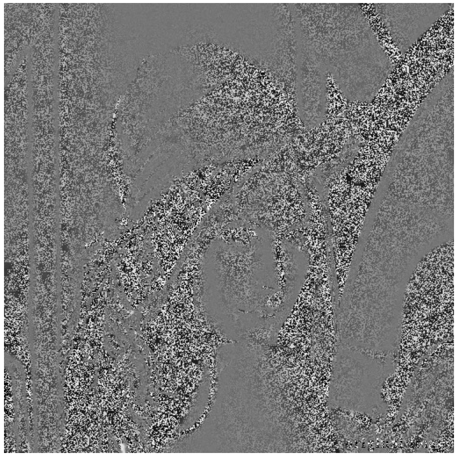
IFIP CMS 2005

Selective Image Encryption Using JBIG

Roman Pfarrhofer and Andreas Uhl
roman@pfarrhofer.at, uhl@cosy.sbg.ac.at



Outline

- Motivation for Selective Encryption
- Basics of the JBIG format
  - Planes
  - Resolution layers
    - Deterministic prediction (DP)
    - Typical prediction (TP)
  - Stripes
  - Bit stream
- Selective Encryption using JBIG

Outline

- Implementation
- Experiments
- Attack resistance
  - Median filtering
  - Edge detection
  - Replacement attack
- Conclusion

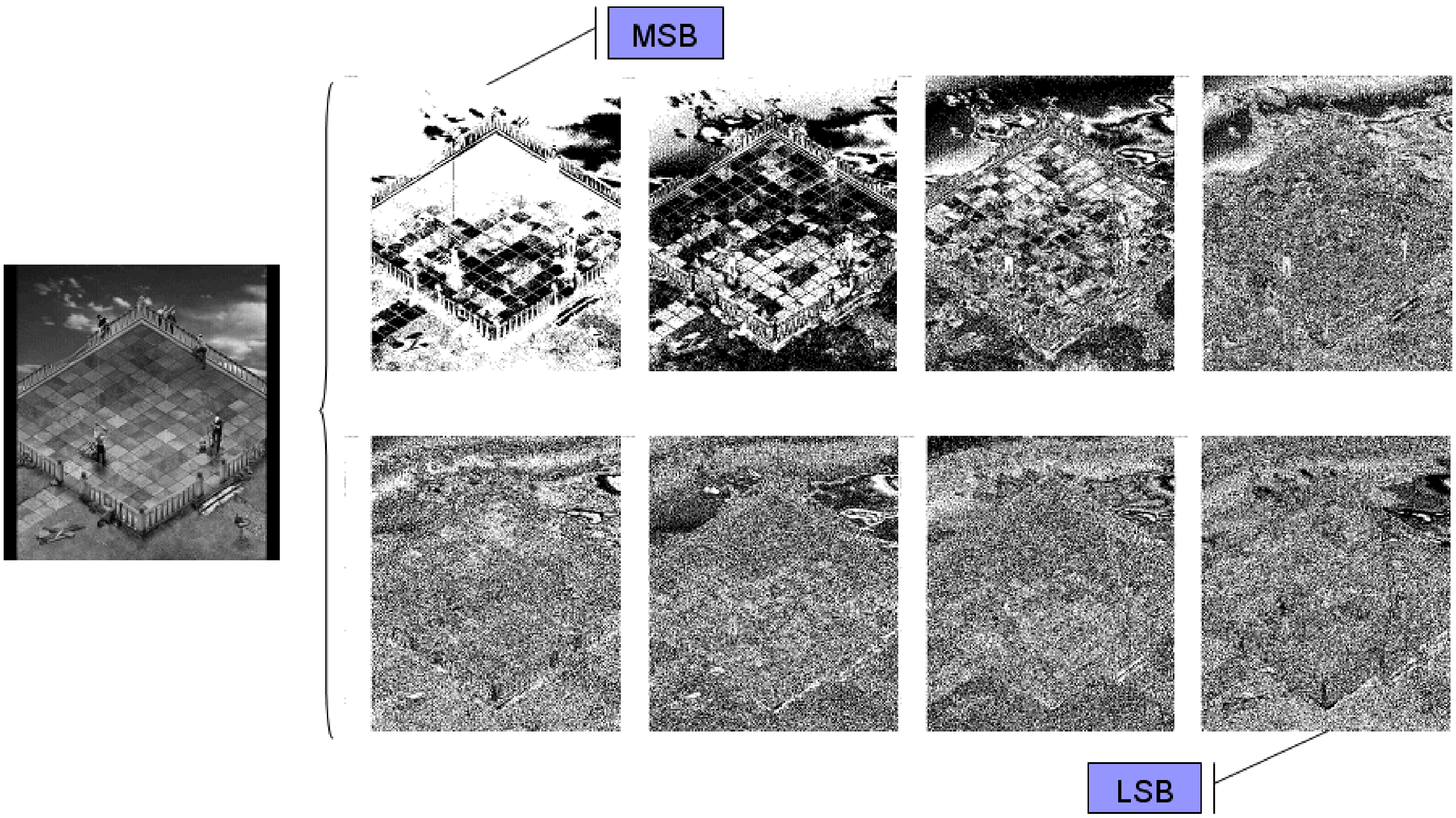
Motivation for Selective Encryption

- Security requirements for multimedia content
  - trade off between security and complexity
- Especially for real-time video encryption it's important to reduce encryption effort
- Selective encryption schemas are targeting to only encrypt relevant parts of multimedia data

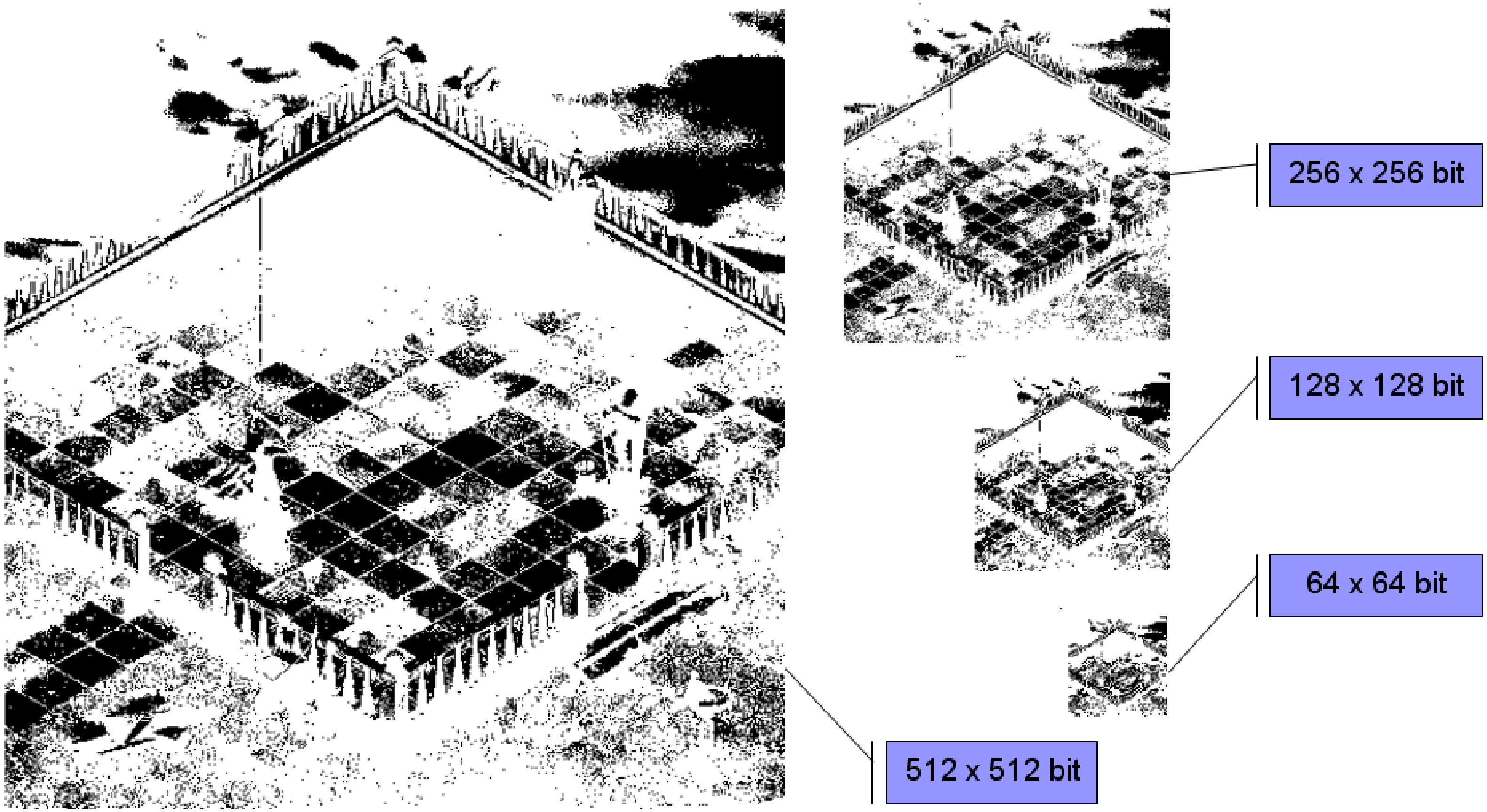
Basics of the JBIG format

- **J**oint **B**i-Level **I**mage Experts **G**roup was standardized 1993 (ITU-T T.82)
- JBIG was meant to improve fax compression standards
- Binary context-based adaptive arithmetic coder
- Supports hierarchical progressive mode
- JBIG differs between
  - Planes
  - Resolution layers
  - Stripes

