

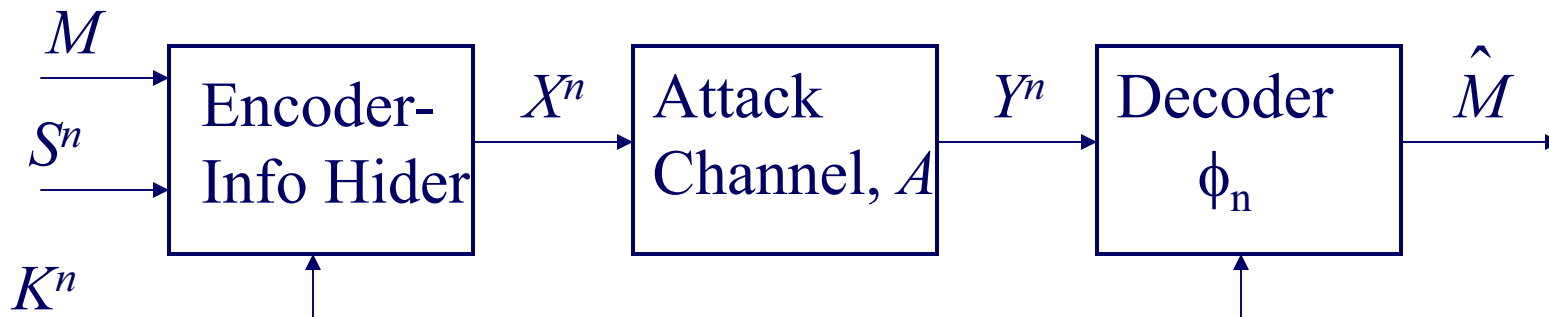
Information Hiding Problems: Hiding Capacity and Key Design

Joseph A. O'Sullivan

Electronic Systems and Signals Research Laboratory
Department of Electrical Engineering
Washington University in St. Louis

- **Information Hiding Problems**
 - **Game-Theory Formulations**
- **Examples → Constraints**
- **Hiding Capacity**
- **Spectrum of problems**
 - **Private → Key → Public**
- **Conclusions**

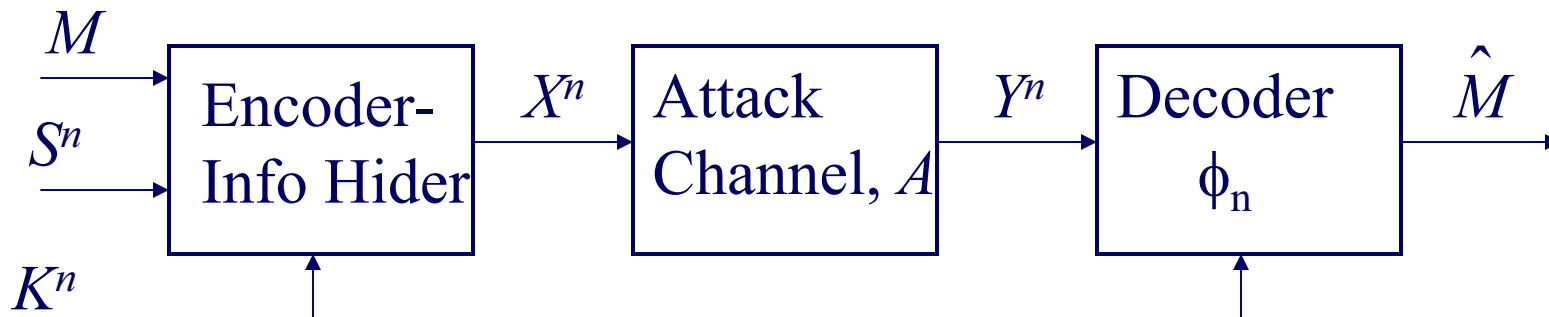
Information Hiding Problems



- Coverttext, Key (S_i, K_i) are pairwise i.i.d.; Source
- Sets of allowable information hiding and attack channels: \mathcal{Q} and \mathcal{A}
- Rate R , Encoder f_n , Decoder ϕ_n
- Probability of Error:

