Image encryption for Secret image sharing and Reversible data hiding

William PUECH

ICAR (Image & Interaction)
LIRMM - CNRS, Univ. Montpellier

January 16, 2018

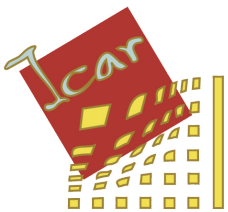


Image security

During ...

- Storage
  - Access control: identification and authorization
  - Availability
- Transmission
  - Confidentiality
  - Integrity
  - Authentication
- Visualization

Image security

- From CISCO, visual data (image and video) = 80% of the global internet traffic en 2019 (against 67% en 2014)
- Need to propose specific methods to protect visual data:
  - Data hiding (watermarking, steganography)
  - Image forensics
  - Biometrics
  - Image encryption

Image security

Data hiding

Image security

Image forensics



Image security

Biometrics

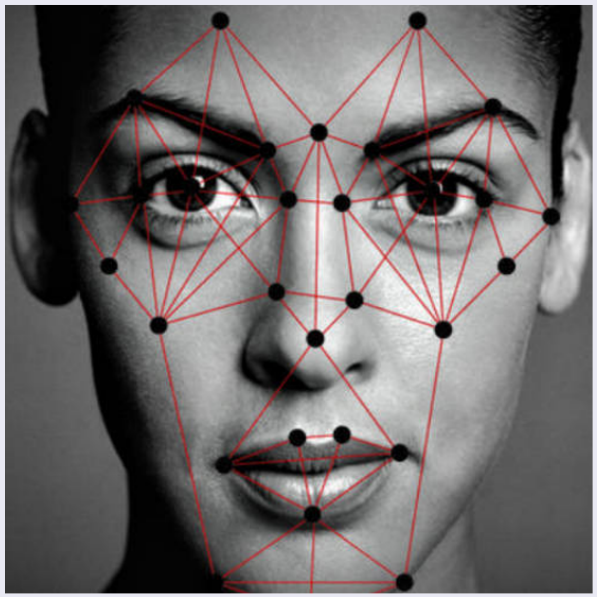


Image security

Image encryption

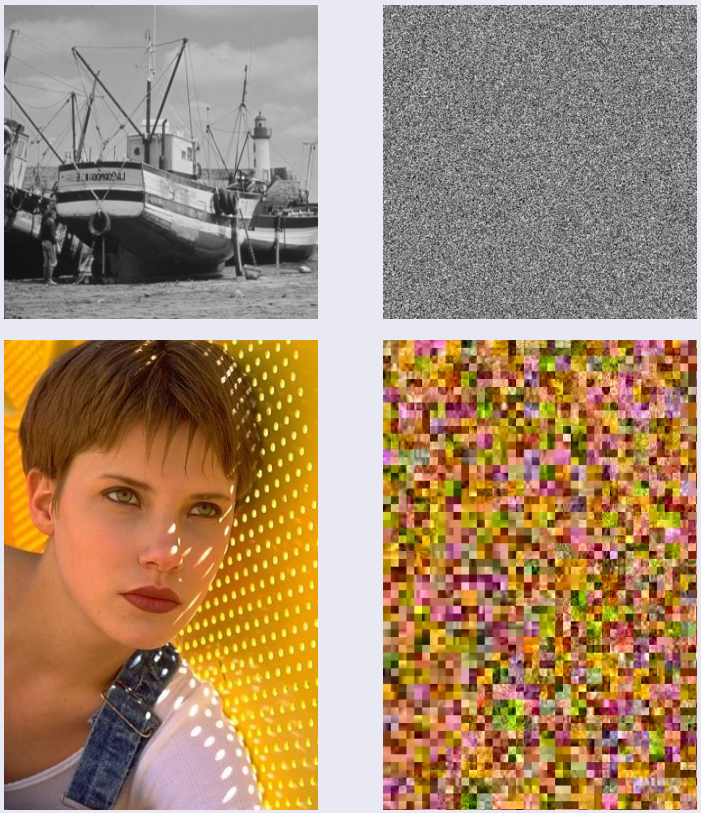


Image security

Hybrid coding for safe transmission

- Encryption, data hiding and compression
- Images, image sequences, videos and 3D objects

Image security

Hybrid coding for safe transmission

- Encryption, data hiding and compression
- Images, image sequences, videos and 3D objects

