# *An Empirical Study of Secure MPEG Transmissions*

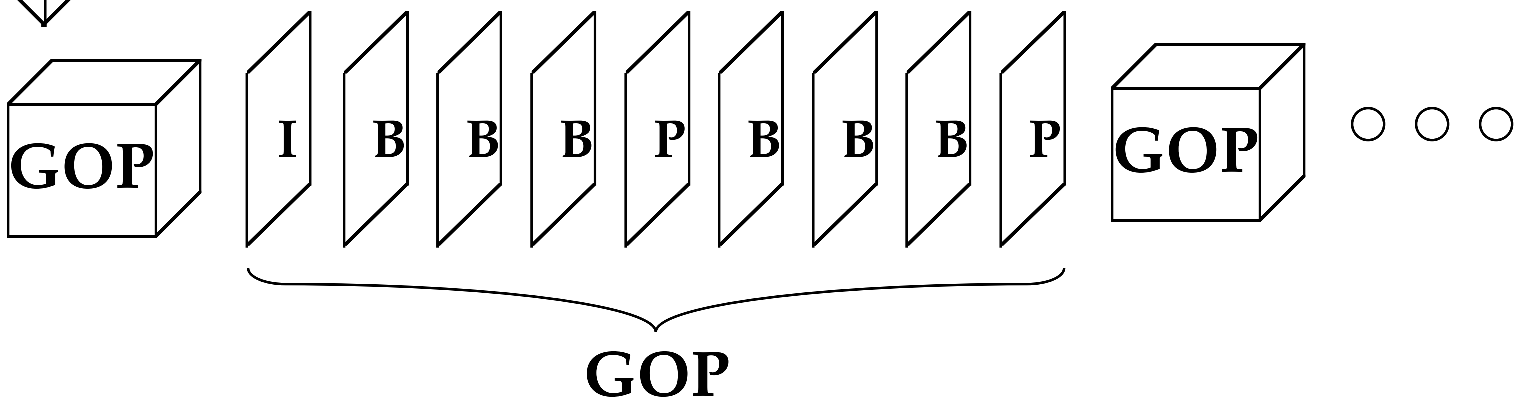
Iskender Agi and Li Gong

*Computer Science Laboratory*
*SRI International*
*Menlo Park, CA 94025*
*{iskender,gong}@csl.sri.com*

# *MPEG Encoding*

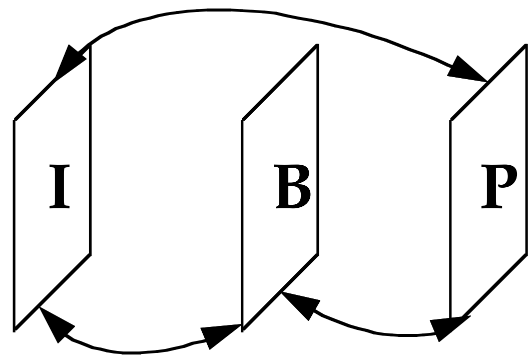
- Compresses video by reducing spatial and temporal correlation
- Further increases compression by using quantization and Huffman encoding
- Asymmetric encoding
  - Encoding requires larger computation
- Resynchronization signals and fault-tolerance

# *MPEG Frame Pattern*




- Group of Pictures (GOP) is a random-access unit in MPEG bit-stream
  - The integrity of the GOP depends on initial I-frame
  - A series of GOPs make up the MPEG bit-stream

# *MPEG Frame Dependency*




- P- and B-frames increase compression by reducing temporal correlation
- Motion-estimated (predicted) P- and (bilinearly predicted) B-frames depend on *correctness* of I-frames