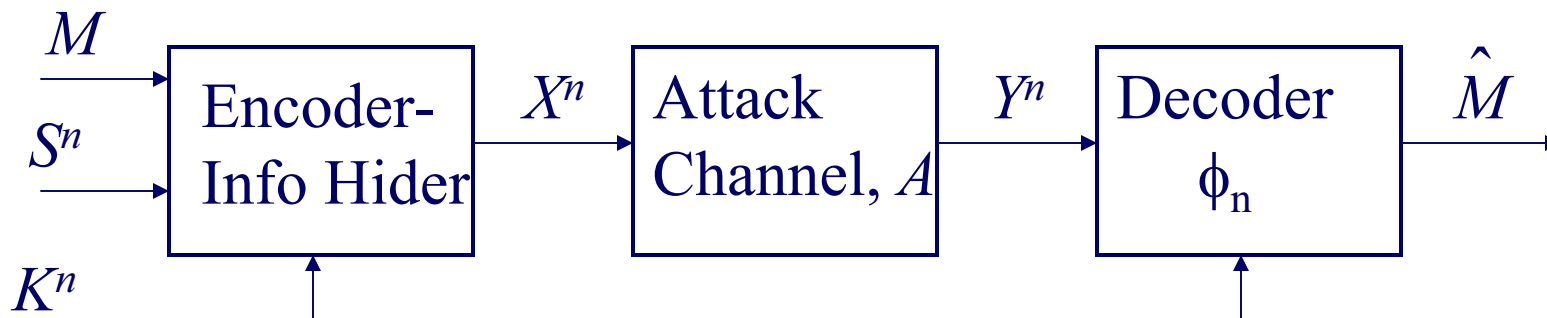
$$P_e = \frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} P(\phi_n(Y^n, K^n) \neq m \mid X^n = f_n(S^n, K^n, m))$$

Information Hiding Problems



- Private Game: $K = S$
- Public Game: K independent of S
- Range in between: $K \rightarrow V \rightarrow S$
- V quantifies information provided about S by K
- Key selection: Fix V , vary K

