



$$U \rightarrow (S, X) \rightarrow Y$$

$$C = \max[I(U; Y) - I(U; S)]$$

The Information Hiding Game

Four difference between our systems and Pinsker's:

- Distortion constraint
- Side information at the encoder and decoder
- Encoder does not know the attack channel
- Unavailability of S to the attacker

$$(USK) \rightarrow X \rightarrow Y$$

The Information Hiding Game

Payoff function

$$J(Q, A) = I(U; Y | K) - I(U; S | K)$$

$$I(U; Y, K) - I(U; S, K) =$$

$$H(U | S, K) - H(U | Y, K)$$

$$C = \max_Q \min_A J(Q, A)$$

Non-blind data hiding: $C = \max_{p(x|s)} \min_{A(y|x)} I(X; Y | S)$

No attack (blind or non-blind): $C = \max H(X | S)$

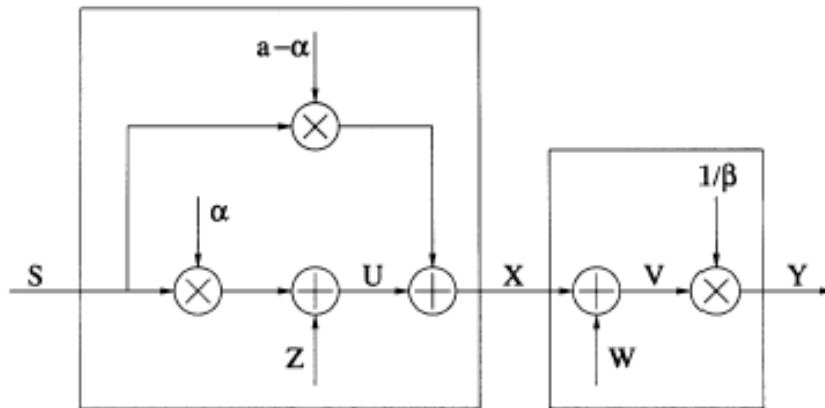
Capacity

Binary Channels

Gaussian Channels

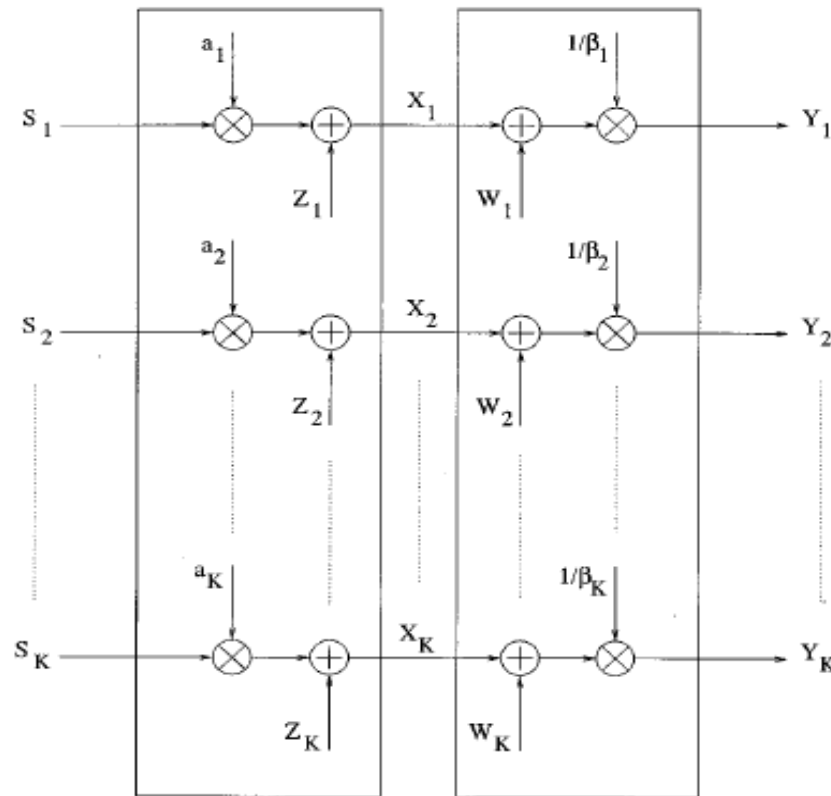
$$d_1(x, y) = d_2(x, y) = (x - y)^2$$

$$d_i^N(x^N, y^N) = \frac{1}{N} \sum_{k=1}^N d_i(x_k, y_k)$$



$$\Gamma(\sigma^2, D_1, D_2)$$

Practical Case



$$C = \max_{d_1} \min_{d_2} \sum_{k=1}^K r_k \Gamma(\sigma_k^2, d_{1k}, d_{2k})$$

