Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments

Martina Podesser, Hans-Peter Schmidt, and Andreas Uhl
uhl@cosy.sbg.ac.at

Outline

- Introduction
- Selective or Partial Encryption
- Selective Bitplane Encryption
- Evaluation of Selective Bitplane Encryption: Ciphertext-only Attacks
  - Attack 1: Replacement Attack
  - Attack 2: Reconstruction Attack
- Conclusions

Introduction

- Application area: secure transmission of visual data
  (video server $\longrightarrow$ clients, videoconferencing including mobile devices,. . .)
- Problem: many clients, or low-power devices at the sending or receiving end
- Possible solution: Selective Encryption: encrypt the data, but just some parts while maintaining security
- But: which parts?

Multimedia Security: Providing Confidentiality

- Multimedia security often trades off security for computational complexity: "soft encryption"
- E.g., real-time encryption for an entire video stream using classical ciphers (like AES) requires much computation time
- Many multimedia applications require security on a lower level (e.g. TV broadcasting)
- This results in a search for fast encryption procedures specifically tailored to the target environment

Selective/Partial Encryption

- Application specific data structures are exploited to create more efficient encryption systems (e.g. encrypting I-coded macroblocks in MPEG streams only)
- Visually most "important" parts are protected by secure but slow "classical" ciphers
- Available for DCT, Wavelet, and Quadtree based multimedia representations
- Wireless Environments: selective encryption resistant to bit errors and compliant to video formats recently proposed

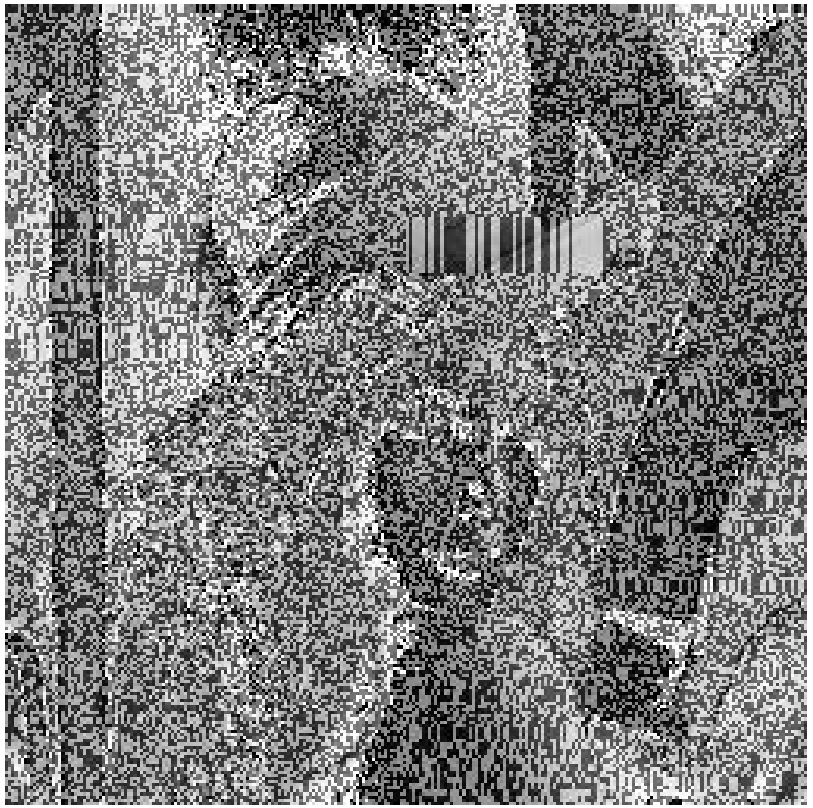
Environment and Interplay with Compression

- Target environment: Lossless (e.g. medical imaging) and no compression scheme should be applied due to the low processing power of the involved hardware (e.g. mobile clients)
- Idea: to reduce computational cost of encryption, apply compression FIRST, in order to reduce amount of data to be encrypted (up to a factor of 5 in the lossless case).
- Not a good idea: time demand for compression is significantly higher as the time demand for encryption (e.g. lossless compression with JPEG2000 takes a factor 100 (!) longer as compared to AES encryption)
- After image aquisition, plain image data may be accessed directly without being compressed
- Sample application: teleradiology with mobile image capturing clients to enable fast and exact on-site diagnosis after an accident