Planes



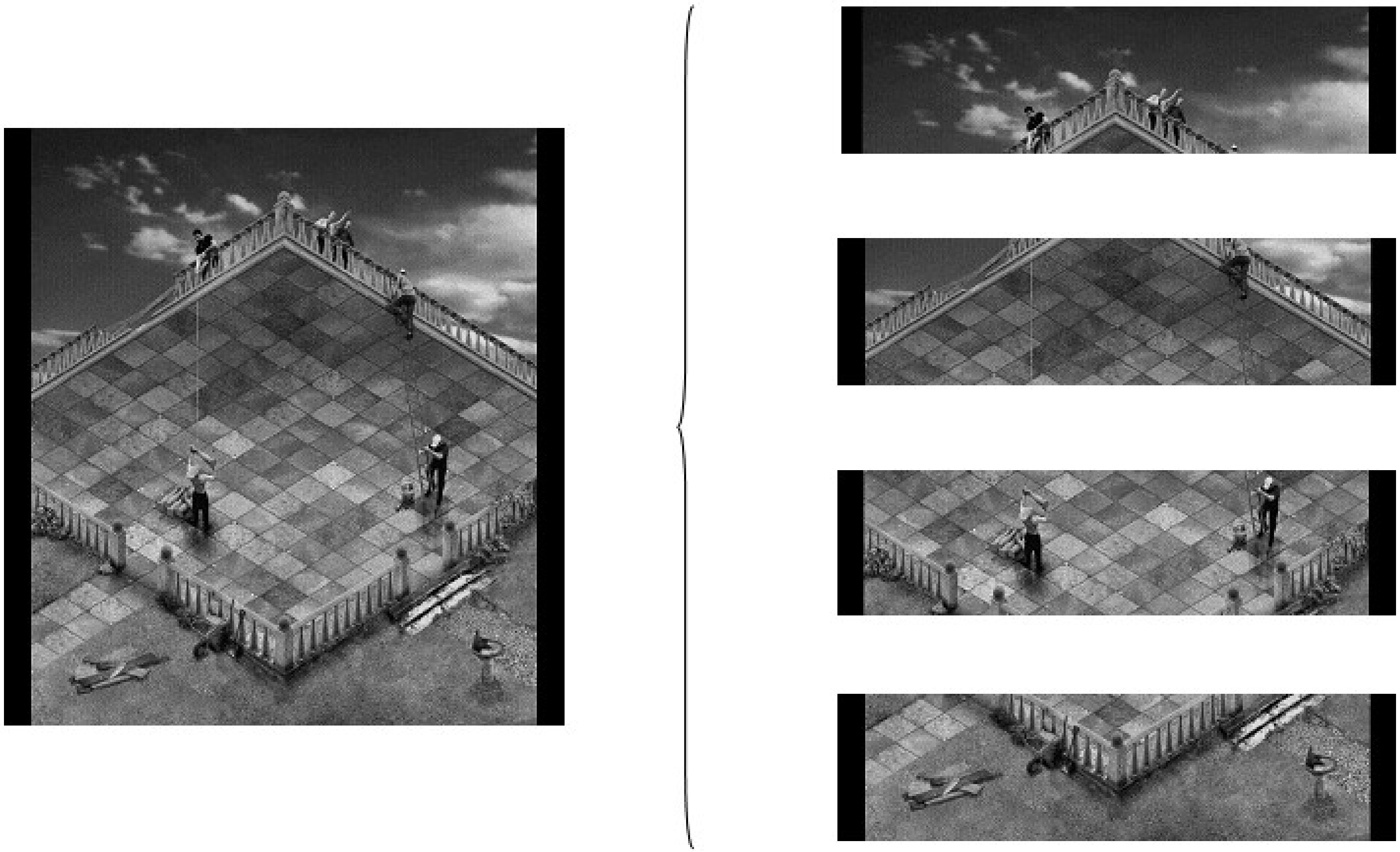
Resolution layers



Resolution layers

- Cross-layer contexts
  - "*typical prediction*": Identical lines in the lowest resolution layer are only coded once and labelled as typical for higher layers
  - "*deterministic prediction*": Pixel values which can be predicted due to neighbouring pixels of the current and – in particular – the lower resolution layer are not encoded

Stripes



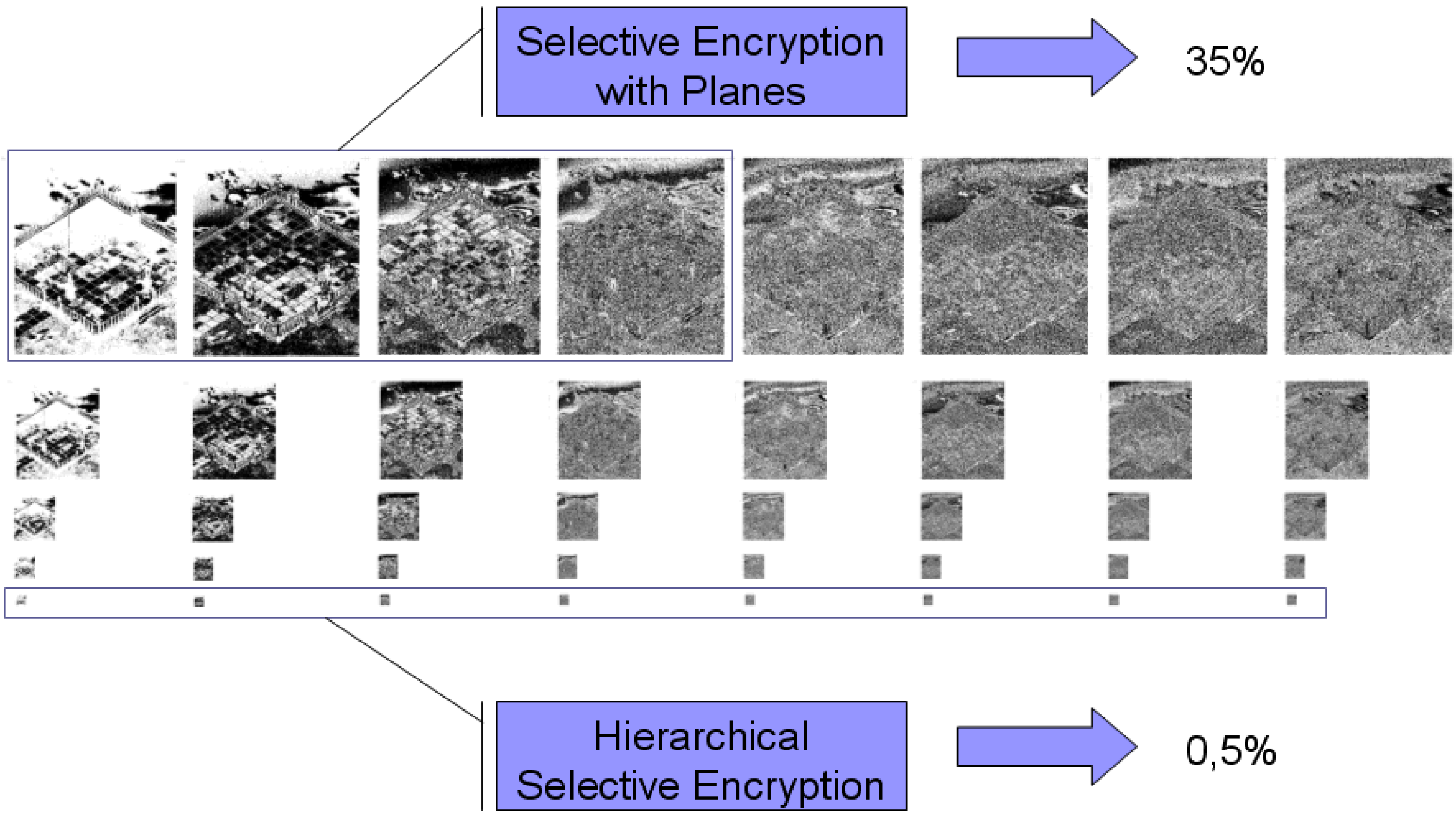
Bit stream

20-byte header (with image size, #planes, #layers, stripe size, first layer, options, SDE ordering, ...)
[optional 1728-byte table]
stripe data entity
[optional floating marker segments]
stripe data entity
. . .
stripe data entity

