Adaptability in Multimedia Data Security

Bharat Bhargava, Changgui Shi and Sheng-Yih Wang
Department of Computer Science
Purdue University

Adaptability in Multimedia Data Security

- Different levels of security on Video Encryption
  - Maximum Security: Heavy-Weight Cryptography
    - Apply DES, IDEA, RSA, etc to the whole data
  - Medium Security: Light-Weight Cryptography
    - Selective Encryption using DES/IDEA, etc.
  - Minimum Security: Light-Weight Encryption
    - XOR, encoding table permutation, etc.

Adaptability in Multimedia Data Security

- Challenges on Video Security
  - Large Data Size
    - Two-Hour MPEG-I Video: 1GB
  - Real-Time Requirement
    - MPEG-II Video: 4MB/sec to 10MB/sec
    - 30 frames/sec

Adaptability in Multimedia Data Security

- Four Light-Weight Video Encryption Algorithms
  - CPA, VEA, MVEA and RVEA
  - Incorporate encryption and MPEG compression in one step
  - Add little overheads
    - software implementation is fast enough

Adaptability in Multimedia Data Security

- CPA (Codeword Permutation Algorithm)
  - Use a permutation of the Huffman codeword as the secret key
  - No overhead in MPEG Codec
  - Dose not decrease compression rate
  - Limited key spaces

Adaptability in Multimedia Data Security

- VEA (Video Encoding Algorithm)
  - Secret key XORed on sign bits of DCT coefficients in I frames
  - No limit on secret key length
  - Weak for plaintext attack

Adaptability in Multimedia Data Security

- MVEA (Modified VEA)
  - Secret key XORed on sign bits of DCT coefficients in I frames
  - Secret key XORed on sign motion vectors on P/B frames
  - More secure than VEA because all frames are changed

Adaptability in Multimedia Data Security

- RVEA (Real-Time VEA)
  - Secret key cryptography applied on sign bits of DCT coefficients in I frames and motion vectors on P/B frames
  - Bounded encryption time
    - Encrypt at most 64 bits for each macroblock
  - Most secure in all four algorithms

Adaptability in Multimedia Data Security

- Adaptability Features
  - Data Selection
    - Base: Sign bits of DCT coefficients in I frames
    - Additional: Sign bits of motion vectors on P/B frames
  - Encryption Algorithms (in increasing strength)
    - XOR
    - DES/IDEA
    - RSA

Adaptability in Multimedia Data Security

- Experiments
  - Currently we have four separate implementations for the four algorithms
  - A generic implementation which encompass all four algorithms with adaptable features is our next step
  - We will experiment on the dynamic adaptation of adaptable security features based on the resource constraint such as CPU utilization, Value of the video, etc.

MPEG encryption algorithms

Algorithm	Security Ideas	Overhead	Security Level
VEA	Encryption on sign bits of DCT coefficients of I frame using XOR operation	Low	Low
MVEA	VEA + encryption on sign bits of motion vectors of P and B frame	Medium	Medium
MVEA	MVEA with XOR replaced by secret key cryptography. Encrypt only up to 64 bits per macroblock.	High	High