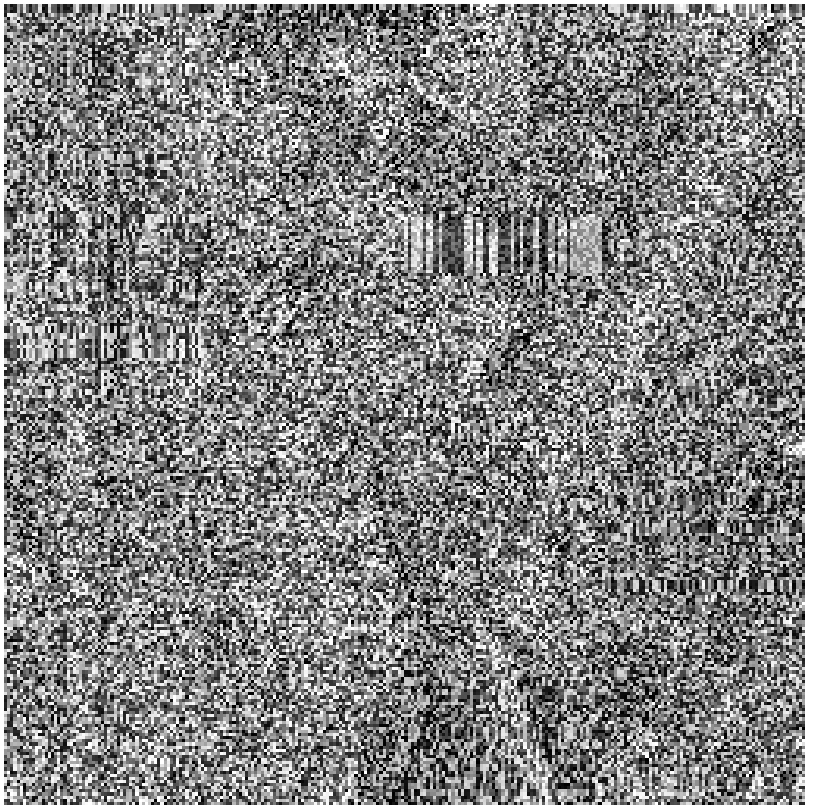
Selective Bitplane Encryption I

- Assume an 512×512 pixels image to be given in 8bit/pixel (bpp) precision
- We consider the 8bpp data in the form of 8 bitplanes, each bitplane associated with a position in the binary representation of the pixels
- AES encrypt a subset of the bitplanes (starting with the MSB)
- AES implementation with blocksize 128 bit and a 128 bit key. The 128 bit block is filled with a quater of a bitplane line ($512/4 = 128$ bits)
- The encrypted bitplanes are transmitted together with the remaining bitplanes in plain text

Selective Bitplane Encryption: Visualization



(a) 12.5% encrypted



(b) 25% encrypted, 9.0dB

Selective Bitplane Encryption II

How to eventually increase security:

- Start from LSB and continue with increasing bit-significance

# Bitplanes	1	2	3	4	5	6	7	8
First: LSB	51	44	38	32	26	20	14	9
First: MSB	9	9	9	9	9	9	9	9

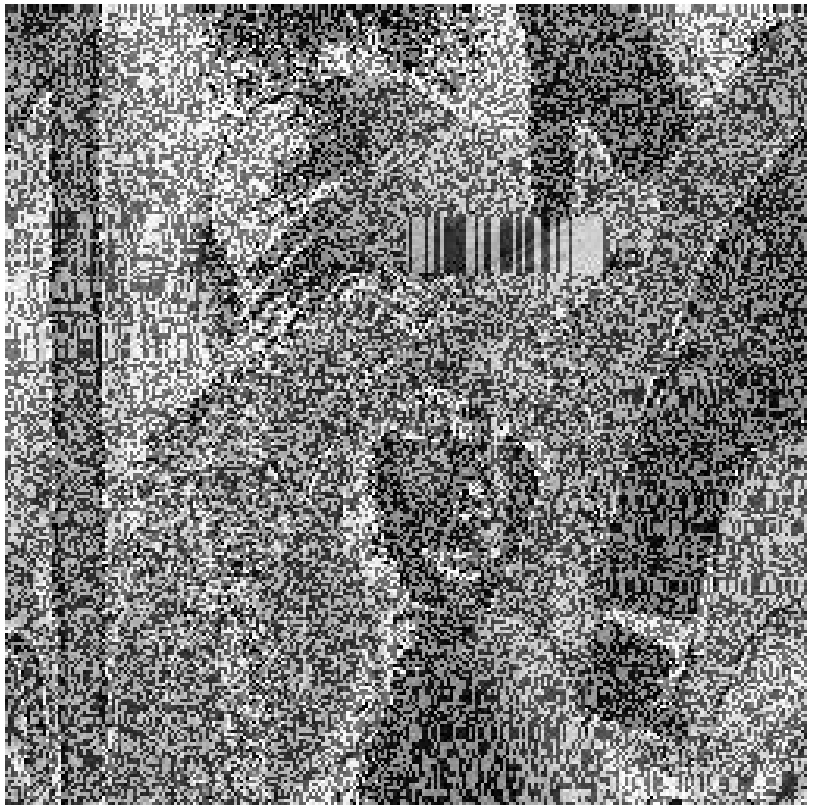
Selective Bitplane Encryption III

How to eventually increase security:

- Encrypt MSB and additional bitplanes, do not disclose which have been encrypted

Bitplane	MSB	2	3	4	5	6	7	LSB
Plain	45	39	32	20	11	5	4	4
Encrypted	4	4	4	4	4	4	4	4

Selective Bitplane Encryption: More Visual Examples



(c) MSB + 4th

(d) 4 bitplanes starting from LSB, 31.8dB

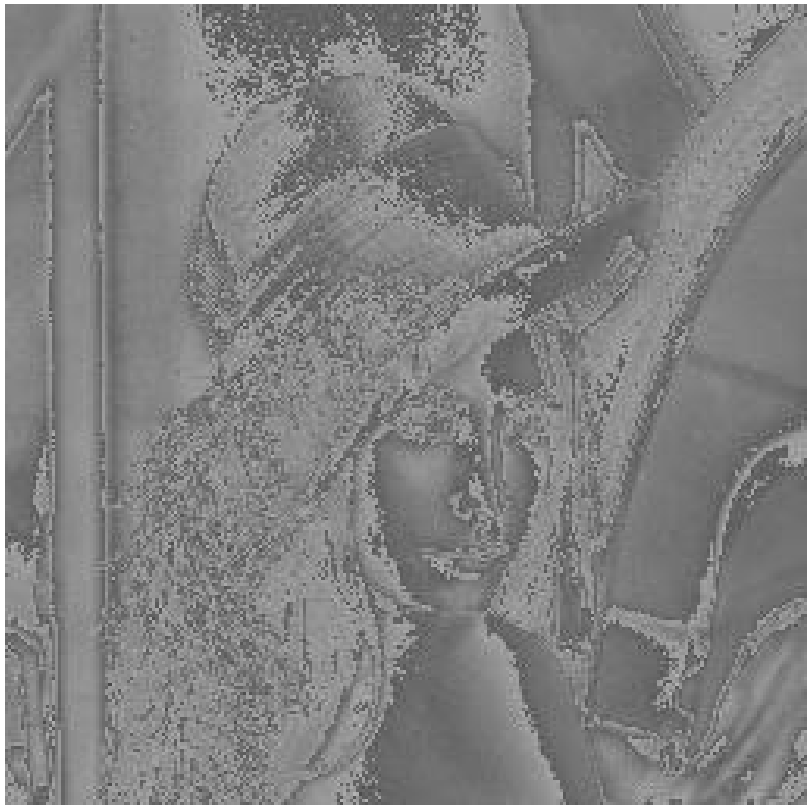
Evaluation of Selective Bitplane Encryption