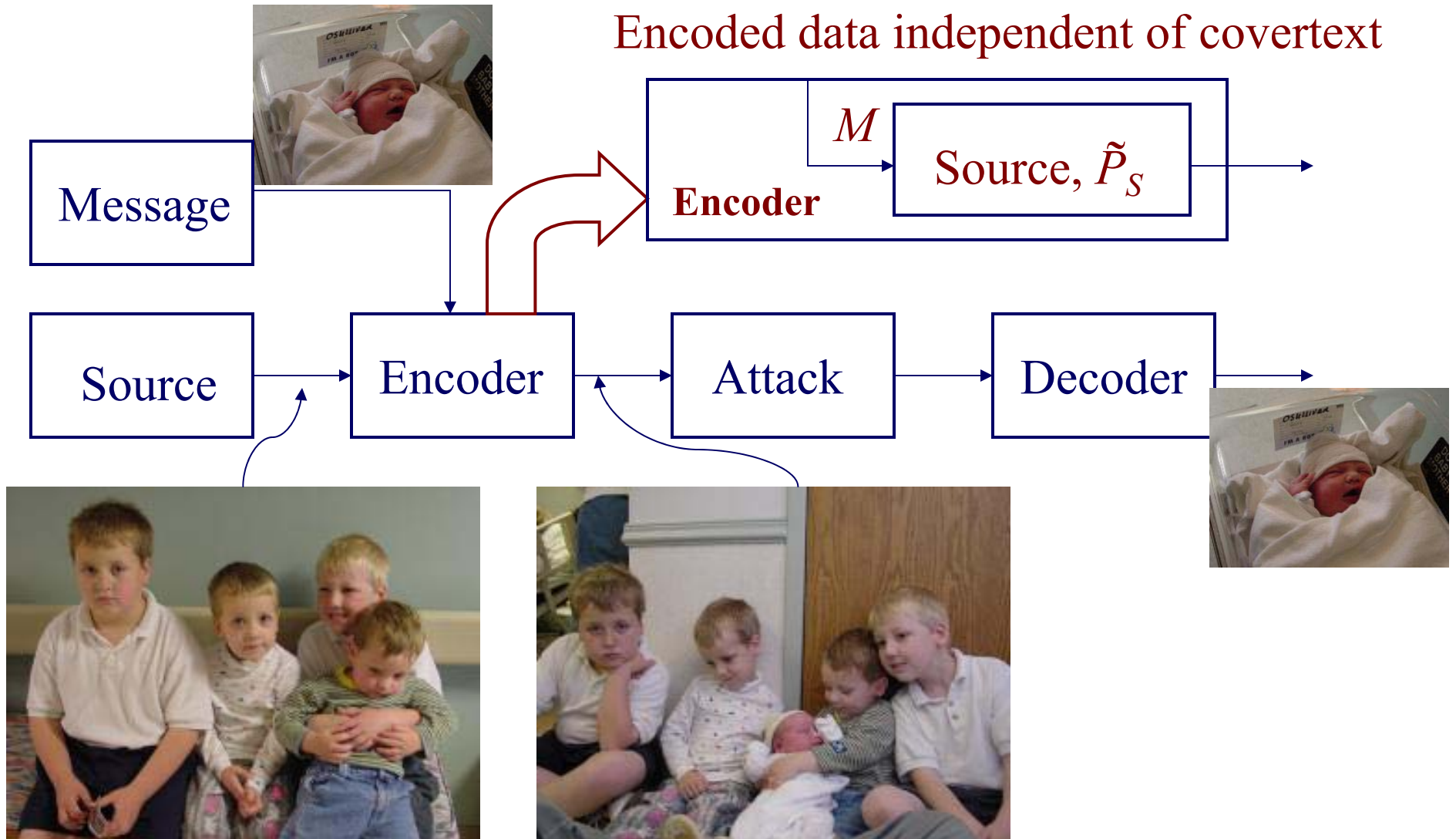
Information Hiding Games



- Fix sets of allowable information hiding and attack channels: Q and A
- **Capacity Game:** Determine maximal achievable rate $R \rightarrow$ hiding capacity C
 - Moulin and O'Sullivan; Cohen and Lapidoth; Merhav and Somekh-Baruch; Chen, Wornell, and Barron
- **Error Exponent Game:** Determine maximum error exponent for each value of rate $R \rightarrow E(R)$