Practical Case

Optimal power allocation for parallel Gaussian channels
in rate distortion theory and channel coding

Constraints: $(3K+2)$

$$\sum_{k=1}^K r_k d_{1k} \leq D_1 \quad 0 \leq d_{1k}$$
$$\sum_{k=1}^K r_k d_{2k} \leq D_2 \quad d_{1k} \leq d_{2k}$$
$$\quad \quad \quad \quad \quad \quad \quad d_{2k} \leq \sigma_k^2$$

Spike approximation:

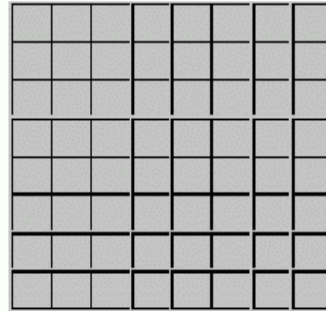
Two channel: strong and weak

$$C = \frac{1}{2} r^* \log\left(1 + \frac{D_1}{D_2 - D_1}\right)$$

DCT Model



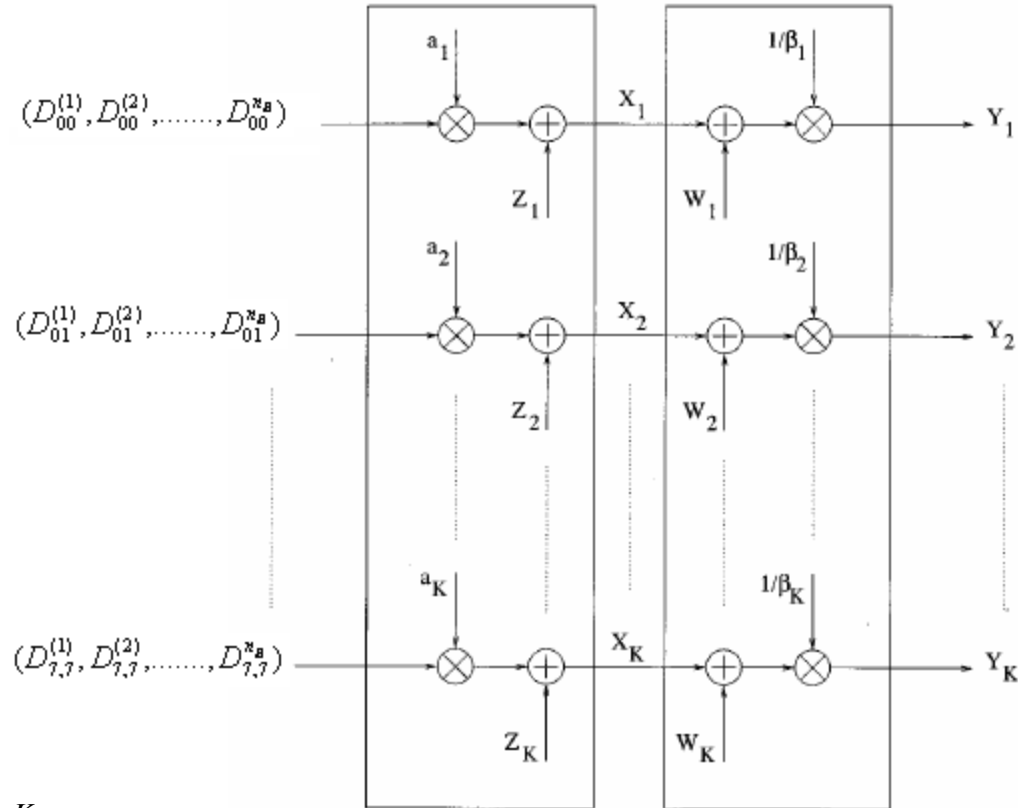
DCT
→



64 equal size channels

Assumption: Data in each channel are i.i.d. Gaussian

DCT Model



$$C = \max_{d_1} \min_{d_2} \sum_{k=1}^K r_k \Gamma(\sigma_k^2, d_{1k}, d_{2k})$$

