ICIP 2019
IEEE International Conference on Image Processing

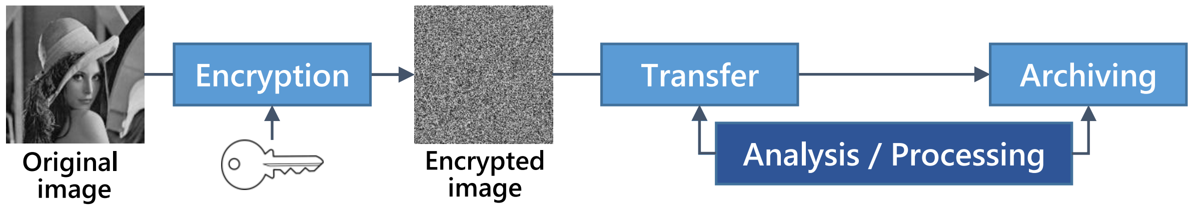
3 Minute Thesis Competition

Image Analysis and Processing in the Encrypted Domain

Pauline Puteaux – LIRMM, Univ. Montpellier/CNRS, France
pauline.puteaux@lirmm.fr

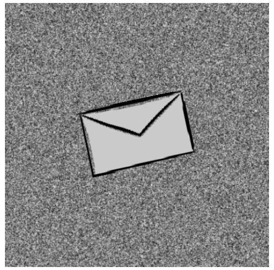
LIRMM

Context



- Thousands of images shared everyday on Internet
- Multimedia security issues
- Transfer (networks) or archiving (cloud) of these data in the encrypted form
- Format compliance and size preservation
- Necessity of analyzing and processing these data without knowing the encryption key

MSB-Based Reversible Data Hiding in Encrypted Images



- Effective technique to embed data in the encrypted domain
- Use of MSB (Most Significant Bit) instead of LSB
- Three different approaches:
  - Correction of prediction errors
  - Embedding of prediction errors
  - Recursive processing of each bit-plane
- Very high embedding capacity (higher than 1 bit-per-pixel)
- Lossless reconstruction

P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," IEEE Transactions on Information Forensics and Security, vol. 13, no. 7, pp. 1670–1681, 2018.

Recompression of JPEG Crypto-Compressed Images

- Limited bandwidth or storage capacity
- Direct JPEG recompression does not allow decryption
- Recompression directly in the encrypted domain
- Division by 2 of each quantized encrypted DCT coefficient
  - Non-zero: removal of the last bit
  - Zero: encoded in the RLE of the next non-zero
- Decoding with adapted quantization table, multiplication by 2
- No artifact, visual confidentiality

V. Itier, P. Puteaux, and W. Puech, "Recompression of JPEG crypto-compressed images without a key," IEEE Transactions on Circuits and Systems for Video Technology, 2019.

Correction of Noisy Encrypted Images

- Encrypted data can be damaged during its transmission
- Difficult to reconstruct the original image, even with the key
- New error detection and correction framework
- Knowing if a block is in clear or still encrypted using:
  - Shannon entropy after quantization
  - Convolutional neural network
- Alternative to error correcting codes
- No additional data and format compliance

P. Puteaux and W. Puech, "Noisy encrypted image correction based on Shannon entropy measurement in pixel blocks of very small size," in 2018 European Signal Processing Conference (EUSIPCO), 2018, pp. 161–165.

Privacy Protection for Social Media

- Multi-party privacy protection conflicts on social networks
- Hierarchical secret image sharing scheme
- Application of Belenkiy's disjunctive multi-level approach
- (k, n) scheme
  - n users
  - k users are needed to reconstruct the image
  - Use of a public share
- Efficient in terms of security in real application cases

S. Beugnon, P. Puteaux, and W. Puech, "Privacy protection for social media based on a hierarchical secret image sharing scheme," in 2019 IEEE International Conference on Image Processing (ICIP), 2019, pp. 679–683.