Secret JPEG Image Sharing

Pauline Puteaux

CRIStAL, Université de Lille, Centrale Lille, CNRS (Lille)

Journées Nationales du GDR Sécurité Informatique – Journée commune des GT C2 et SDM du GDR ISIS

June 26th 2023

Motivations

- Intensive image exchanges over social networks.
- Standard compression format is JPEG.

How can we ensure JPEG image security ?

G.K. Wallace, "The JPEG still picture compression standard." Communications of the ACM 34.4 (1991): 30-44.

Motivations

- Intensive image exchanges over social networks.
- Standard compression format is JPEG.

How can we ensure JPEG image security ?

- Crypto-compression is often used **BUT** depends on a secret key.

Solution: Using secret sharing jointly to JPEG compression.

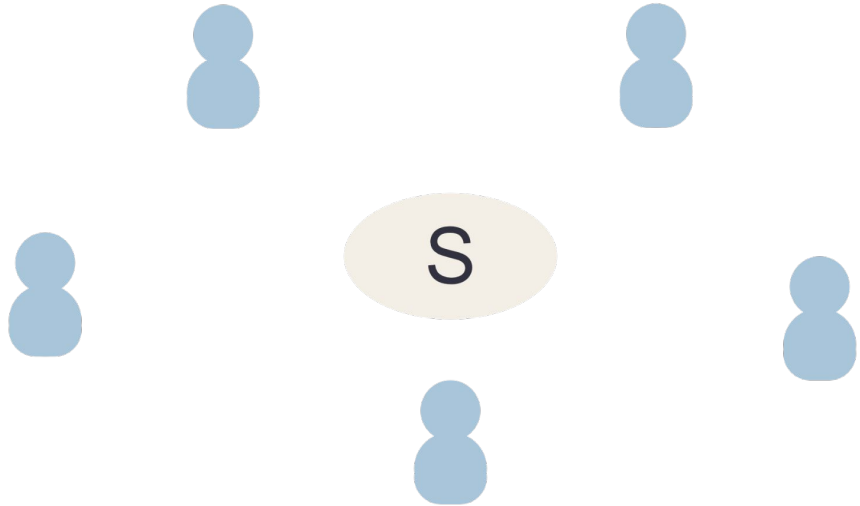
G.K. Wallace, "The JPEG still picture compression standard." Communications of the ACM 34.4 (1991): 30-44.

Secret sharing

- Number of users: n

- For instance:

  $n = 5$



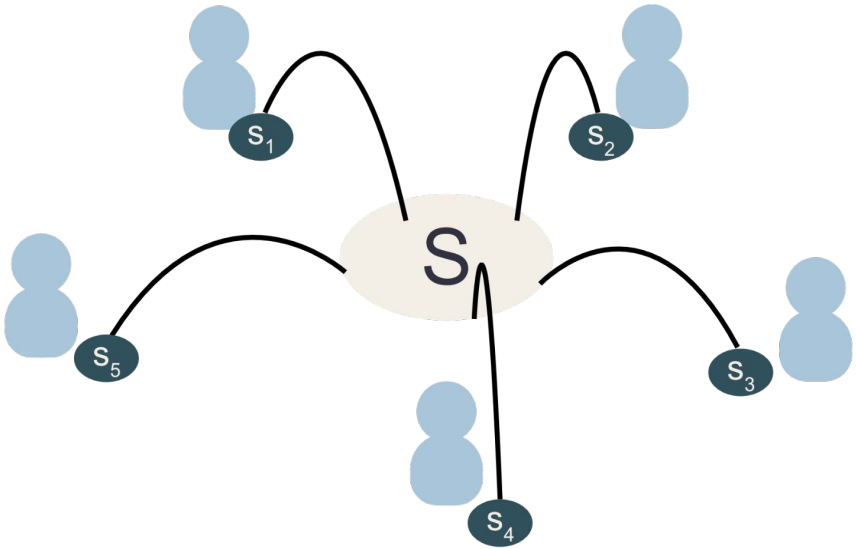
A. Shamir, "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

Secret sharing

- Number of users: n

- For instance:

  $n = 5$



A. Shamir, "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

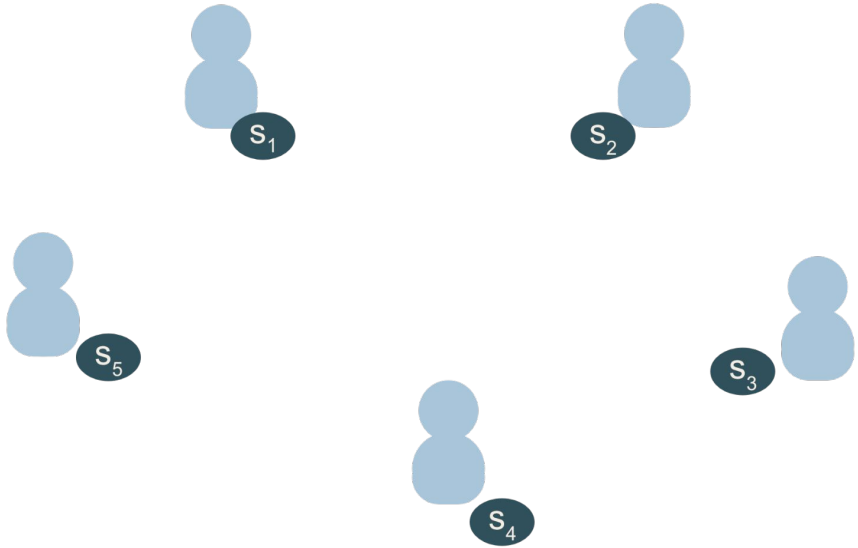
Secret sharing

- Number of users: n
- Threshold: k

- For instance:

  $n = 5$

  $k = 3$



A. Shamir, "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

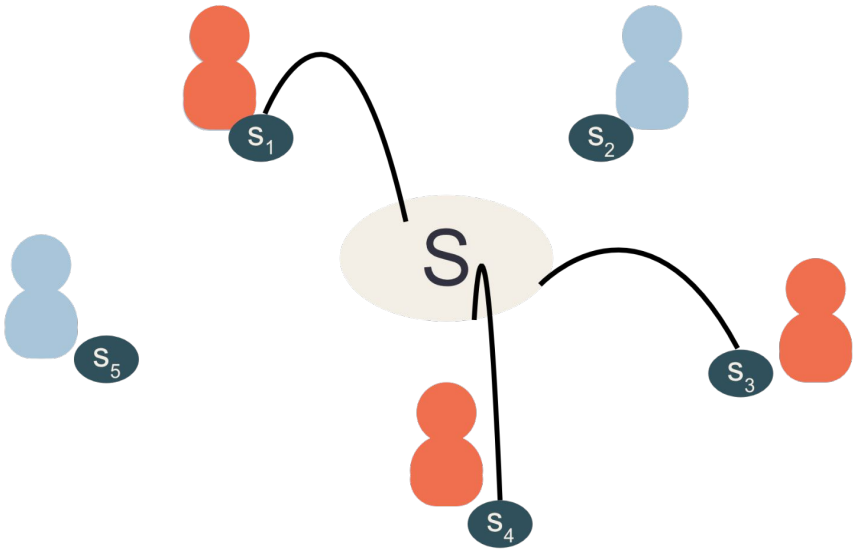
Secret sharing

- Number of users: n
- Threshold: k

- For instance:

  $n = 5$

  $k = 3$



A. Shamir, "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

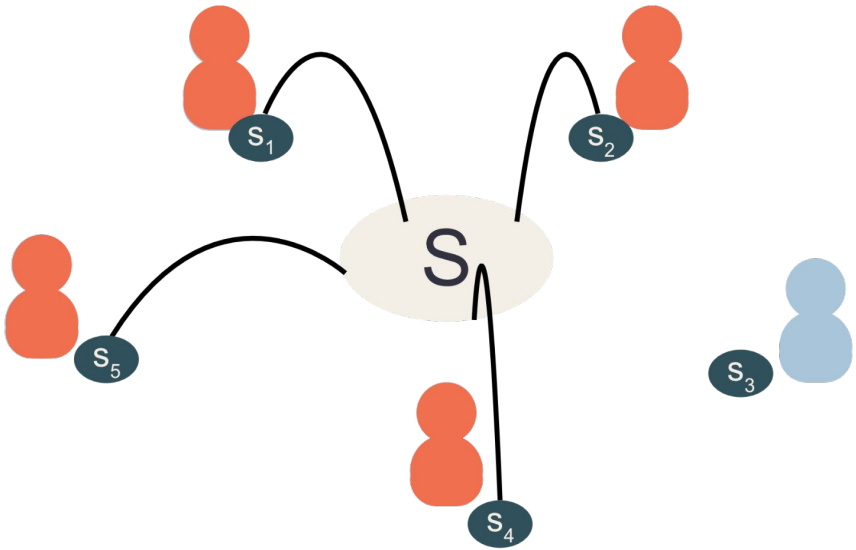
Secret sharing

- Number of users: n
- Threshold: k

- For instance:

  $n = 5$

  $k = 3$



A. Shamir, "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

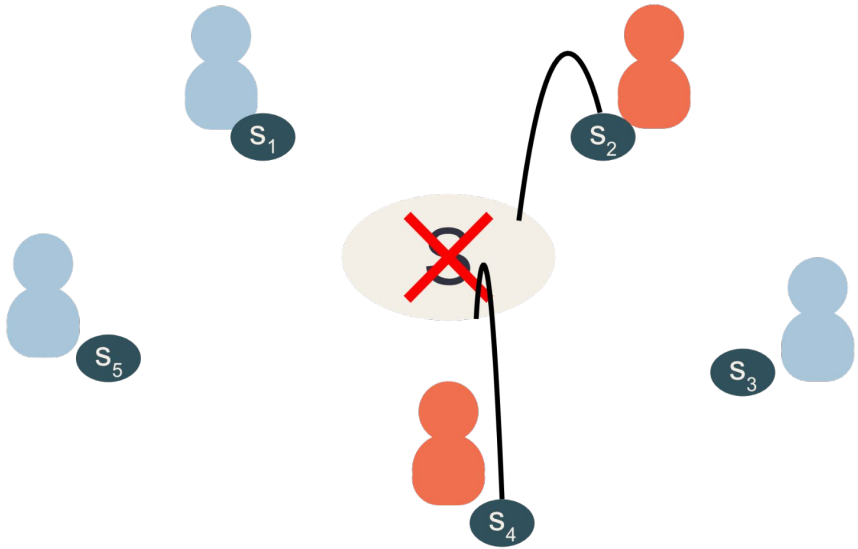
Secret sharing

- Number of users: n
- Threshold: k

- For instance:

  $n = 5$

  $k = 3$



A. Shamir, "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

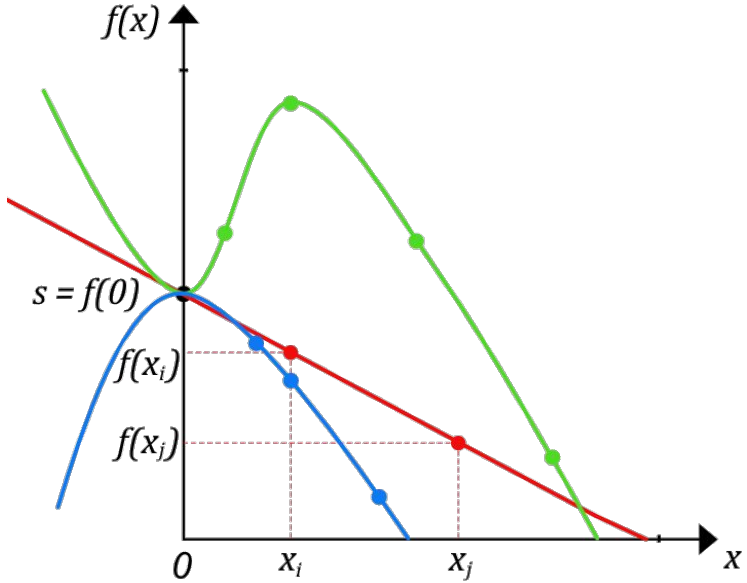
Secret sharing

- Number of users: *n*
- Threshold: *k*

How does it work?