DCT Model

Problems:

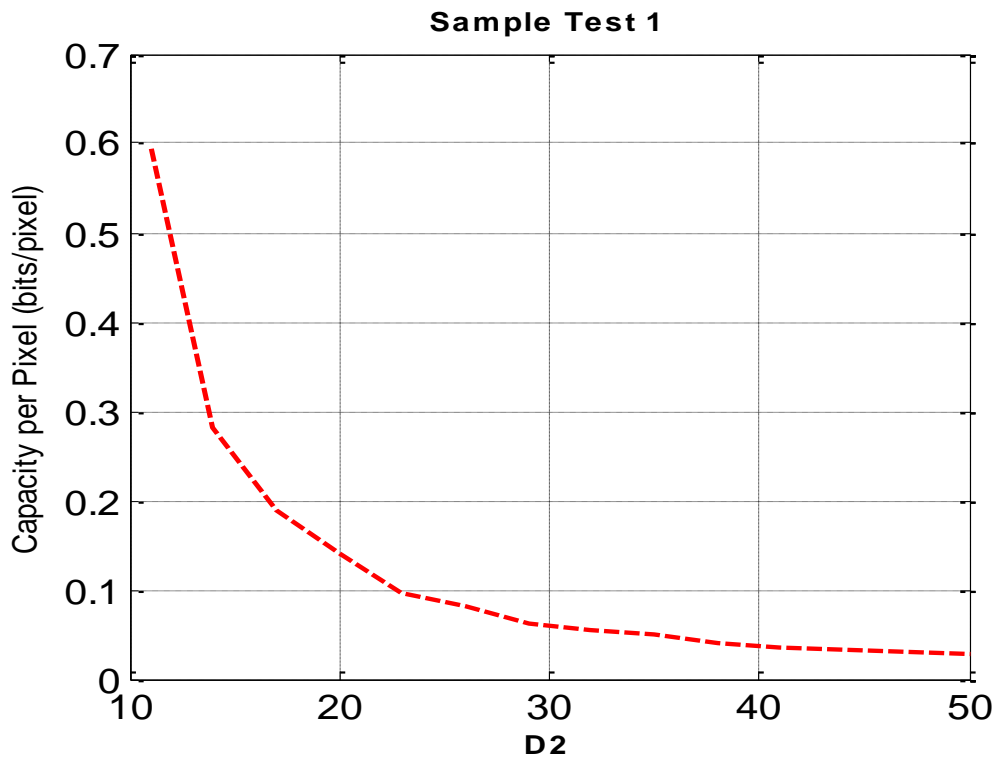
DC coefficients of adjacent channel are not independent

Laplacian models are used for DCT coefficients



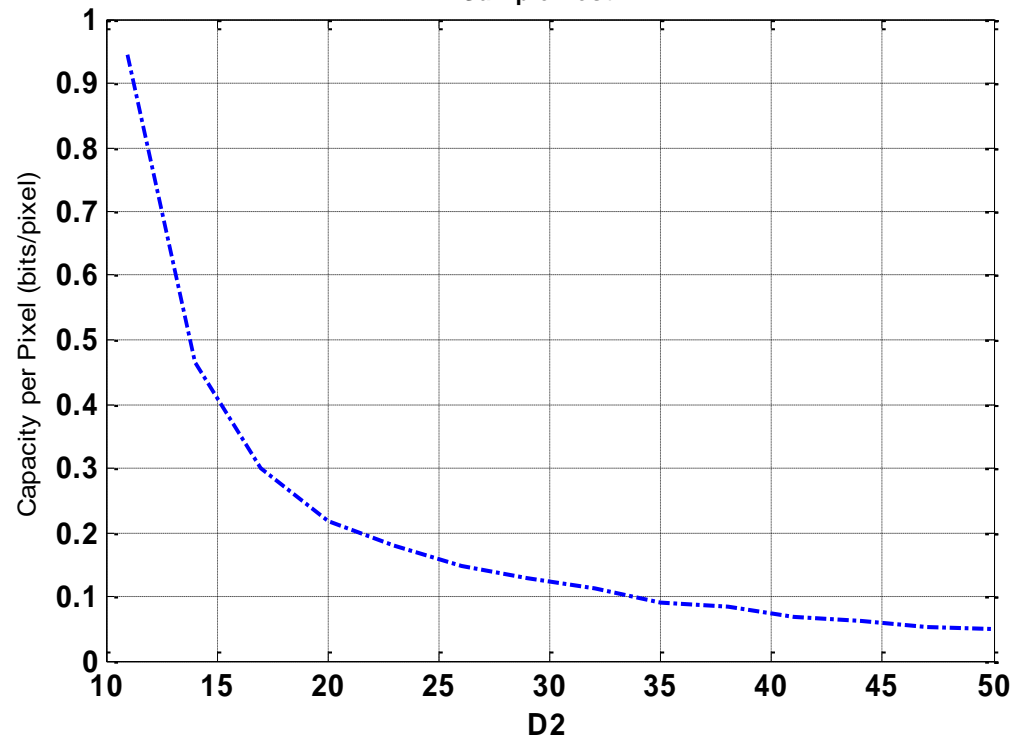
Game theoretic approach give an upper bound for capacity