 - Merhav and Somekh-Baruch
- Other Games: identification, detection and estimation, fingerprinting, ... Moulin, et al.; Merhav and Steinberg; etc

Information Hiding Constraints

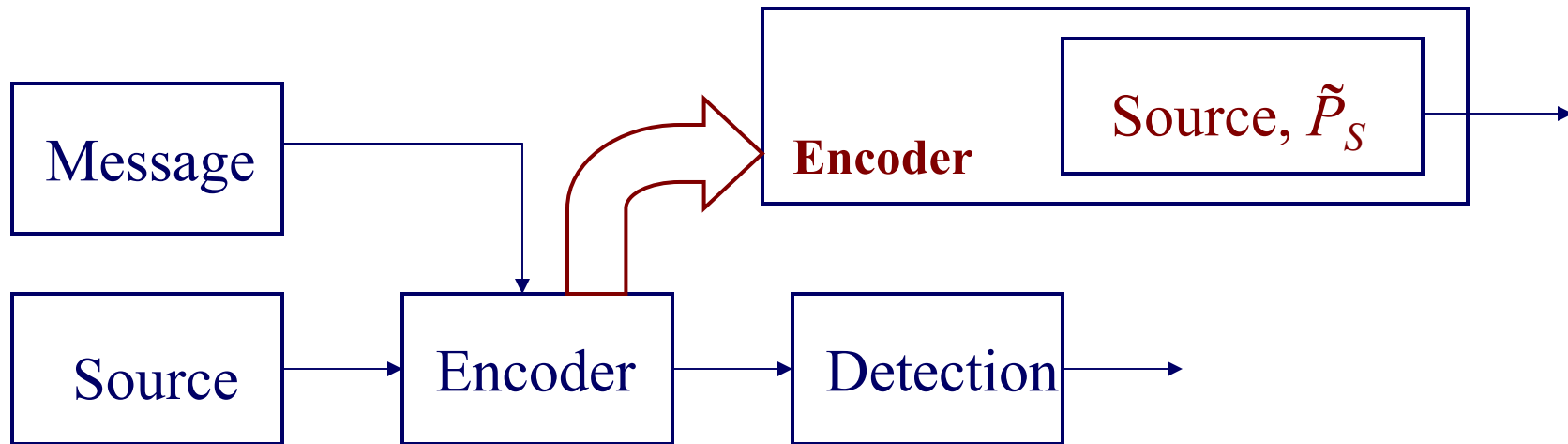
Encoded data independent of covertext



Steganography

- hiding information so that its presence is undetectable

Encoded data need not be independent of covertext.

