

Modern Steganography

Hiding Information in Plain Sight

Professor Joseph A. O'Sullivan
Department of Electrical and
Systems Engineering

 Washington University in St. Louis


Center for Security
Technologies

Center for Security
Technologies

Securing our World through Technology

Modern Steganography

- Applications
 - National Security Applications
 - More than security: \$
 - Multimedia and Consumer Applications
- Baby Example
- Fundamental Performance Bounds → Practical Implementations



National Security Applications

- Document authentication
 - International communications
- Digital fingerprinting
 - Traitor tracing
- Covert communications
 - February 2001: USA Today reported that Osama Bin Laden used steganography to communicate with operative

Multimedia and Consumer Applications

- Audio
 - Rampant music sharing, violation of copyright laws
- Images
 - Photographers: authenticity and/or copyright
 - 2001: Disney announced plans to digitally watermark every frame of every movie for copyright protection
- Video-on-demand
 - Video sharing
- Broadcast video (*VEIL Interactive*)
 - Broadcast verification
 - Broadcast quality (cropping, time-warping, etc.)
 - Copyright and authentication issues
- Legal, ethical issues
 - Digital Millennium Copyright Act (DMCA)
 - Political power of movie, music industries

“Bootleg copies of Oscar-nominated movies showing up on Internet”

AP Jan. 14, 2004

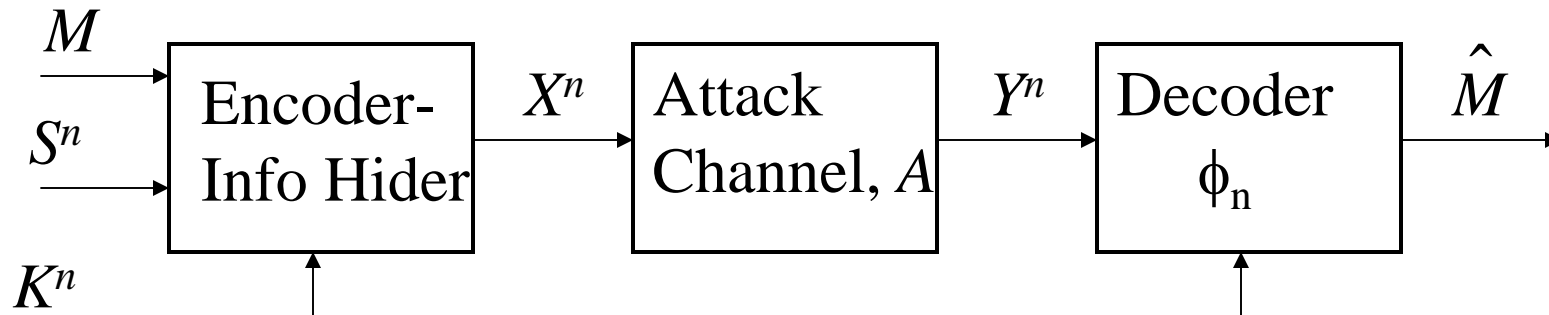
- “The Last Samurai,” “Something's Gotta Give,” “Cold Mountain,” “House of Sand and Fog”
 - “The Los Angeles Times reported that security features on the tape [Cold Mountain] indicated that it belonged to Ivan Kruglak, an academy member and president of a wireless data communications company.” AP Jan. 15, 2004
 - Fingerprinting based on Philips Research Lab Technology



Oscar Bootlegs 2004

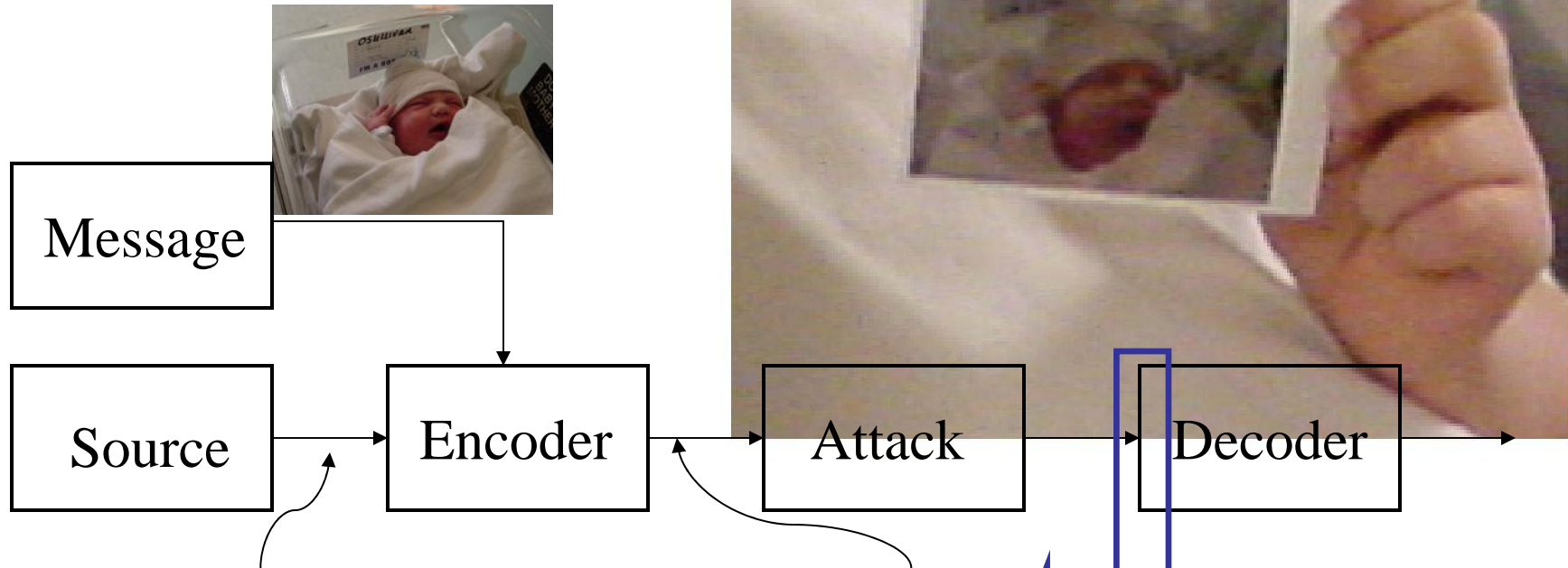
- Fri Jan 16, 2:12 AM ET *By Gregg Kilday and Paul Bond* (Hollywood Reporter)
- FBI confirmed involvement
- "Something's Gotta Give," "The Last Samurai," "Master and Commander: The Far Side of the World" and "thirteen."
- "Illegal copies ... have been traced ... to character actor Carmine Caridi, a member of the Academy of Motion Picture Arts and Sciences"
- "It was a pretty professional job... all visible markings were removed."
- "This year the screeners carried invisible markings for the first time; the studios were able to identify the Academy member for whom they had been intended."