- In most evaluations of selective encryption schemes, mostly visual examples are provided only
- Reason: poor correlation of PSNR and other simple quality measures and perceived quality especially for low-quality images
- Example: PSNR computed between the image Lena and its entirely AES encrypted version is 9.2 dB whereas PSNR between Lena and an image with constant grayvalue 128 is 14.5 dB !
- 2 ciphertext only attacks:
  - Replacement Attack
  - Reconstruction Attack

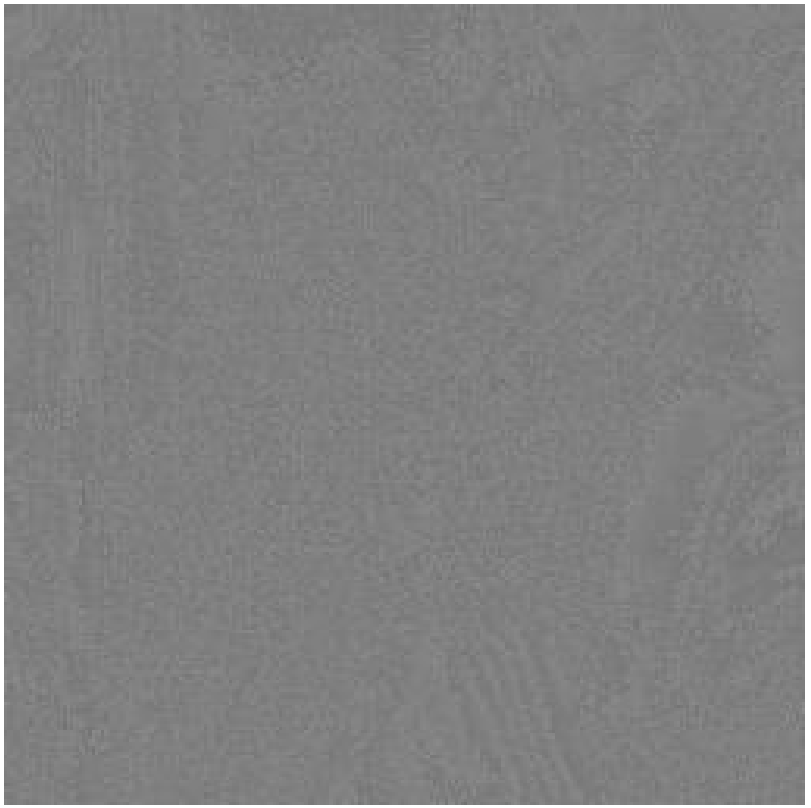
Replacement Attack

- When using direct reconstruction, the encrypted parts introduce noise-type distortions
- We replace the encrypted bitplanes by a constant 0 bitplane
- The resulting decrease in average luminance is compensated by adding 64 to each pixel if only the MSB bitplane was encrypted
- Reconstruction is performed as usual

Replacement Attack: Visual Examples



(e) 25% encrypted, 13.2dB



(f) 50% encrypted

Reconstruction Attack

- Assume the MSB bitplane to be encrypted only
- Aim: reconstruct the MSB data with the aid of the unencrypted remaining data
- We exploit the fact that most regions of natural images are covered by areas with smoothly changing gray values
- In these areas, the MSBs of all pixels tend to be identical (except for the case of medium luminance)
- Automatic detection procedure for such regions