Sample Test 1

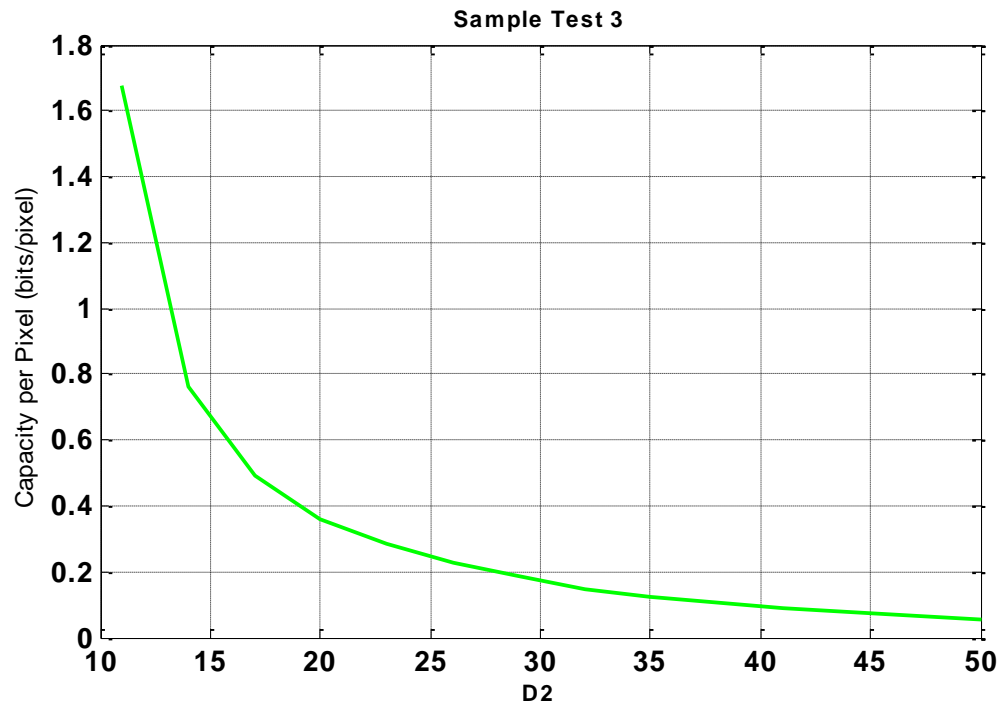


Sample Test 2

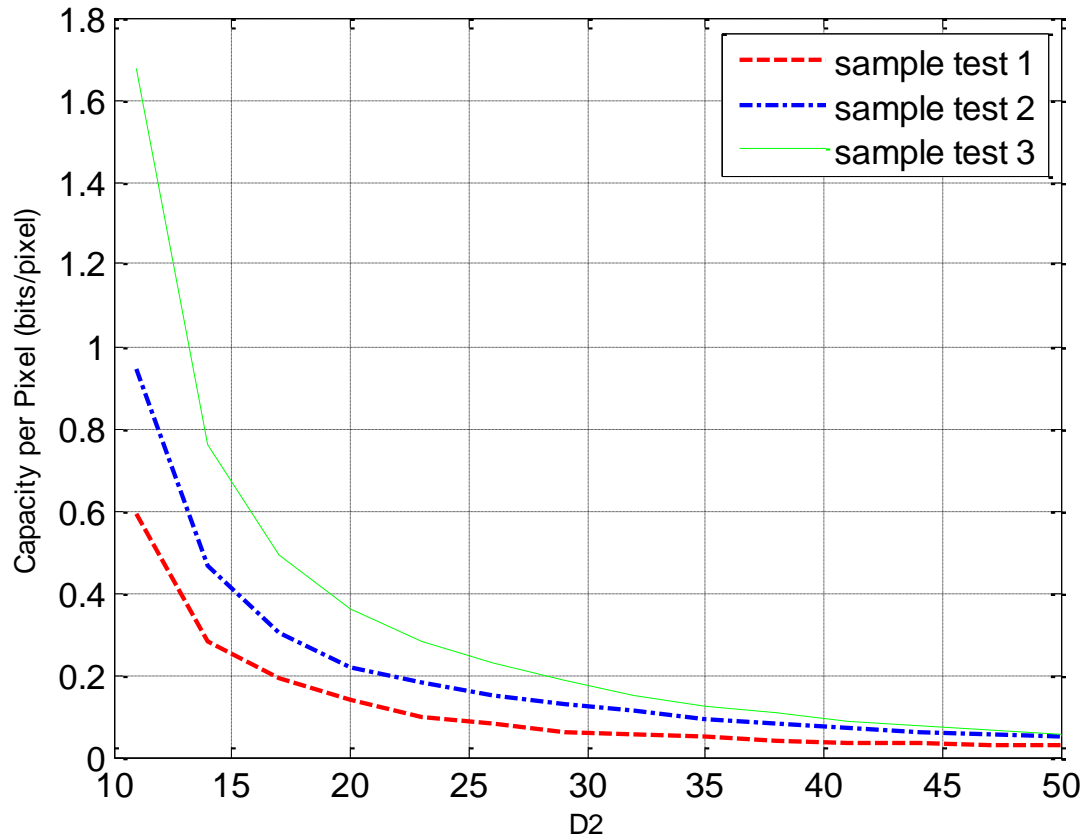
Sample Test 2



Sample Test 3



Comparison



Wavelet Model

Wavelet Transform

Estimation of local variance