Information Hiding Problems

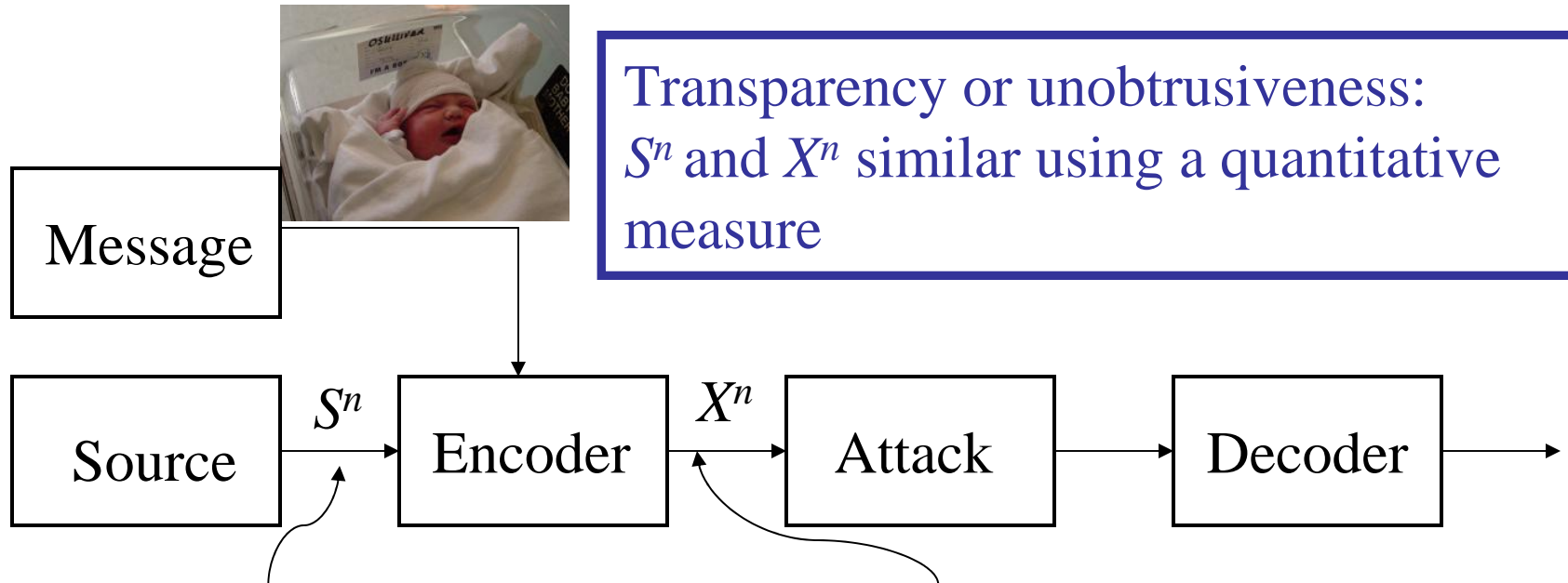


- Coartext S_i : image, video, data
- Key K_i : shared information (image, features, where is information hidden)
- Sets of allowable information hiding and attack channels
- Rate R : how much information is hidden?
- Probability of Error
- Moulin and O'Sullivan 1997-2003

Baby Version of Problem



Information Hiding Constraints



Game Theory View:

Information Hider Viewpoint

- 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

Game Theory View:

Information Attacker Viewpoint

- Acknowledge that an attack will occur
- Acknowledge intelligent information hiding
- Design attack as if it would be published
- Define goal of attack
- Need for randomized attack, families of attack strategies
- Need to tune attack strategy to different information hiding strategies
(robustness of optimal attack)

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

Practical Implementation

- 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



Modern Steganography:

Hiding Information in Plain Sight

- National Security Applications
 - Document authentication, fingerprinting, covert communications
- Multimedia and Consumer Applications
 - Audio, images, video, broadcast video
 - Copyright issues, broadcast verification
- Fundamental Performance Bounds
 - Practical Implementations