- Secret value to share: *s*
- Finite field
- Based on polynomial interpolation:

$$f(x) = \left(\sum_{l=1}^{k-1} a_l x^l \right) + s$$

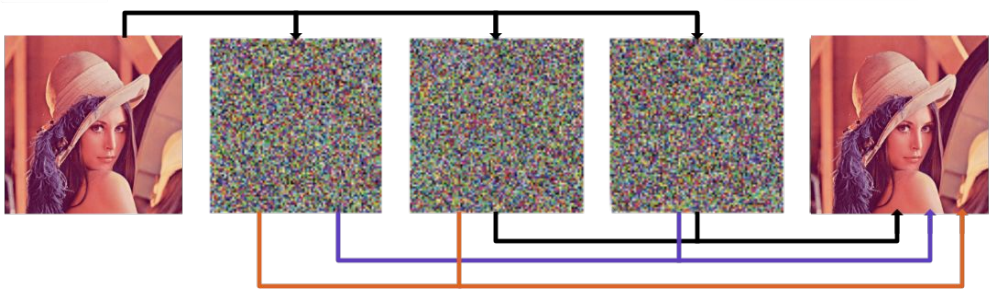


A. Shamir, "How to share a secret." Communications of the ACM 22.11 (1979): 612-613.

Secret image sharing

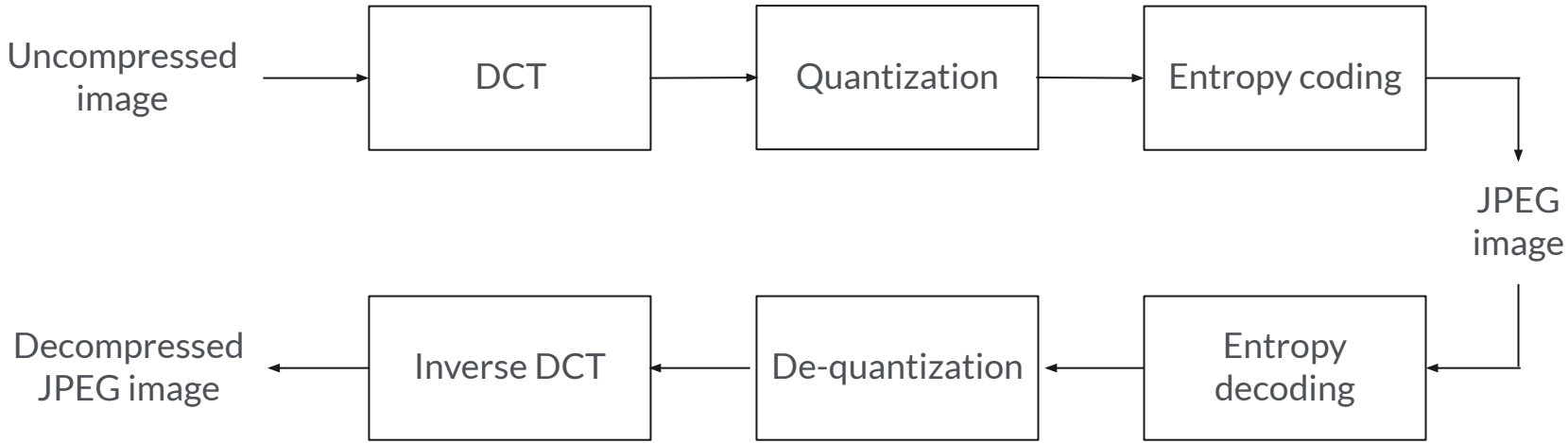
- Sharing pixel values.
- Each user receives a shared image.

How to extend this principle to JPEG images?