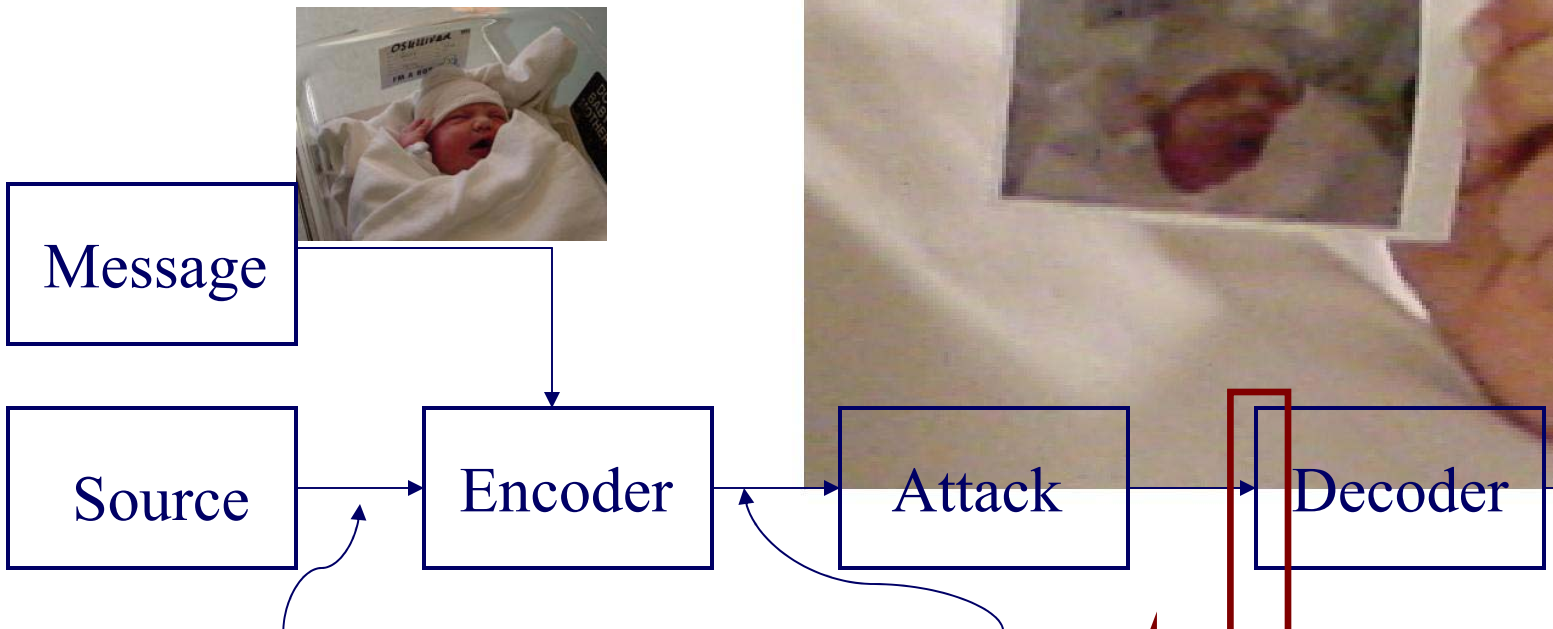
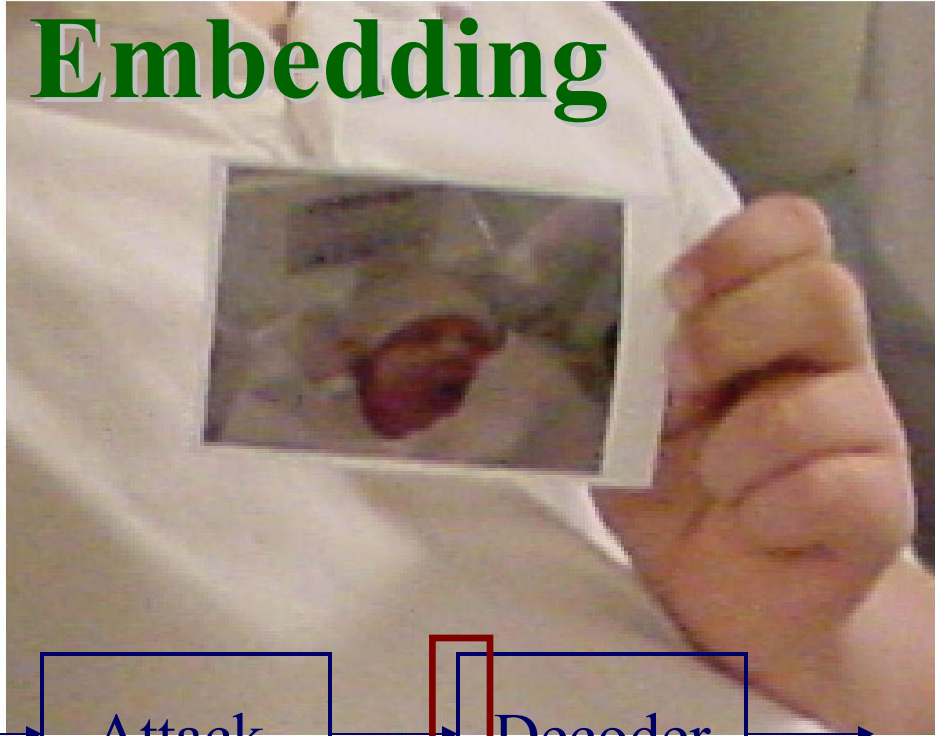