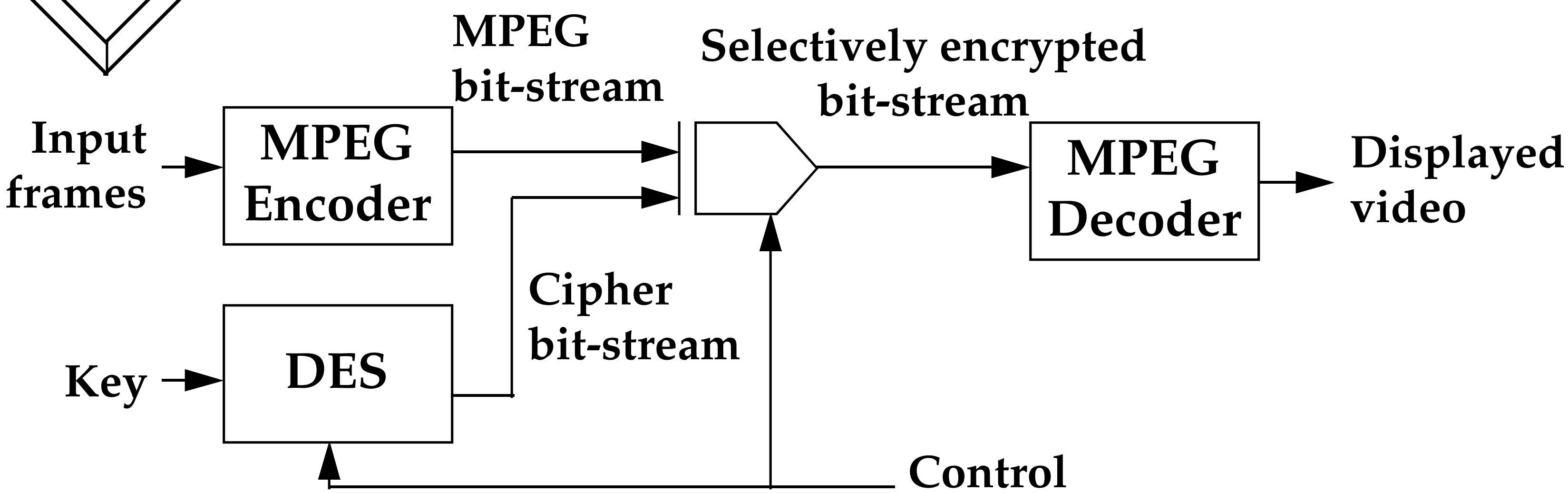
# *Selective Encryption*

- Takes advantage of the MPEG structure
  – Encrypts only the reference data
  – Dependent data will be *corrupted*
- Reduces encryption/decryption computation by 40-60%
- Proposed as a *low-cost* alternative to wholesale encryption

# *Objective*

- Evaluate selective MPEG encryption, especially for sensitive applications
- Analyze trade-off between
  - Encryption complexity
  - Computational load at encoder/decoder
  - Compression
- When is selective encryption useful?

# Description of Experiment




- Encode video using MPEG-1 and -2
- Encrypt encoded intracoded (I) video
- Eavesdrop on encrypted video using a *fault-tolerant* decoder

# *Things We Don't Consider*

- Header information
  - Not MPEG-specific and guessable
- Resynchronization signals
  - MPEG was designed to survive bit-errors
- Altering MPEG bit-stream format
- Encryption algorithm
  - Our results are not DES-specific

# *Input Data Statistics: Bits per Frame Type*

| Frame Type | *Miss America* | *Flowers* |
|---|---|---|
| I | 58% | 37% |
| P | 20% | 55% |
| B | 22% | 8% |

- Teleconferencing (*Miss America*)
- Action video (*Flowers*)

# *Miss America Sequence*

- Low levels of motion
- Similar to teleconference
- Extensive use of motion compensation

# Miss America Sequence I-Frame Encryption

- Quality severely degraded
- Observer can still detect motion and recognize human features