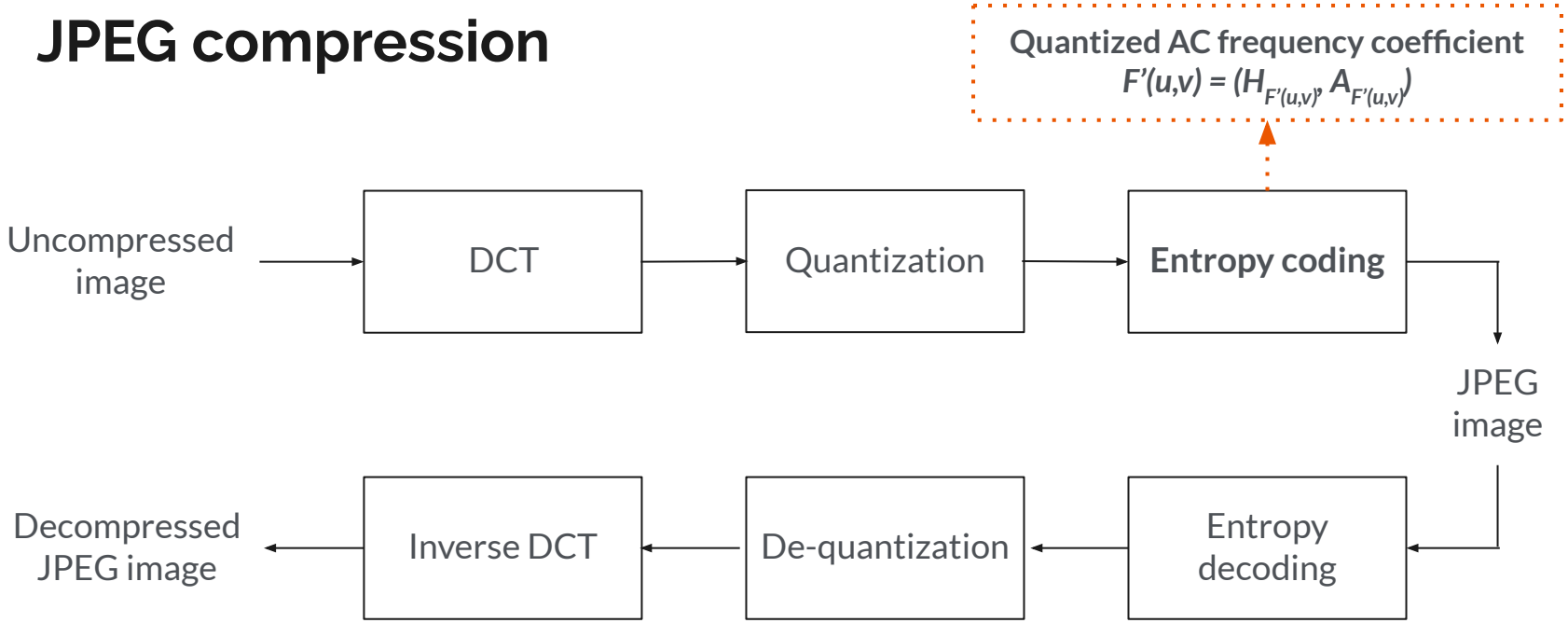


C. C. Thien and J. Lin, "Secret image sharing." Computers & Graphics 26.5 (2002): 765-770.

JPEG compression



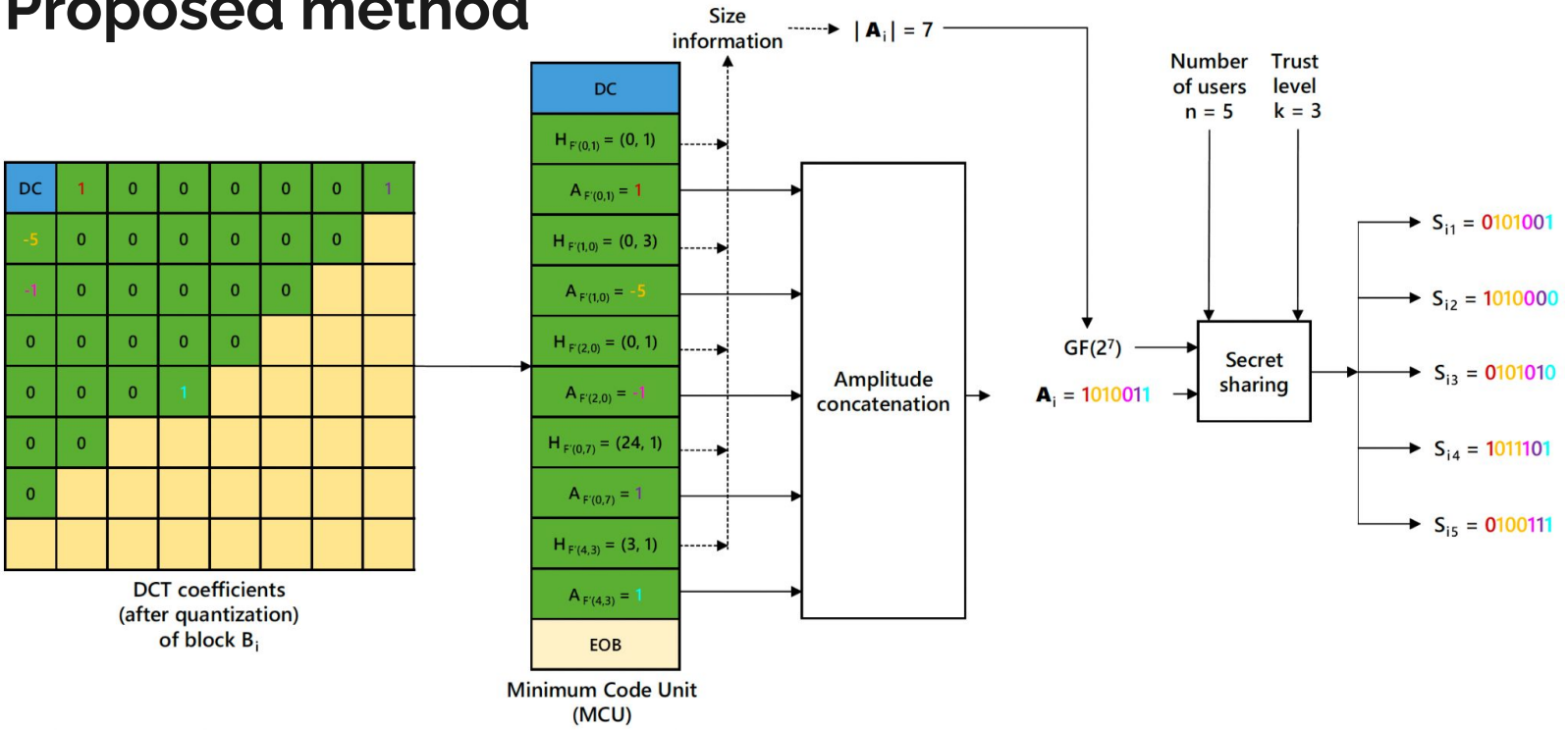
JPEG compression



Proposed method

- During the **entropy coding** of JPEG
- For each quantized DCT block B_i
- **Concatenation** of the amplitudes $A_{F'(u,v)}$ to obtain a **secret** $\boldsymbol{A}_i$
  - If $|\boldsymbol{A}_i| < log_2(n+1)$: B_i remains in the clear domain.
  - If $|\boldsymbol{A}_i| \geq log_2(n+1)$:
    - ***(k,n)*-secret sharing over the Galois field $GF(2^{|Ai|})$**