Image compression

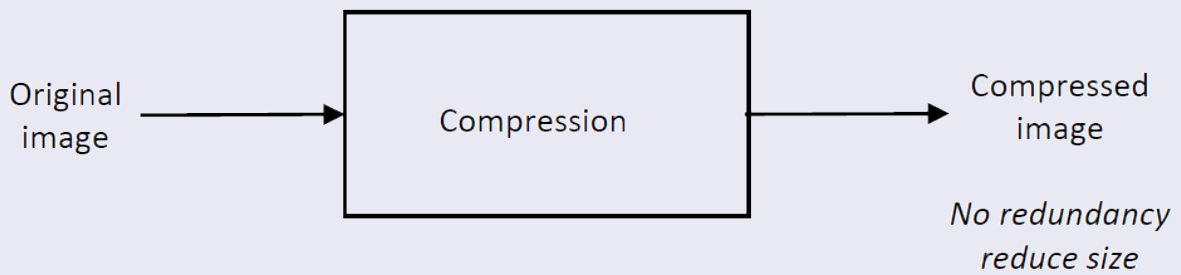


Image security

Hybrid coding for safe transmission

- Encryption, data hiding and compression
- Images, image sequences, videos and 3D objects

Image encryption

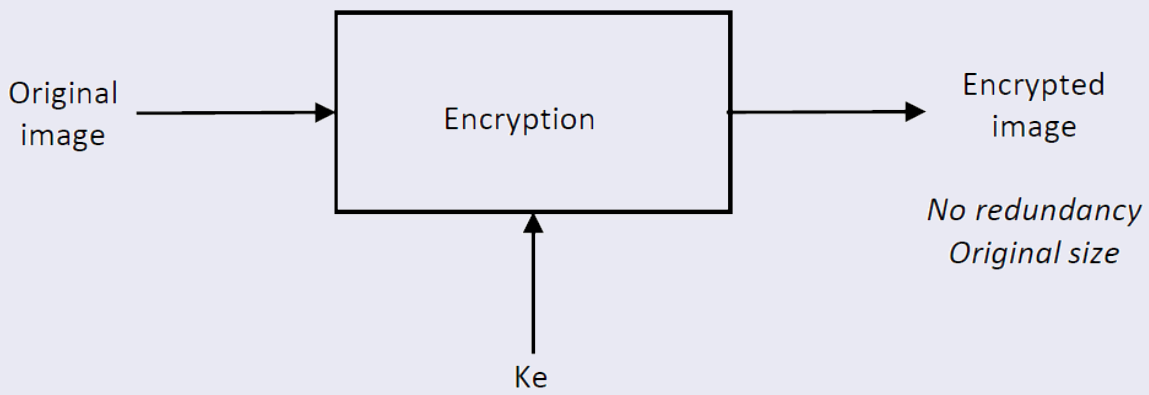


Image security

Hybrid coding for safe transmission

- Robust to noise
- Compatible with compression
- Fast: access in real time
- The secret is based on a key (secrete or private key)
  - The Algorithm is known
  - Principle of Kerckhoffs [KER 83]
- Norms and standards

A. Kerckhoffs.
La cryptographie militaire.
Journal des sciences militaires, vol. 9, pp. 5–38, 1883.

Image security

Image data hiding

- The art to embed a message in a image [COX 08] :
  - invisibility: statistically invisible
  - no removable: robust to transformations
  - payload: size of the hidden message
  - security: robust to attacks
  - complexity: real time application
- Data hiding: large payload
- Steganography: invisibility
- Watermarking: robust to attacks

I. Cox.
Digital Watermarking and Steganography.
The Morgan Kaufmann Series in Multimedia Information and Systems, M. Kaufmann, Ed. Morgan Kaufmann Publishers, 2008.

Image security

Image encryption

- The art to mask the data:
  - confidentiality: data protection
  - authentication: emitter and receiver
  - integrity: ensure the totality and the content of the data
  - non repudiation: ACK
- For visual data:
  - Image encryption ▸ example
  - Image encryption ▸ another example
  - Perceptual signature ▸ example

I. Cox.
Digital Watermarking and Steganography.
The Morgan Kaufmann Series in Multimedia Information and Systems, M. Kaufmann, Ed. Morgan Kaufmann Publishers, 2008.