# *Flowers Sequence*

- Action video
- Large areas of movement
- Little use of motion compensation

**Direction of pan**

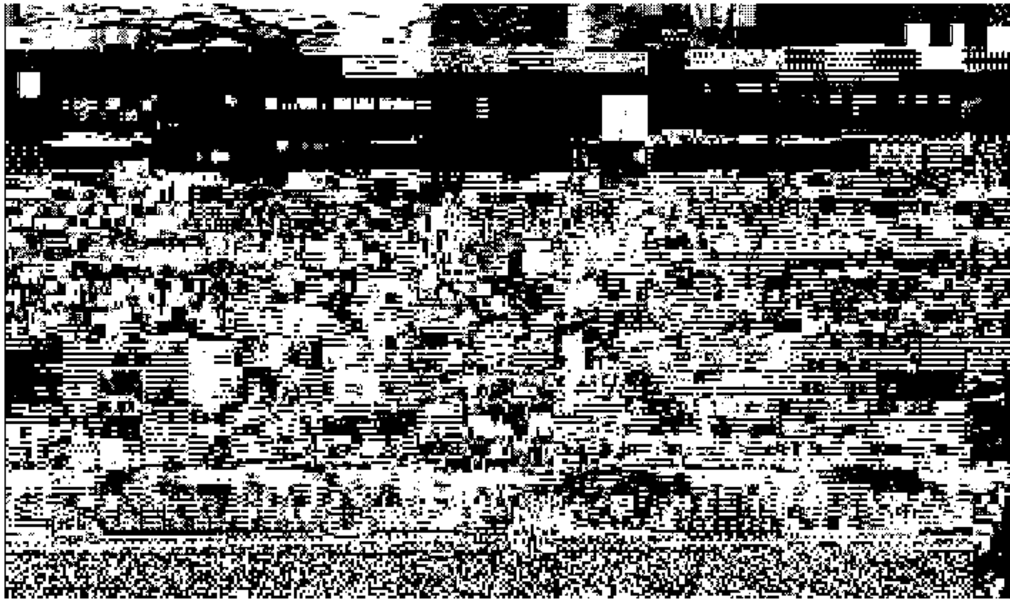
# *Flowers Sequence Encrypting I-Frames Only*

- Many I-blocks in P- and B-Frames
- Motion-compensation is not used
- Inadequate security for sensitive applications

# Increase I-Frame Frequency

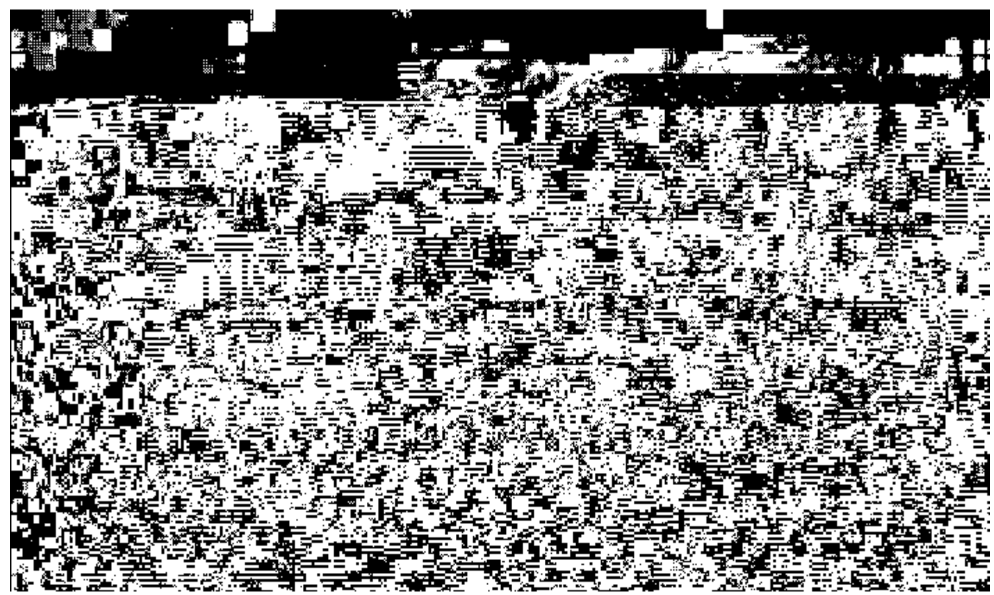
- Improves security
- Decreases compression
- Increases computational load
- Leaves traces of recognizable video