    - n shared values S_{ij} obtained ($1 \leq j \leq n$)
    - S_{ij} injected by substitution into each shared JPEG image SI_j

Proposed method



Detailed example

- Original uncompressed image (197 kB) from UCID database.
- Shared JPEG image, with $k = 3$, $n = 5$ and QF = 90 (79 kB).

- **High frequency details are secured** (PSNR = 14 dB).
- Compressed shared images are of the **same size** as the reconstructed image.

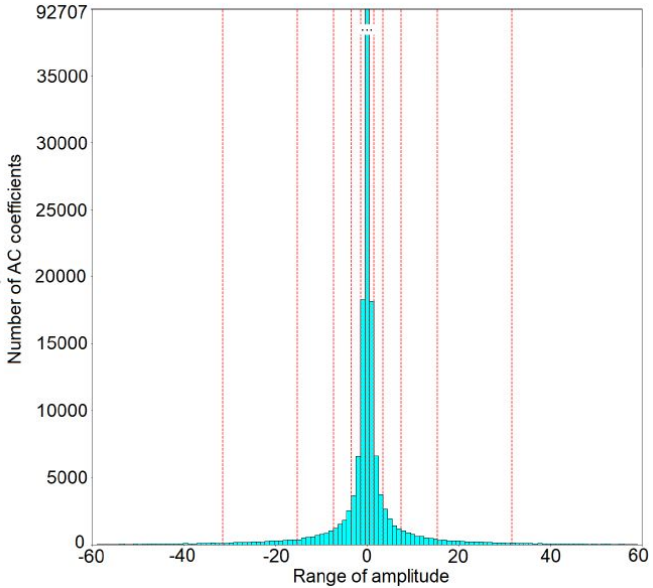
G. Schaefer and M. Stich, "UCID: An uncompressed color image database," in Storage and Retrieval Methods and Applications for Multimedia, vol. 5307, 2004, pp. 472–480.