Selective Encryption using JBIG

- Our approach is mainly based on the high amount of dependencies between resolution layers in progressive mode
- Only encrypting the lower resolution layers (most relevant) is reducing the amount of data to compute

Selective Encryption using JBIG



Implementation

- Implementation is based on the C JBIG-Library from M. Kuhn
- This library was extended to encrypt single stripes with
- C++ AES-Implementation from B. Gladman

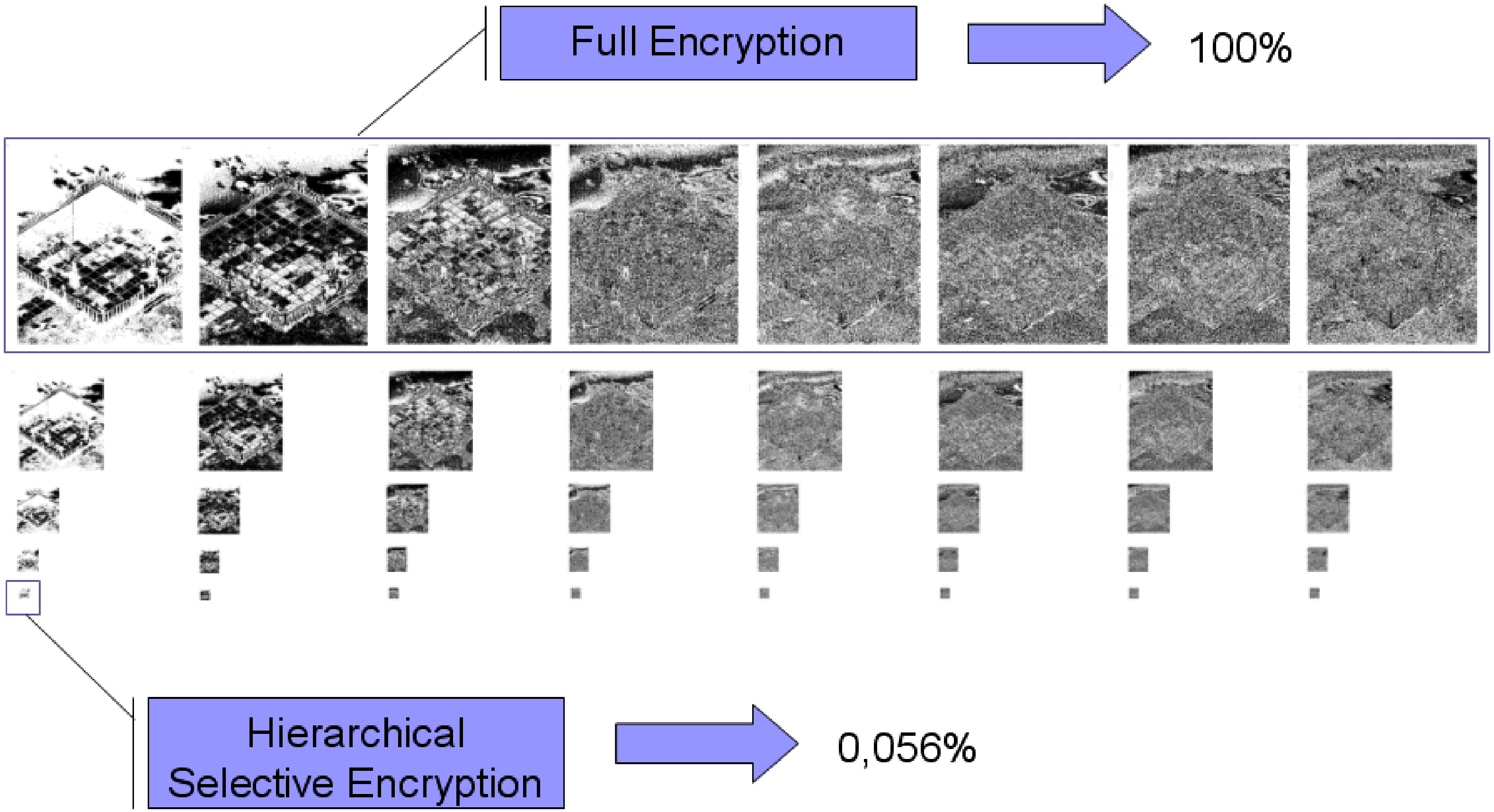
Experiments

- Experiments based on 8bpp 512 x 512 grayscale images with the lowest resolution set to 32 x 32 pixels
- Encrypted images are notated as following:

  Resolution Layer / Plane
- In example:

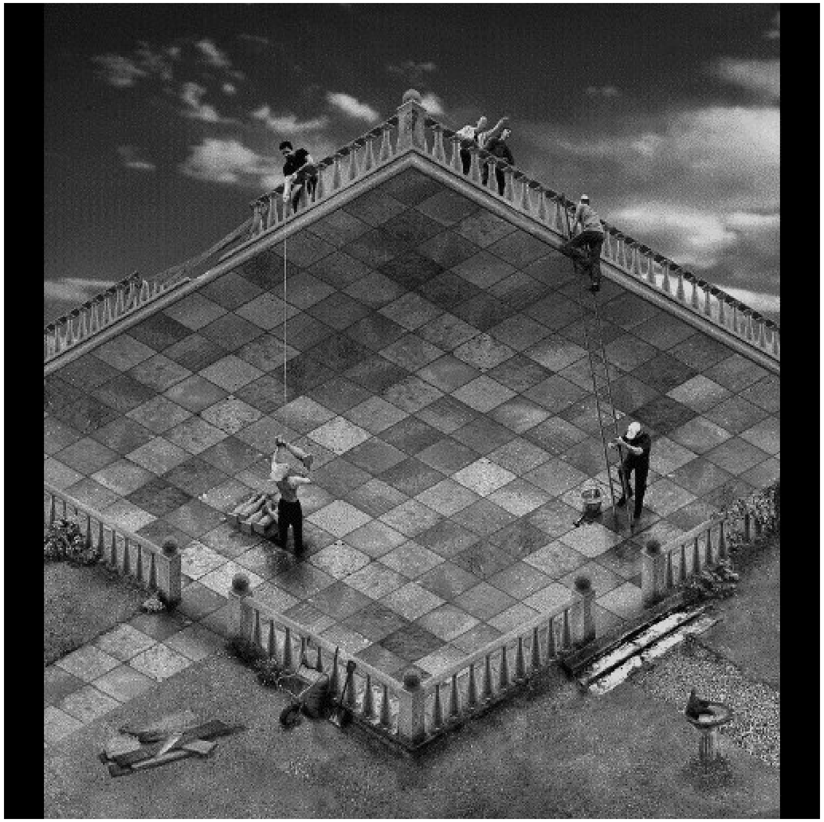
  1(5) / 4(8)