Suppose the attacker simply wants to detect the presence or absence of a hidden message. If

$$D(P_X \| P_S) = 0$$

then perfect hiding is achieved. Otherwise, the error rate is determined by $D(P_X \| P_S)$.

Issues in Embedding



Message

Source

Encoder

Attack

Decoder



Information Hiding Constraints

Transparency or unobtrusiveness:

S^n and X^n similar (mean, w.p.1, exp. bound)

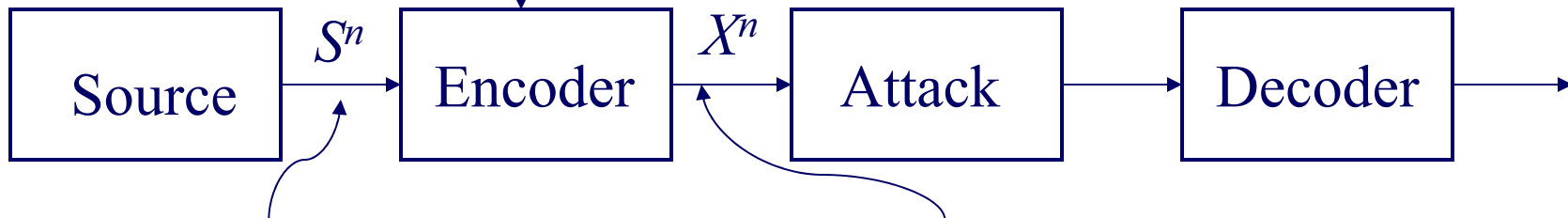
$$E[d_1(S^n, X^n)] \leq D_1$$

$$P[d_1(S^n, X^n) > D_1] = 0, \forall S^n$$

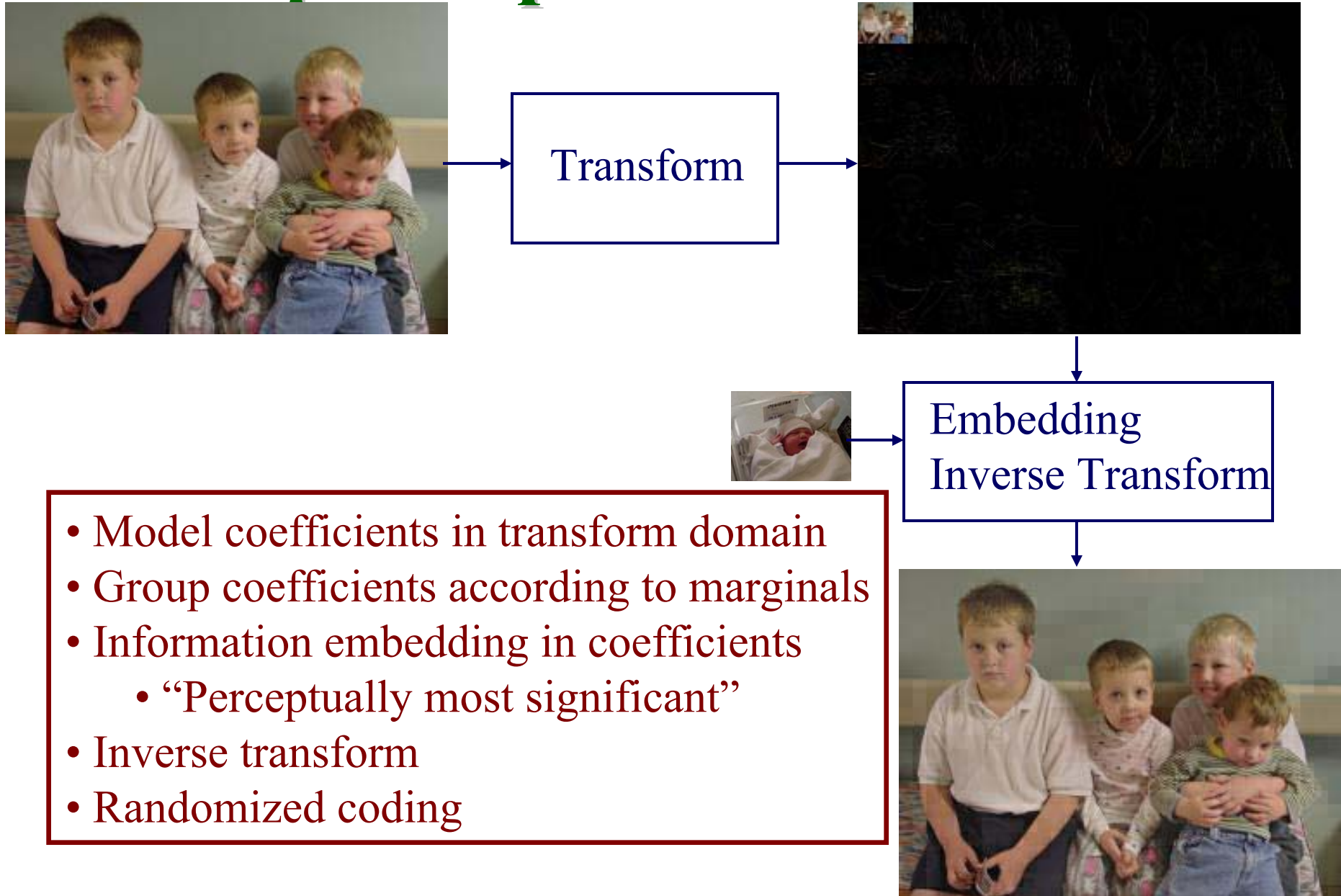
$$P[d_1(S^n, X^n) > D_1 \mid S^n] \leq e^{-vn}, \forall S^n$$



Message



Example Implementation Issues



Attack Channel Constraints

Robustness:

X^n and Y^n similar (mean, w.p.1, exp. bound)