Detailed example

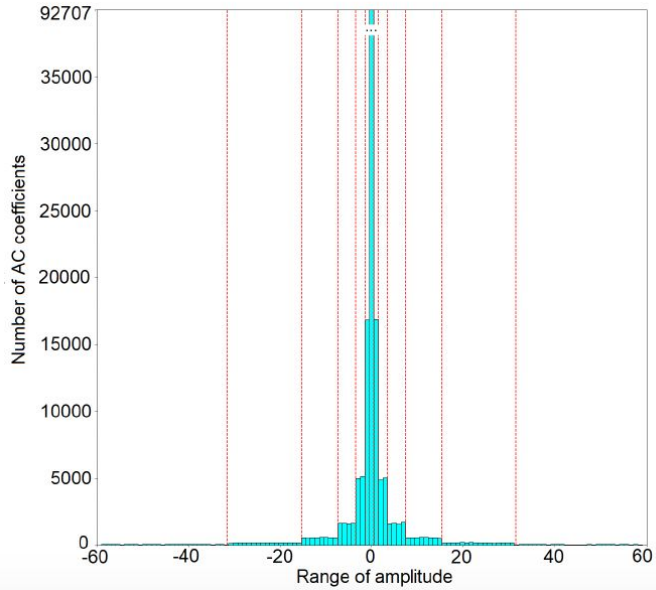
- Original image directly compressed with JPEG, QF = 90 (79 kB).
- Reconstructed JPEG image, QF = 90 (79 kB).

- **The two images are the same.**

AC coefficients' distribution



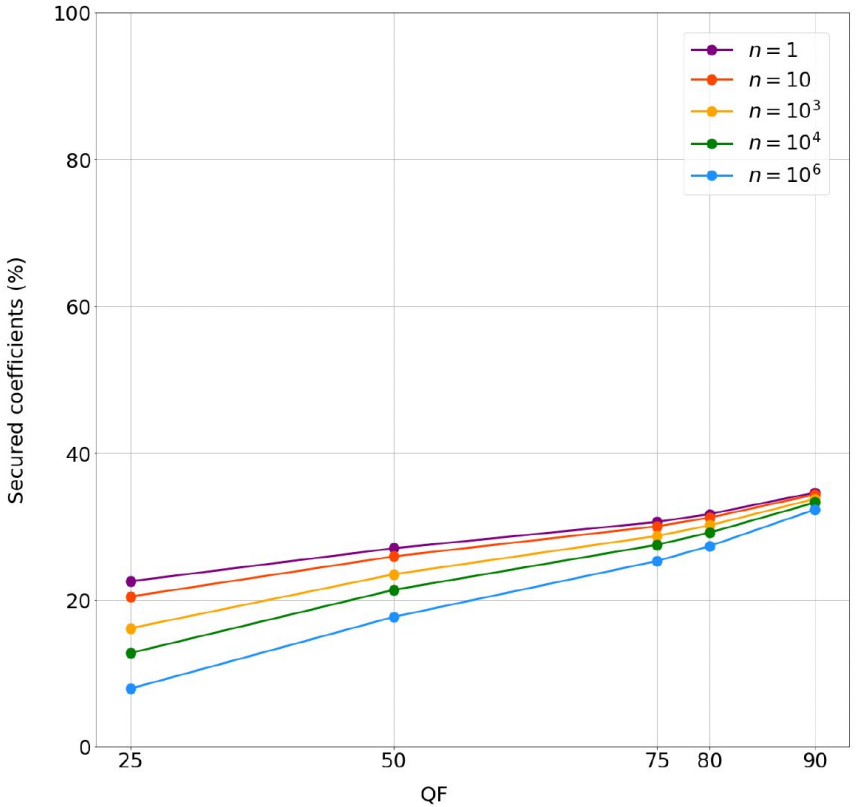
JPEG compressed image (QF = 90).