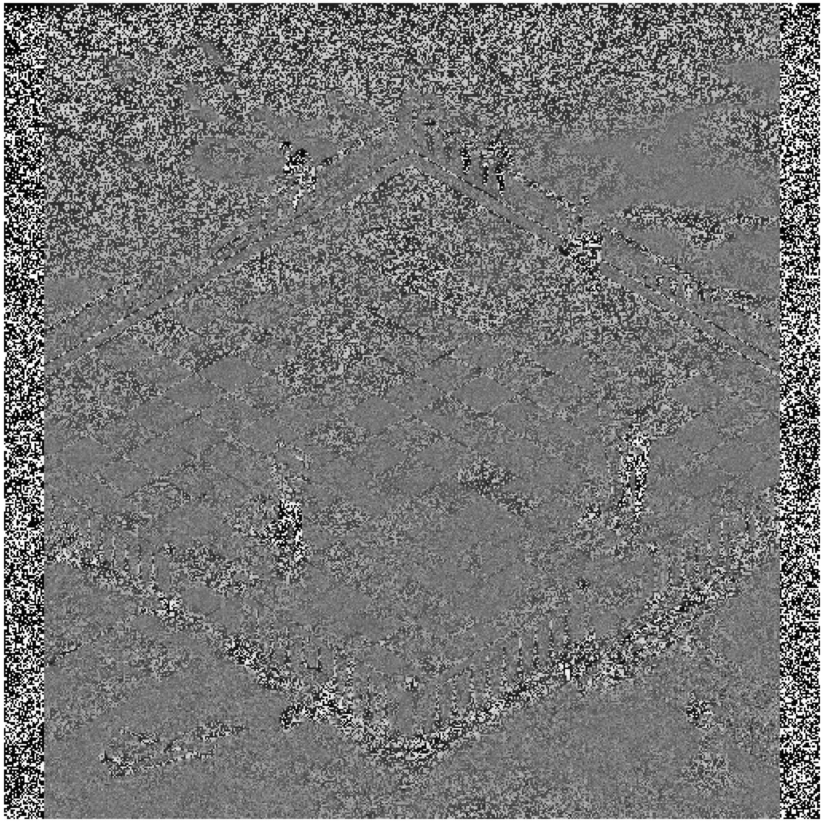
Experiments



Experiments

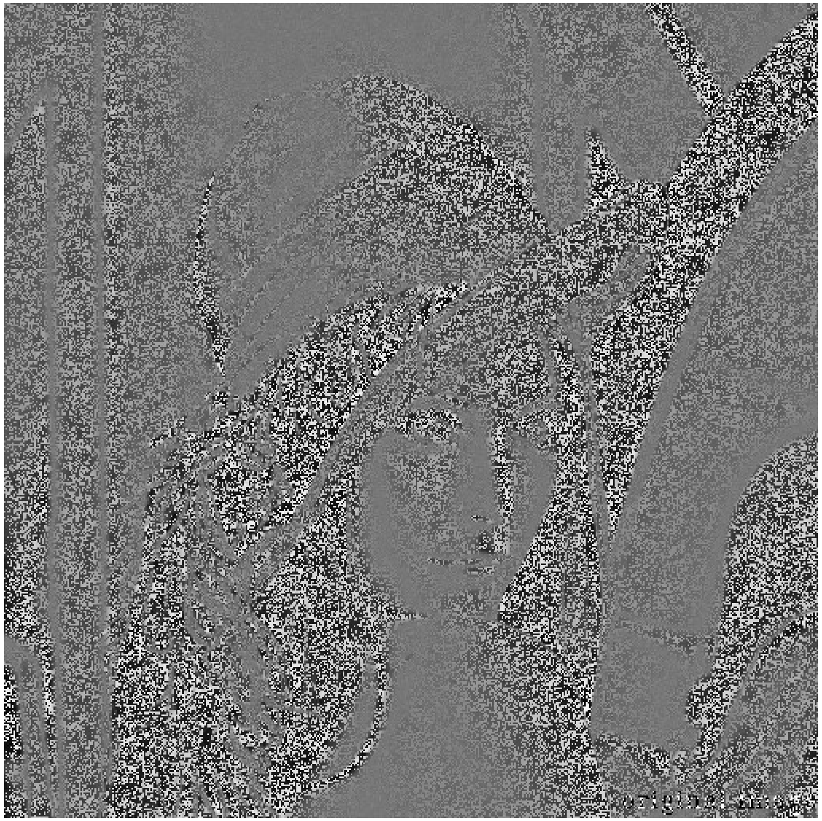
- 1(5) / 1(8) → 0,056 % (116 Bytes)





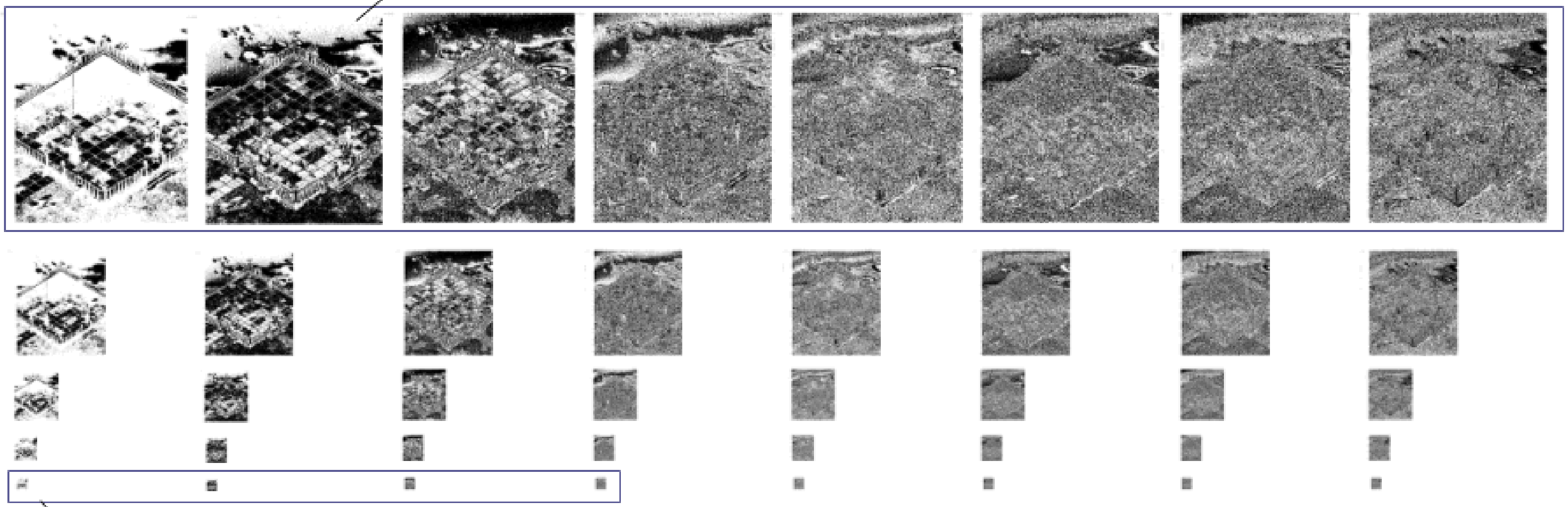
Experiments

- 1(5) / 1(8) → 0,066 % (117 Bytes)



Experiments

Full Encryption → 100%



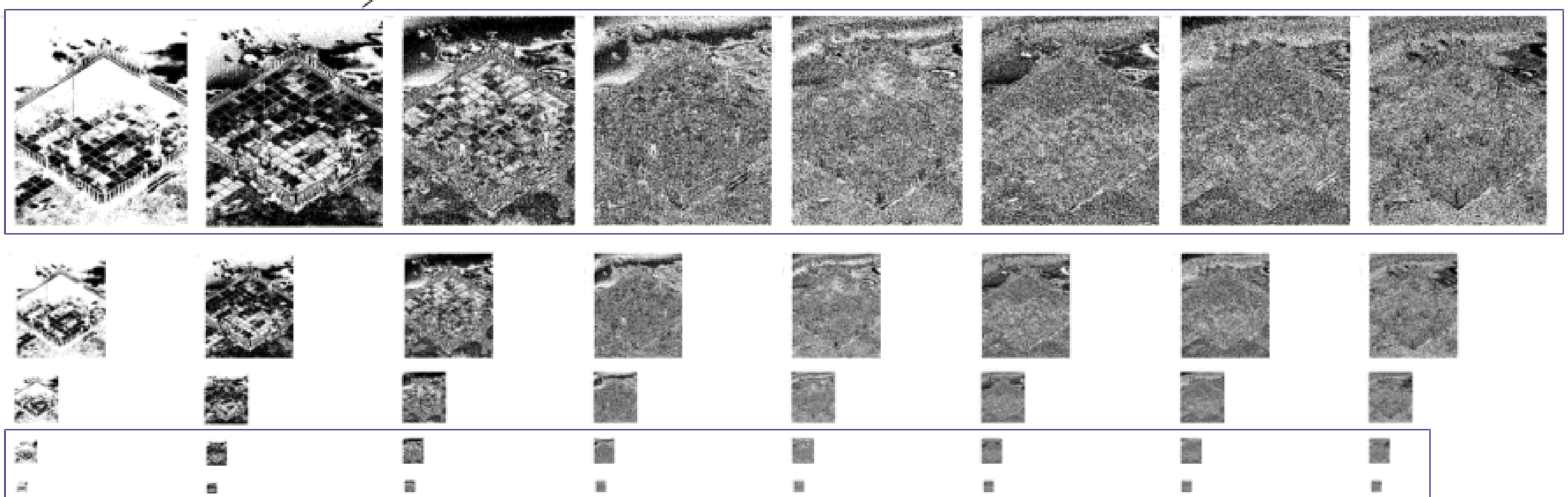
Hierarchical Selective Encryption → 0,265 %