Reconstruction Attack: Detection Procedure

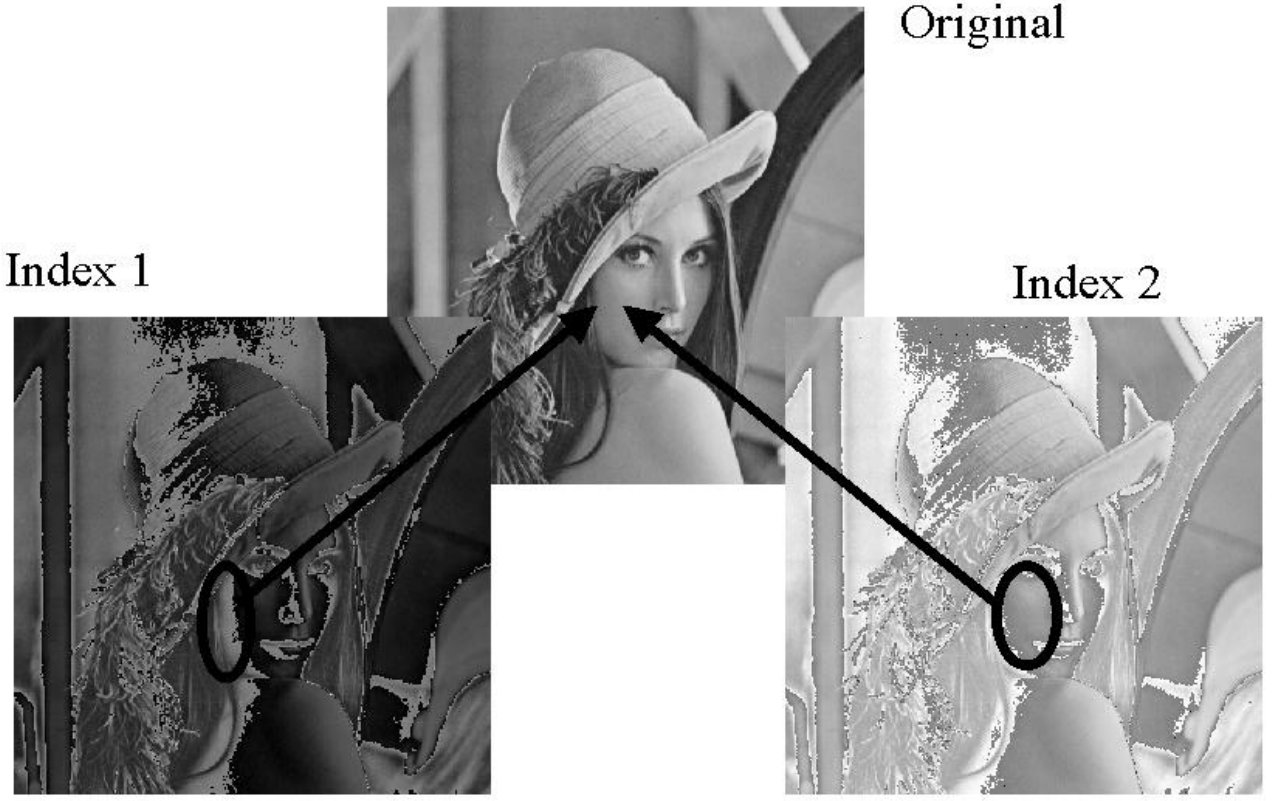
- 2×2 pixels search window in which all 16 possible combinations of MSB configurations are tested
- A certain set of differences among the 4 pixel values is computed for each of the 16 MSB configurations
- The smallest difference is selected and the corresponding configuration of the MSB bits in the search window is defined to be the reconstruction
- "Edge-detection capability": when the search window hits an edge, the difference operation leads to an attempt to compensate (setting the MSB to different values at both sides of the edge)

Reconstruction Attack: Visual Examples I

(g) original MSB

(h) reconstructed bitplane

Reconstruction Attack: Visual Examples II



Combination of two half-images after Reconstruction Attack.

Reconstruction Attack: Limitations

- Complexity increases significantly if more bitplanes are encrypted
- Also, the reliability is drastically reduced
- "Separable" application possible to save computational complexity, but quality suffers severely
- No threat in cases where encryption resists reconstruction attack !

Conclusions & Future Work

- Conclusions
  - Encryption of the MSB bitplane only is not secure enough (Attacks !)
  - Securing two bitplanes severly alienates the image content, encryption of four bitplanes (50 % of data) provides high confidentiality
- Future Work - Employing Selective Compression
  - Bitplanes subject to encryption are selectively compressed first
  - High speed bitplane compression necessary to be profitable