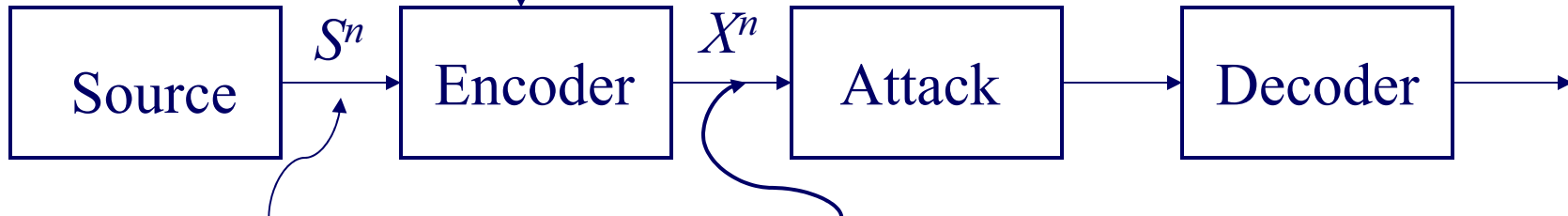
$$E[d_2(X^n, Y^n)] \leq D_2$$

$$P[d_2(X^n, Y^n) > D_2] = 0, \forall X^n$$

$$P[d_2(X^n, Y^n) > D_2 \mid X^n] \leq e^{-\lambda n}, \forall X^n$$



Message



Attack Channel Constraints



Message

Source

Encoder

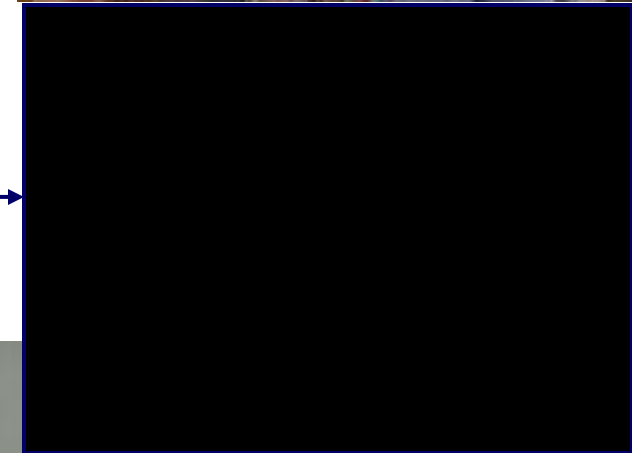
Attack

S^n

X^n

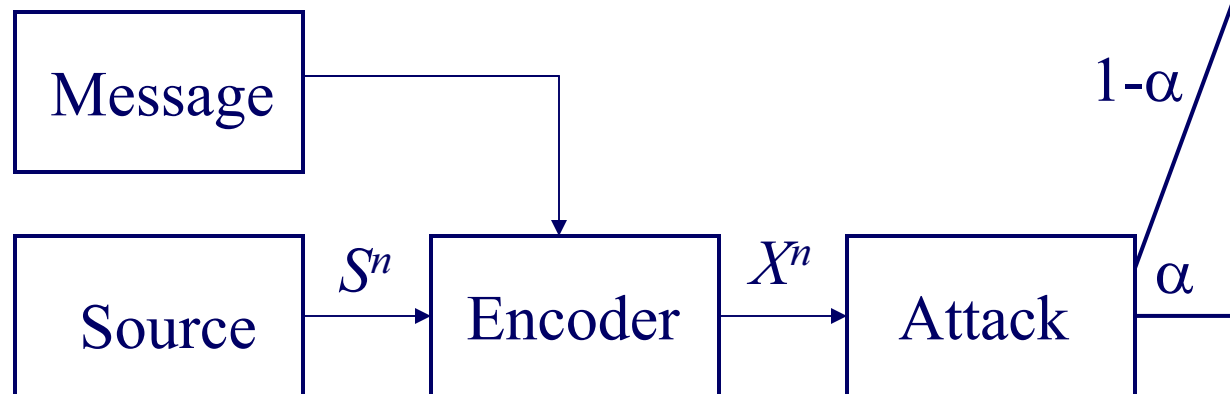
$1-\alpha$

α



Inadequacy of
 $E[d_2(X^n, Y^n)] \leq D_2$

Arbitrary Varying Channel Result



If a deletion attack is allowed with probability bounded away from zero, then the hiding capacity is zero.

Attack Channel Constraints

- Moulin and O'Sullivan: mean $E[d_2(X^n, Y^n)] \leq D_2$

- Memoryless attacks: $A(y^n | x^n) = \prod_{i=1}^n A(y_i | x_i)$

- Block-memoryless: $A(y^{nL} | x^{nL}) = \prod_{i=1}^n A(y_{iL}^{(i+1)L} | x_{iL}^{(i+1)L})$

- Probability one or large deviations bounds

$$P[d_2(X^n, Y^n) > D_2] = 0, \forall X^n$$

$$P[d_2(X^n, Y^n) > D_2 | X^n] \leq e^{-\lambda n}, \forall X^n$$

Attack Channel Constraints

- For many applications, deletion attacks are used
 - Prisoner or subversive communication
 - For other applications, deletion is unacceptable
 - Unauthorized use or acquisition of intellectual property
 - Traitor problems
- Mathematical models may not match reality