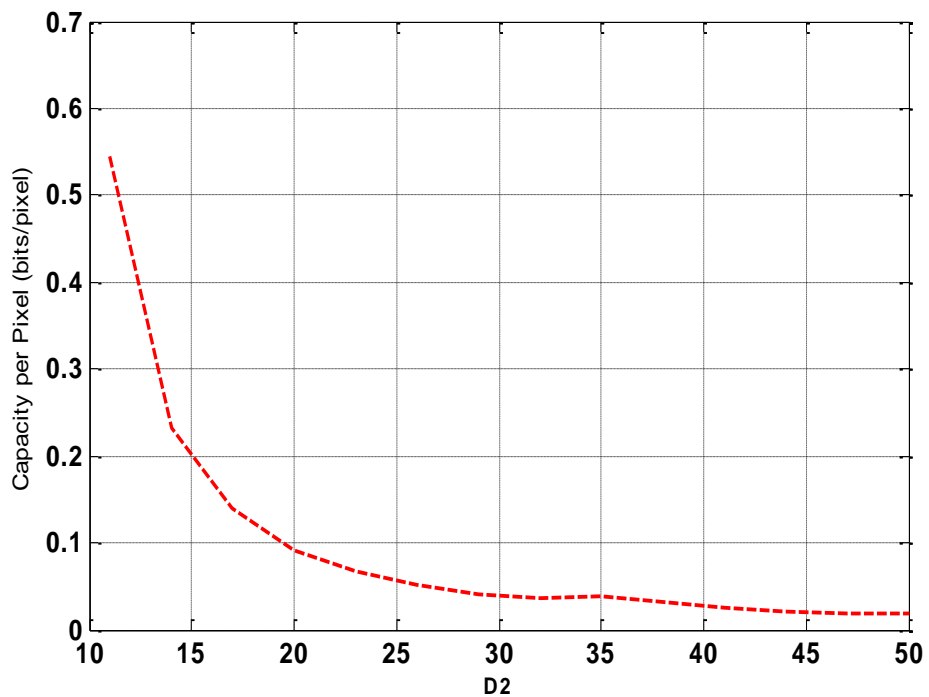
Variance quantization



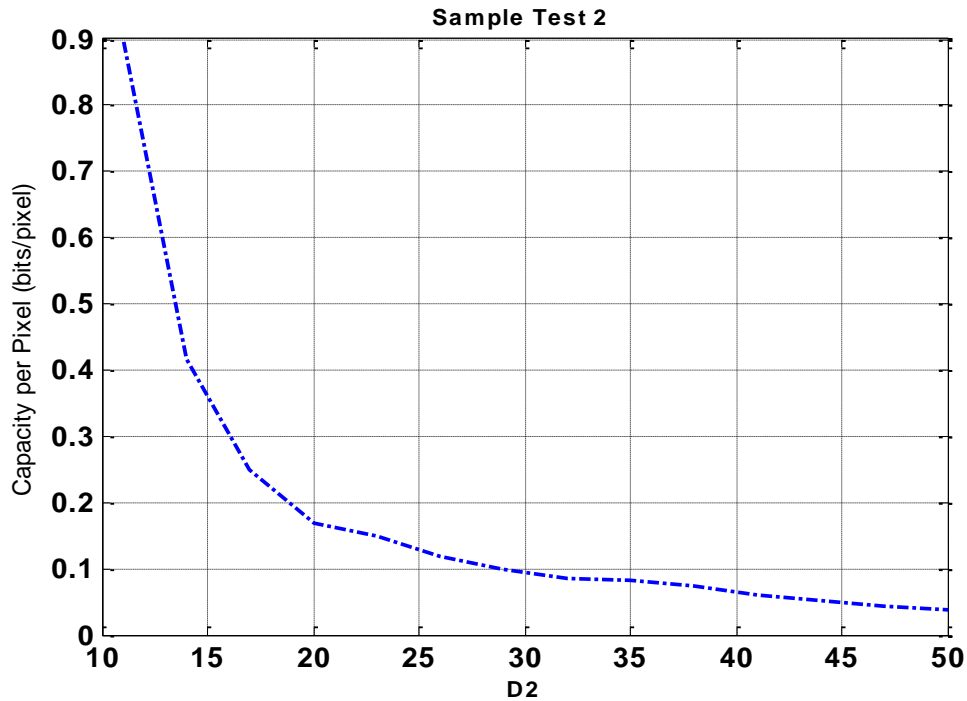
All coefficient within a sub band that have same quantized variance are said to form one channel