Unencrypted

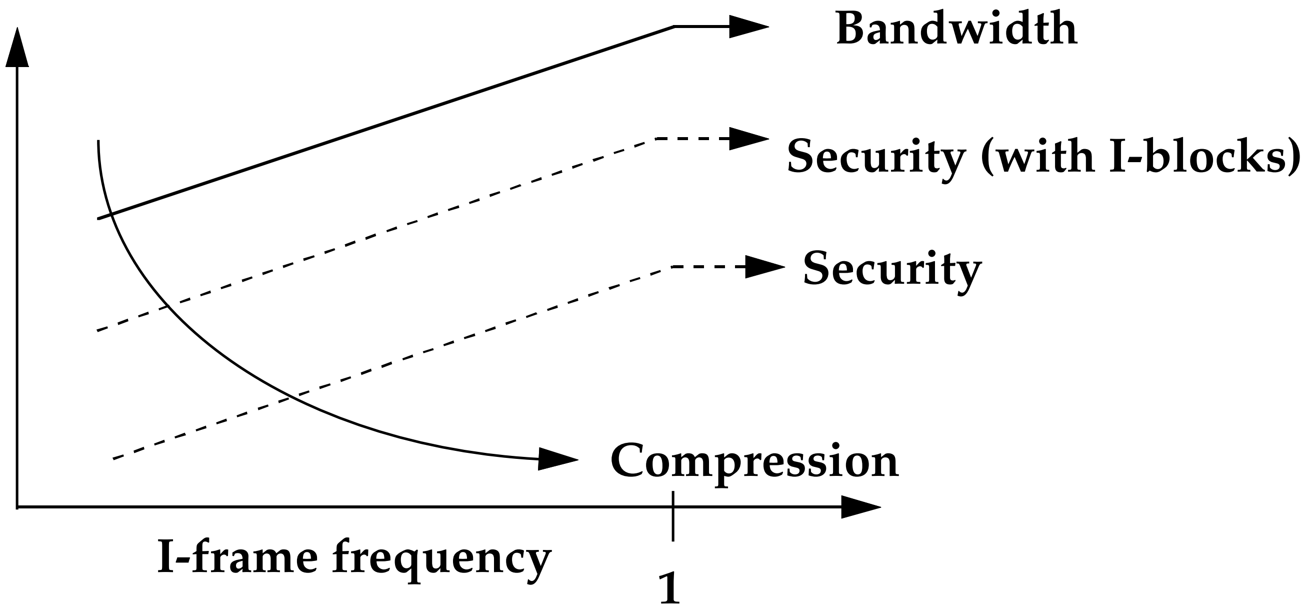


# *Flowers Sequence Encrypt All I-Blocks*

- Improves security over increased I-frame frequency
- Increases bookkeeping
- Good compression



# General Tradeoffs




- No free lunch: Increased security costs in compression, complexity, and time.

# *Analysis of Selective Encryption of MPEG-Encoded Video*

- Encrypting I-frames alone
  - Not the answer for sensitive applications
  - Maybe good enough to degrade quality of service (QOS), e.g., for video distribution
- Encrypting I-blocks helps increase security, but may be cumbersome
- Encrypting P-frames, may help -- inconclusive results

# *Future Research*

- Quantitative measure of information in encrypted video
- Content-based, adaptive encryption
- A *security wrapper* for MPEG video must have
  - Small computational cost relative to decoding (currently 30-50%)
  - Synchronization with other media