Experiments

- 1(5) / 4(8) → 0,265 %

Experiments

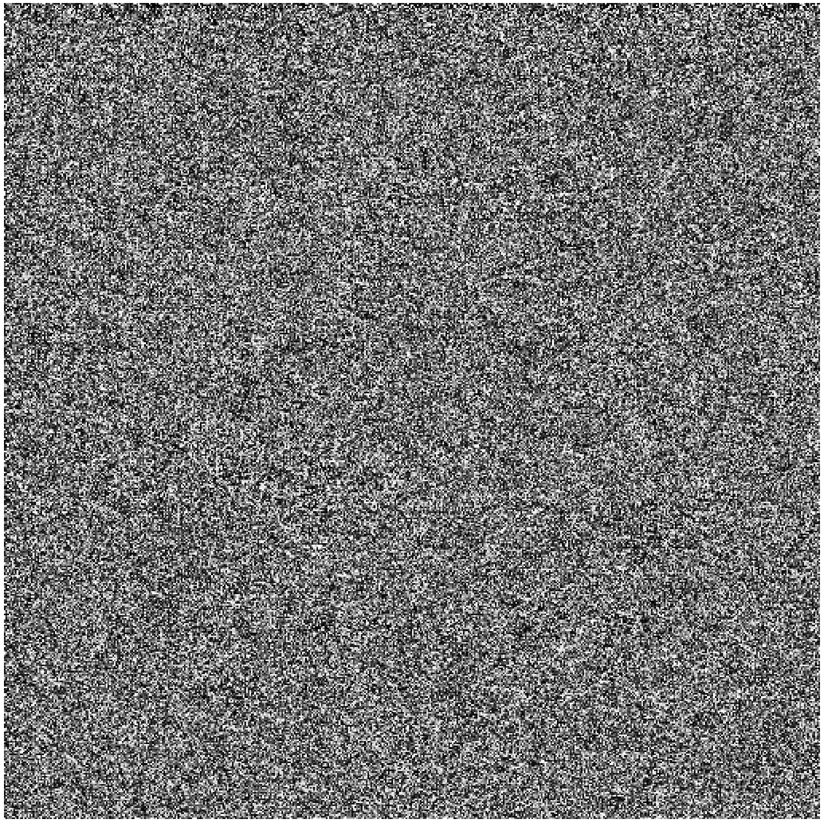
Full Encryption → 100%



Hierarchical Selective Encryption → 2,292 %

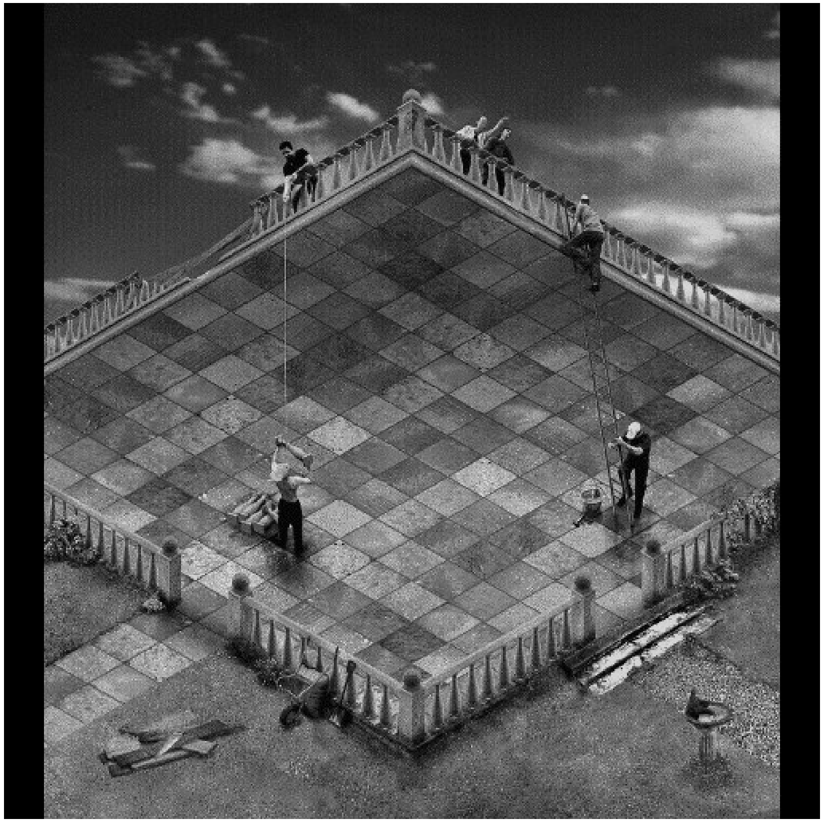
Experiments

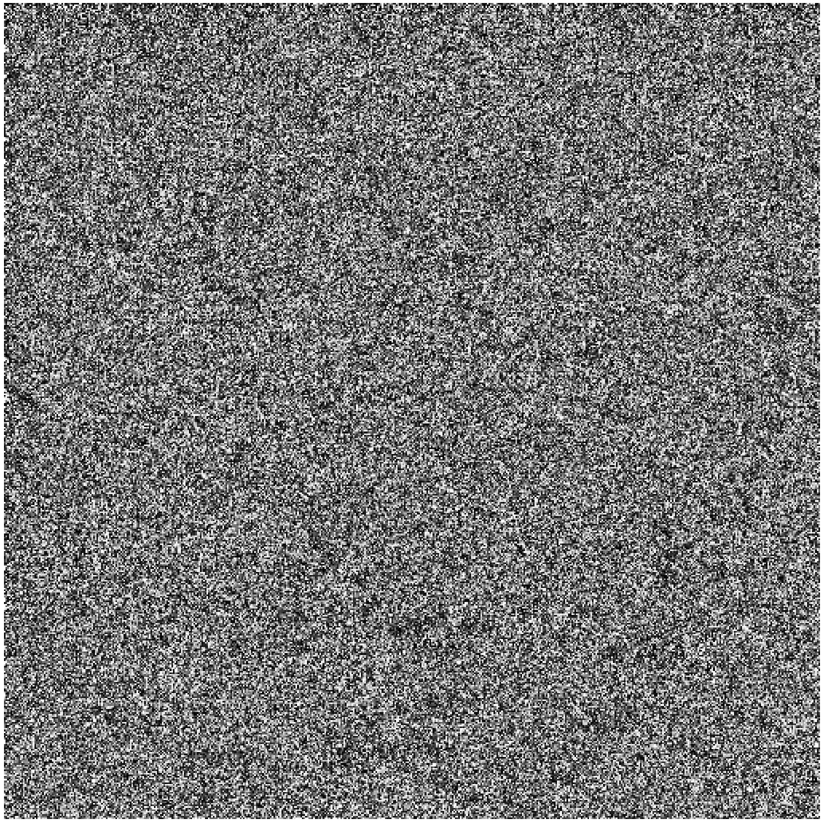
- 2(5) / 8(8) → 2,292 %



Experiments

- 2(5) / 8(8) → 1,977 %



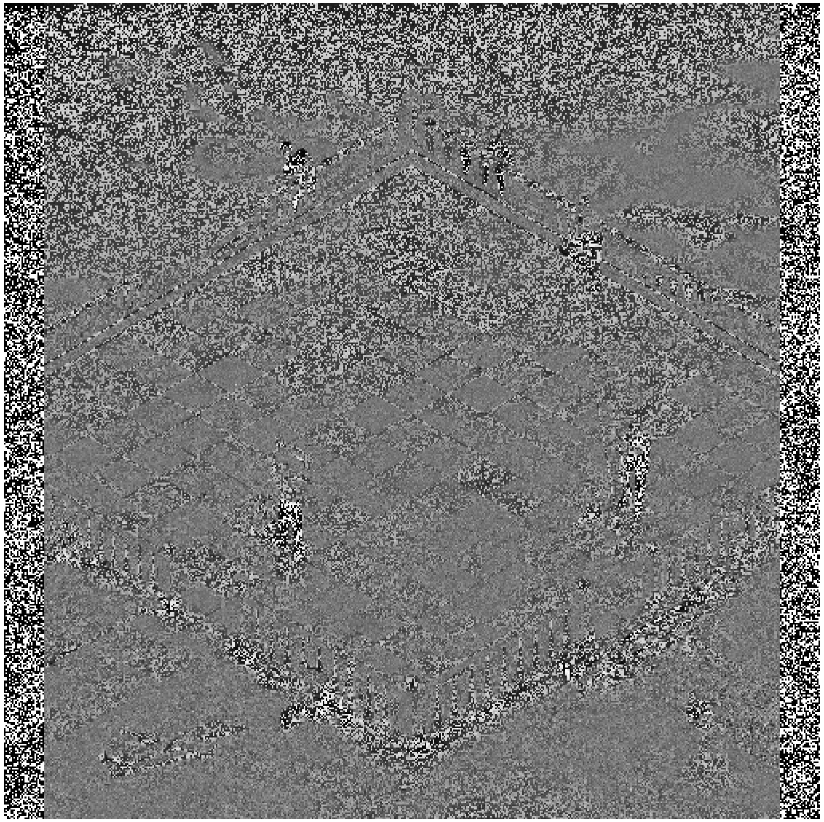


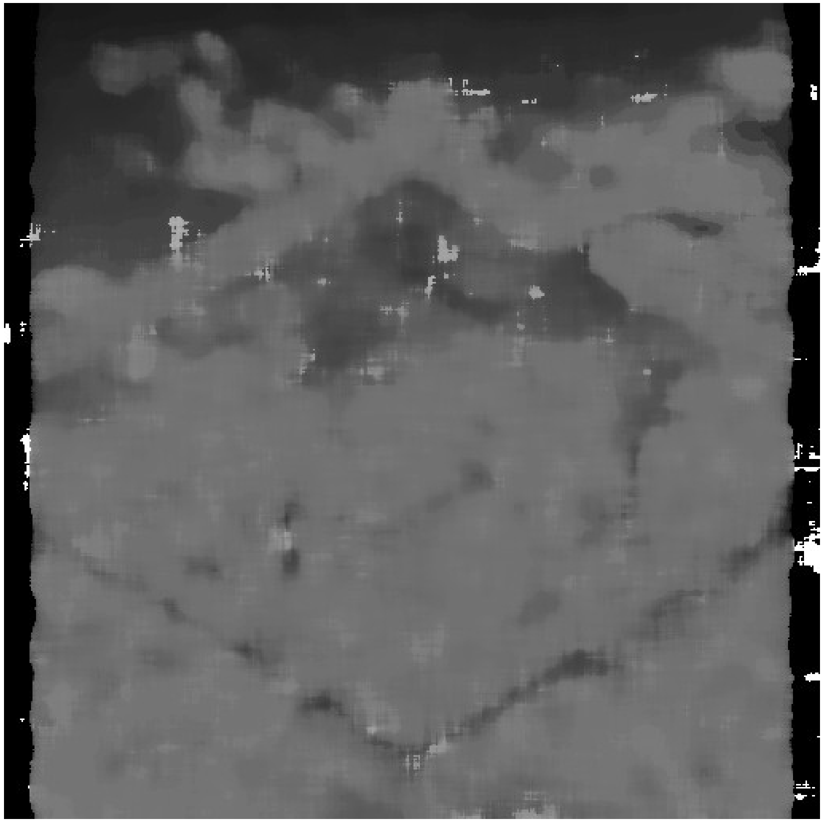
Attack resistance

- For testing attack resistance, we are using