Assumption: wavelet Coefficients are Gaussian

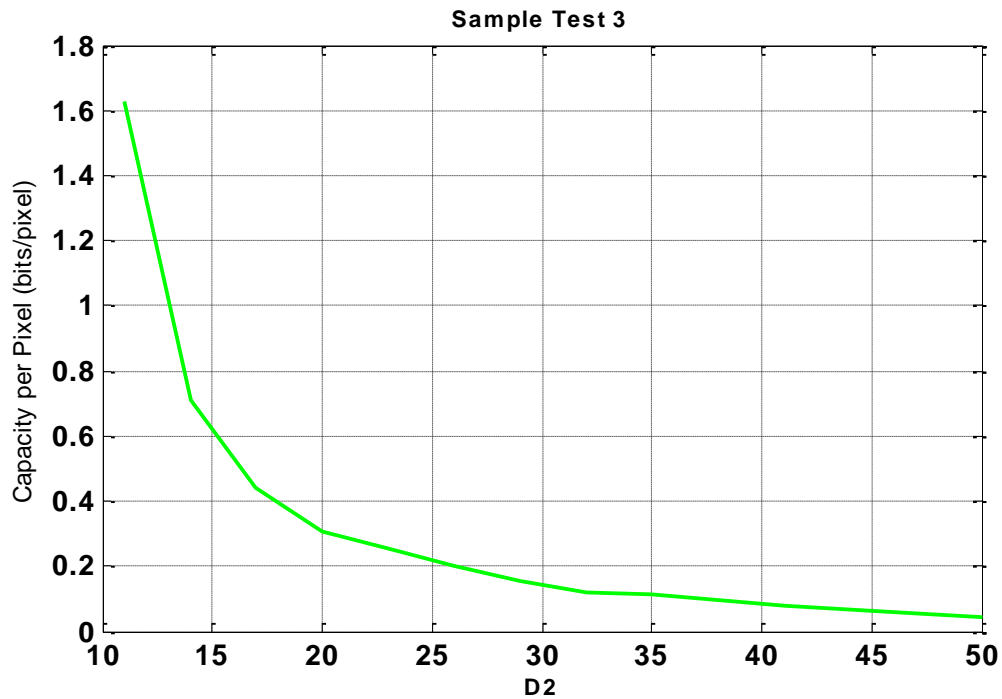
Sample Test 1



Sample Test 2

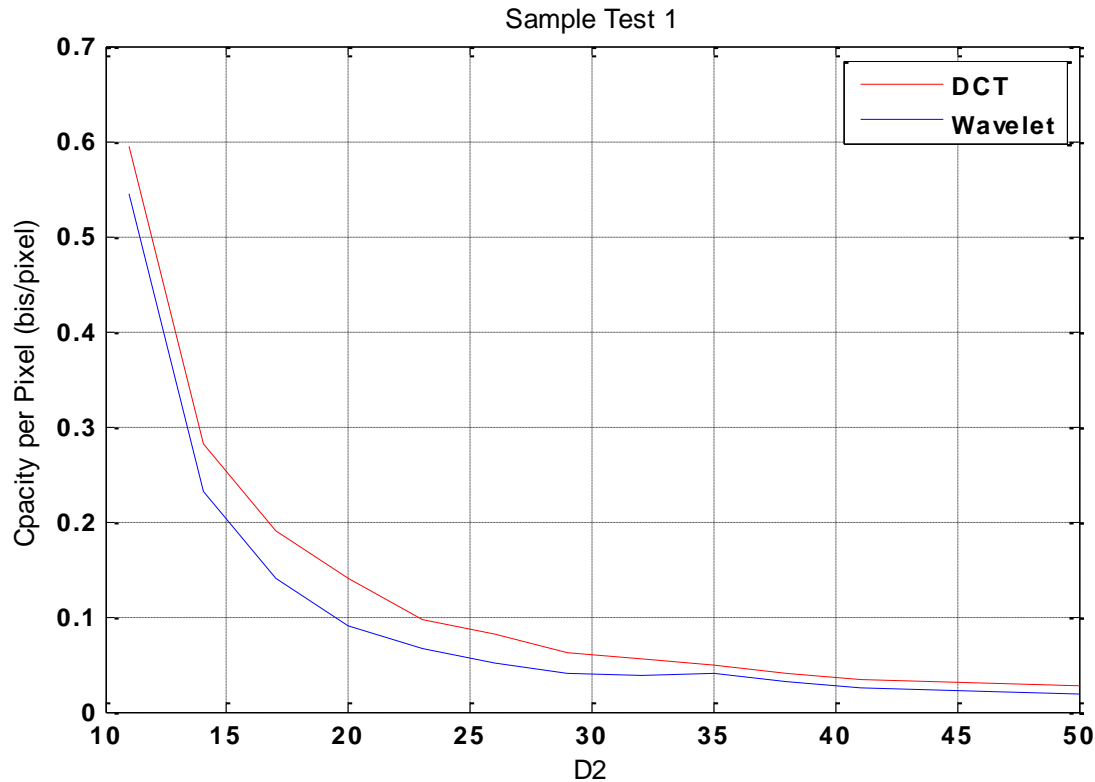


Sample Test 3



Comparison

Wavelet transform are sparser than DCT transform



Conclusion

- Data hiding capacity is associated with the content of the image, more data can be transmitted in a complex image compare with a flat image
- Data hiding capacity can be influenced by the strength of data, but a high strength data not always means a high capacity

Future Work

- Image Modeling :
 - Gaussian Distribution
 - Independent Component
 - Sparseness
- Data Hiding Capacity of Video

References

- [1] Moulin P., O'Sullivan A., "*Information-Theoretic Analysis of Information Hiding*", IEEE Trans on Inform. Theory , vol 49, No. 3, MARCH 2003.
- [2] Moulin P. , Mihcak K., "*A Framework for Evaluating the Data-Hiding Capacity of Image Sources*", IEEE trans on Inform Theory, vol 11, No 9, Sept 2002.
- [3] Moulin P., "*The parallel Gaussian Watermarking Game*" , in Proc 35th conference Information science system, March 2001.
- [4] Gelfand S., Pinsker M., "*Coding for channel with random parameter*", Probl. Contr. Inform Theory, vol 9 , no 1, pp 19-31, 1980.
- [5] Costa M., "*Writing On Dirty Paper*", IEEE Trans Inform theory, vol 29, pp 439-441, May 1983.