Shared JPEG image (QF = 90).

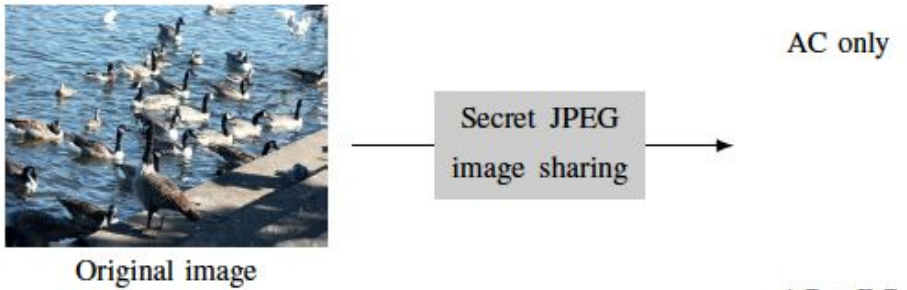
Sharing space

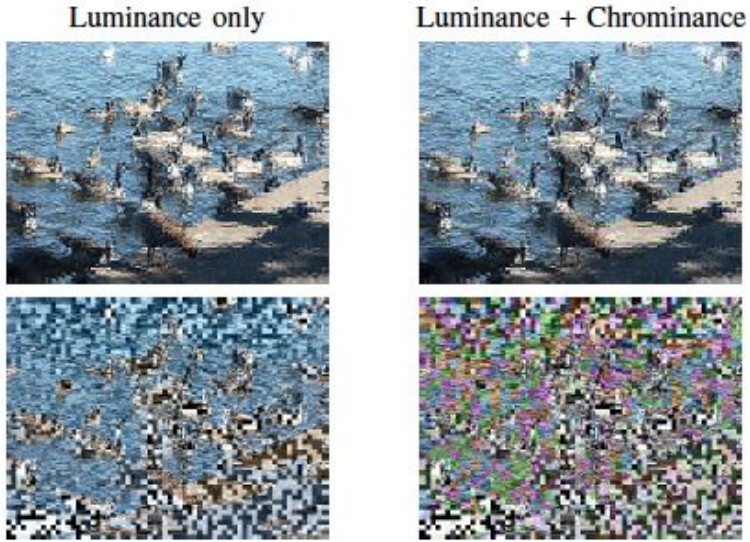
- Percentage of secured bits over the image size (in bits), as a function of the QF.
- The bigger is *n*, the larger is the number of blocks that remain in clear.
- **Similar results as with JPEG crypto-compression.**



Visual security levels (color image)

- QF = 90.
- Four possible combinations of our method.





D. Engel, T. Stütz, and A. Uhl, "A survey on JPEG2000 encryption," Multimedia systems, vol. 15, no. 4, pp. 243–270, 2009.

Conclusion and perspectives

- Secret sharing over **Galois fields** along with JPEG compression.
- **Fully format compliant** and **size preserving** method.
- **Sufficient visual security level** (identical to crypto-compression methods).

Future work?

- Studying the impact of a noisy shared JPEG image during reconstruction.

ICIP2022 BORDEAUX

IEEE Signal Processing Society

Thank you for your attention!

Our paper: P. Puteaux, F. Yriarte, and W. Puech. "**A Secret JPEG Image Sharing Method Over *GF*(2^M) Galois Fields.**"
IEEE Transactions on Circuits and Systems for Video Technology, vol. 33, no. 6, pp. 3030-3042, 2023.

Pauline Puteaux
pauline.puteaux@cnrs.fr

Journées Nationales du GDR Sécurité Informatique – Journée commune des GT C2 et SDM du GDR ISIS
June 26th 2023

cnrs CRIStAL Centre de Recherche en Informatique, Signal et Automatique de Lille — Université de Lille — centralelille