  - Median filtering
  - Edge detection
  - Replacement attack
    - Replacing encrypted planes by constant zero data
    - Compensate zero data by changing average luminance

Attack resistance

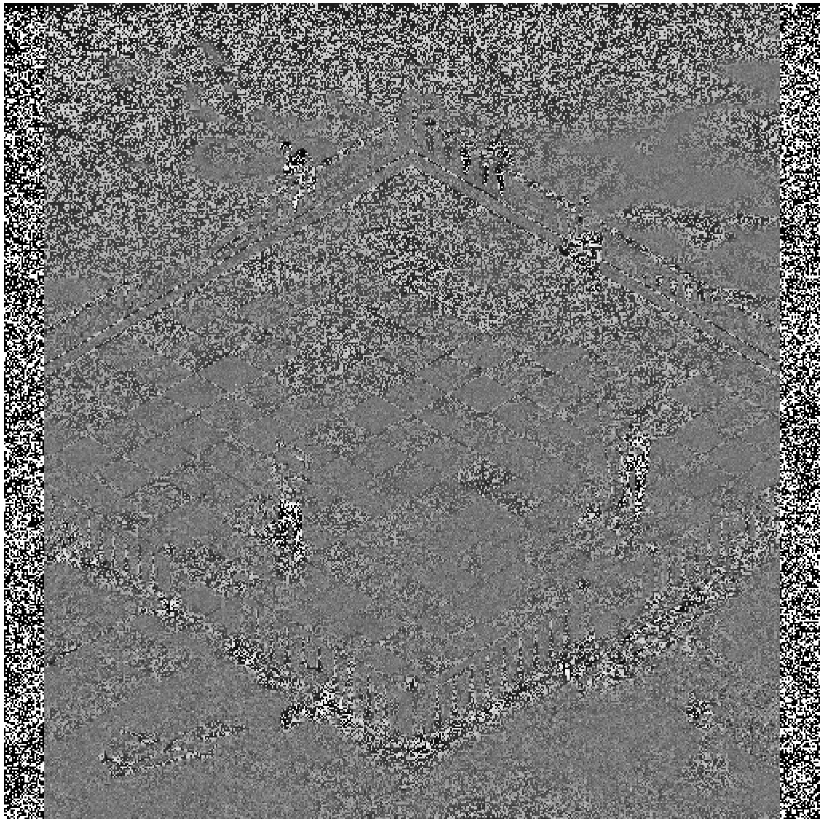
- Median filtering on 1(5) / 1(8) → 0,066 %

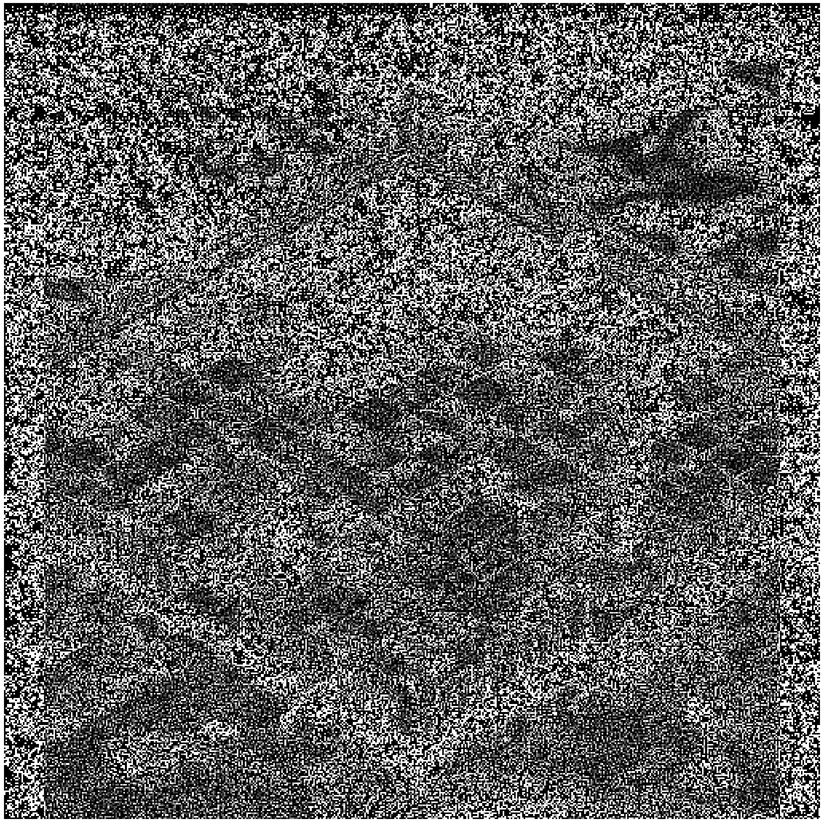




Attack resistance

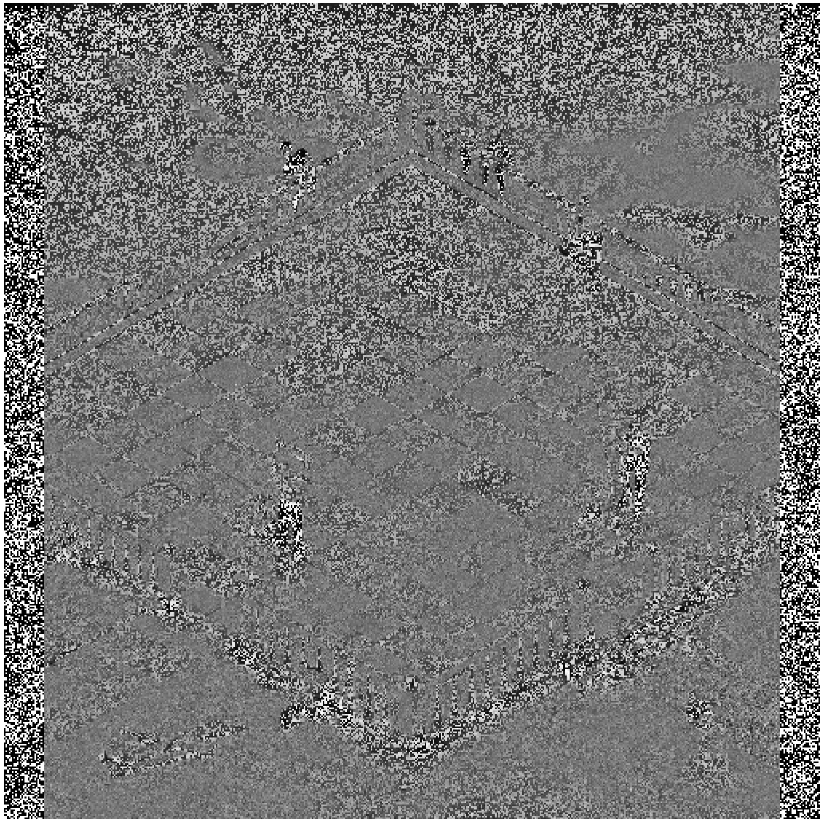
- Edge detection on / 1(5) / 1(8) → 0,066 %