Game Theory View

- Acknowledge information will be hidden
- Acknowledge existence of adversary
- Publish hiding strategy
 - *consistent with standard approaches to cryptography*
- Need for secret key for randomized coding
- Need for encoding robustness against broad families of attacks
- Need for decoder to adapt to or be robust with respect to attacks

Information Hiding Coding Theorems

- Public Game:

$$C = \max_{Q \in \mathcal{Q}_1} \min_{A \in \mathcal{A}_1(Q)} I(U; Y) - I(U; S)$$

- Private Game:

$$C = \max_{Q \in \mathcal{Q}_1} \min_{A \in \mathcal{A}_1(Q)} I(X; Y | S)$$

- Other:

$$C = \max_{Q \in \mathcal{Q}_1} \min_{A \in \mathcal{A}_1(Q)} I(U; Y | K) - I(U; S | K)$$

- Gaussian, squared error game:

- Public and private games have equal capacity

- Where ...

Definitions (finite sets)

- U is an auxiliary random variable over a set of known cardinality
- $Q_1 = \{Q(x, u | s, k) : \sum Q(x, u | s, k) p(s, k) d_1(s, x) \leq D_1\}$
 $q(x) = \sum_{u, s, k} Q(x, u | s, k) p(s, k)$
 $A_1(Q) = \{A(y | x) : \sum A(y | x) q(x) d_2(x, y) \leq D_2\}$

Payoff Function

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

Properties

$$Q(x, u | s, k) = p(x | u, s, k) p(u | s, k)$$
$$A(y | x)$$

- Set $A_1(Q)$ is convex for every Q
- Set Q is convex
- Convex in A
- Concave in $p(u|s, k)$
- Convex in $p(x|u, s, k)$
- **Key Design:** Convex in $p(s, k)$

Payoff Function

- Relationship to Chiang and Cover, ISIT 2001
 - Unified view of channel coding with state information and source coding with side information at the decoder
 - Information available at decoder, information available at encoder

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

Equal Capacity in Public and Private Games

- Barron, Chen, and Wornell, 2001.
- If the (Q^*, A^*) that achieve capacity are such that $U \rightarrow Y \rightarrow S$ is a Markov chain, and the resulting joint distribution on (S, X, Y) is the same as in the public game, then the values of the public and private games are equal.

$$C = \max_{Q \in \mathcal{Q}_1} \min_{A \in \mathcal{A}_1(Q)} I(U; Y) - I(U; S)$$

Key Design Issues

- Primary roles of key:
 - Provide randomization of encoding strategy (encoder-decoder common randomness)
 - Inform decoder about covertext
- Information: $K \rightarrow V \rightarrow S$ Markov Chain

$$Q(x, u | s, k) = Q_k(x, u | s, v)$$

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

$$\sum_{k, v} p(v) p(k | v) [I_{Q_k}(U; Y | V = v) - I_{Q_k}(U; S | V = v)]$$

Comments on Keys

- Arbitrary key K implies select $V=f(K)$.
- Last expansion emphasizes $I(U;Y|V)-I(U;S|V)$
- Suppose $V_1 \rightarrow V_2 \rightarrow S$. Let $V_1 = f_1(K_1)$ and $V_2 = f_2(K_2)$ and assume the marginals on K_1 and K_2 are identical. Then the capacity of the game with K_2 is at least the capacity of the game with K_1 .

Further Implementation Issues

- Distributions on sources
 - Images, video, voice, music
 - Option: base models on successful compression algorithms
- Model real attacks
 - Malicious, benign, unanticipated
 - “Cut-out” of intellectual property; edited photos
- Fingerprinting for traitor problems
 - Collusion attacks (k out of m)



Related Emerging Applications

- Upgrades of legacy communication systems
 - Wornell, Ramchandran, Pradhan, et al.
 - Legacy system defines covertext
 - Digital upgrade is encoded data
 - Importance of Gaussian view, DC-QIM, etc.

Conclusions

- Reviewed capacity results in information hiding games
- Reviewed some roles of keys
- For more information on
 - Our results, see Moulin and O'Sullivan
www.ifp.uiuc.edu/~moulin
 - Error exponent games, see Merhav and Somekh-Baruch
 - Gaussian games, see Cohen and Lapidot
 - Also: Wornell, Ramchandran, Steinberg, several special issues, conferences, etc.