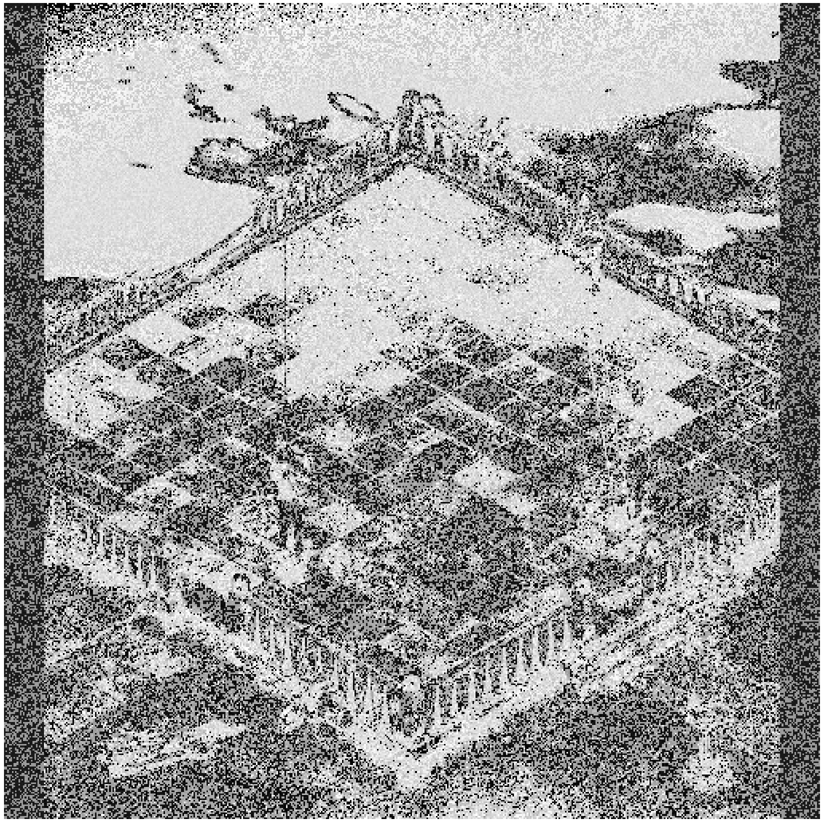




Attack resistance

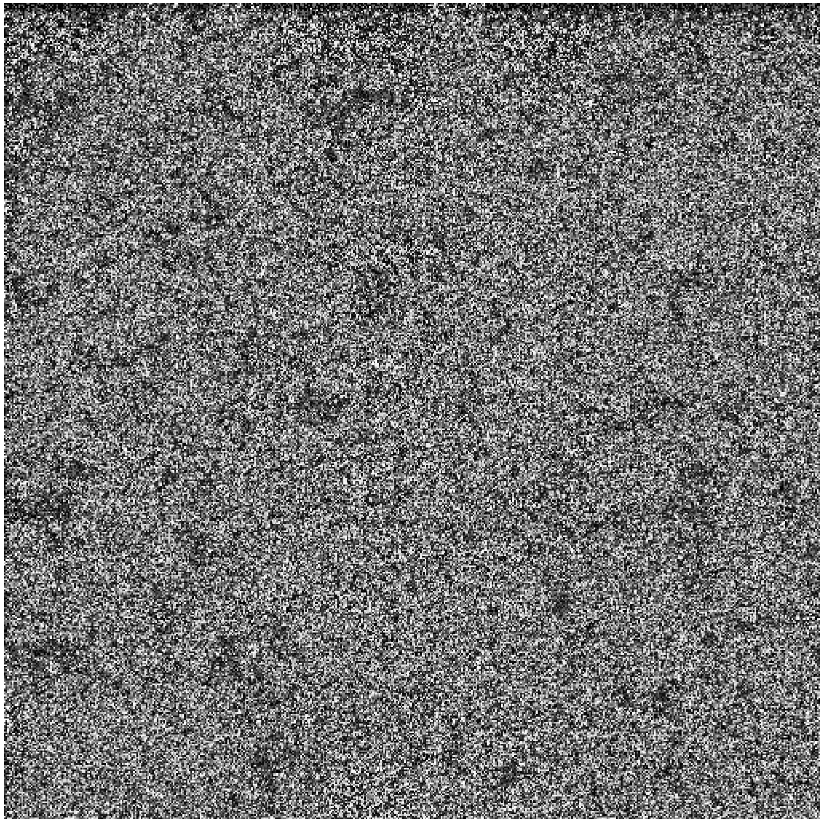
- Replacement attack on 1(5) / 1(8) → 0,066 %

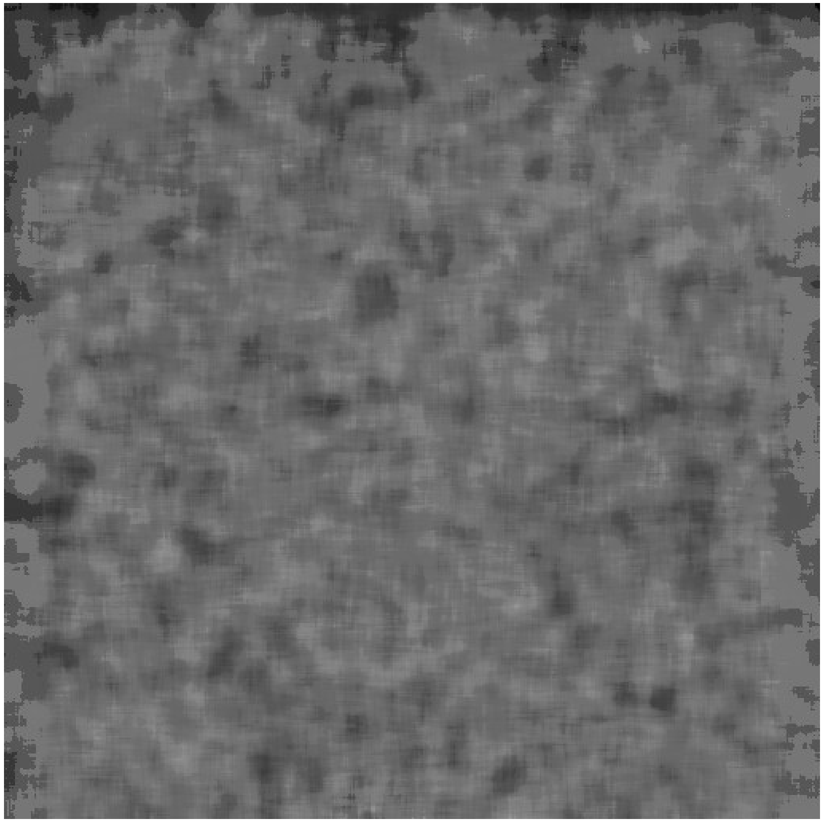




Attack resistance

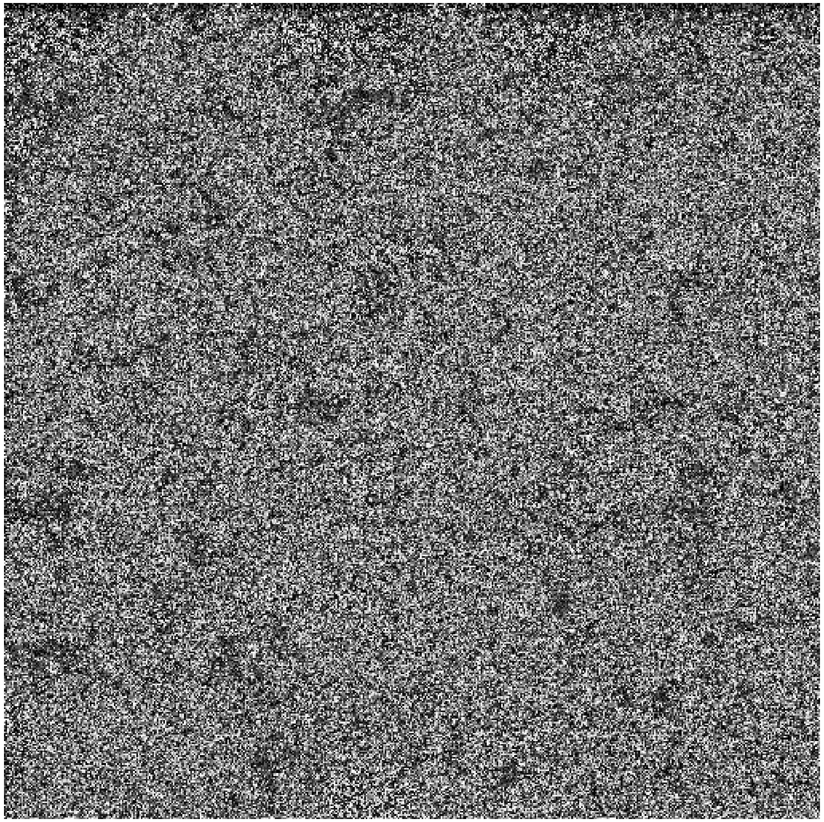
- Median filtering on 1(5) / 4(8) → 0,265 %

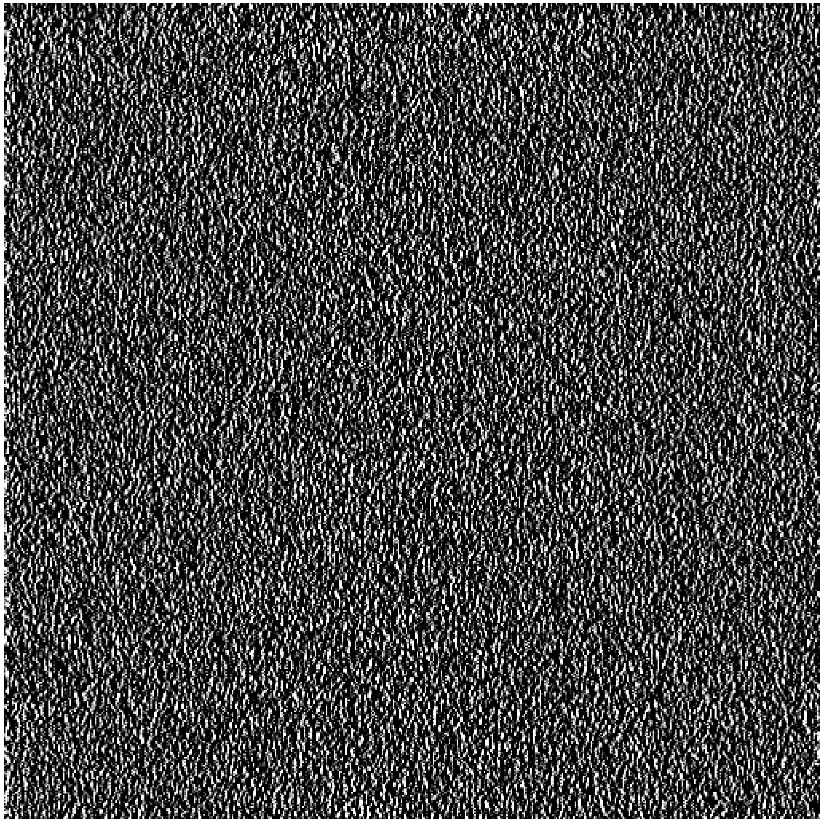




Attack resistance

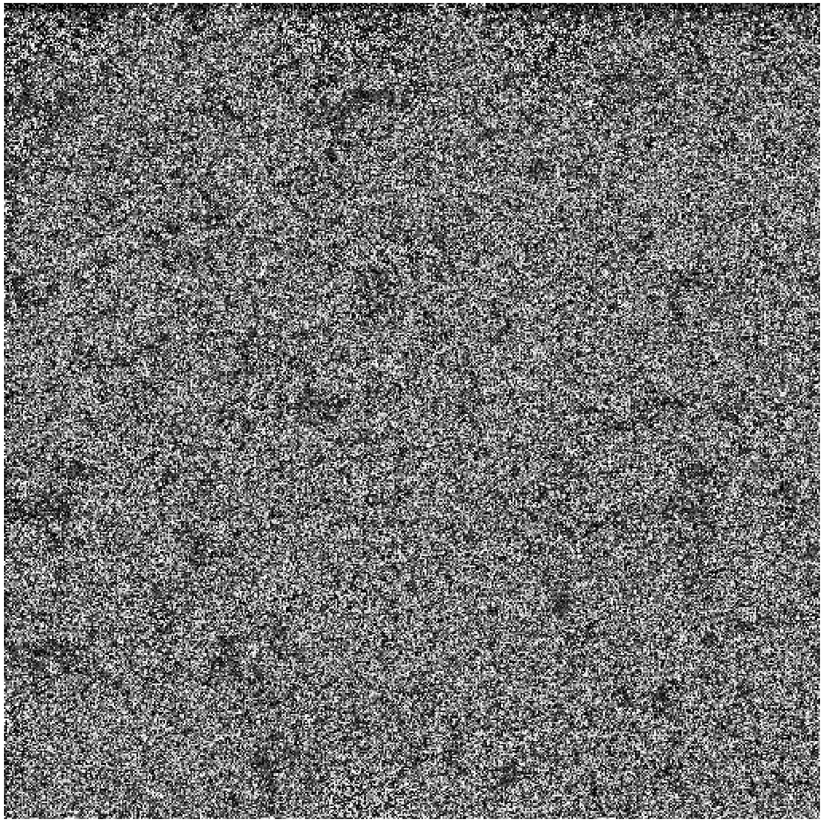
- Edge detection on 1(5) / 4(8) → 0,265 %

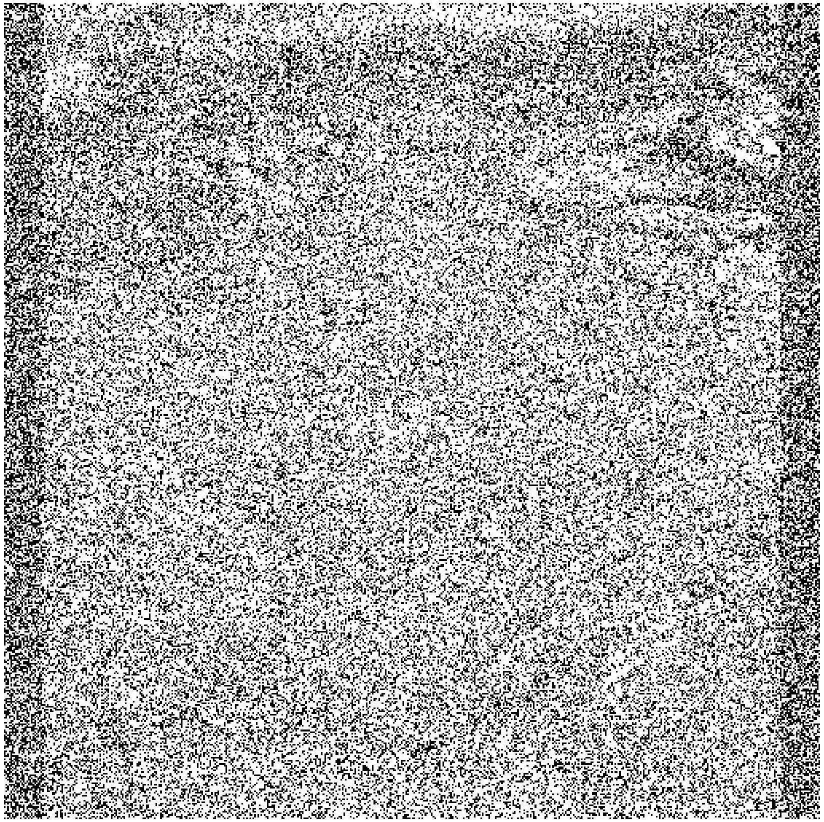




Attack resistance

- Replacement attack on 1(5) / 4(8) → 0,265 %





Conclusion

- The scenario when encrypting the lowest two resolution layers of all planes
  2 (5) / 8 (8)
  can be considered secure in any case.
- In this attack resistant scenario only 1% - 2% of data have to be encrypted.