Image encryption for Secret image sharing and Reversible data hiding

Outline

1) Entropy measurement
2) High capacity RDHEI
3) Secret image sharing

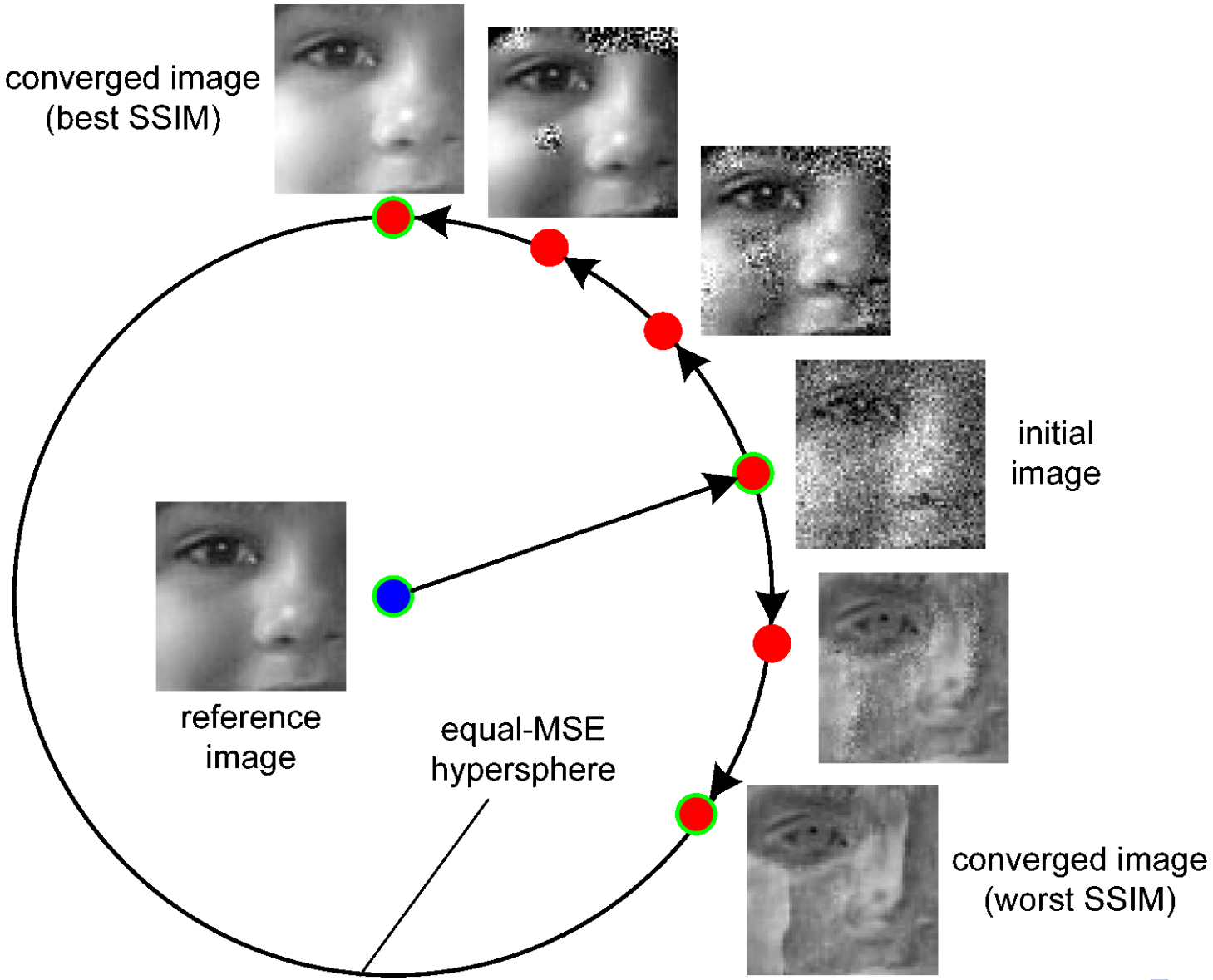
Conclusion

- Image security is necessary ...
- ... and should become mandatory.
- Image encryption can be used for several applications.
- In the case of RDHEI: cryptanalysis ans steganalysis (2016-CNRS PEPS project: WESTERN).
- Confidentiality metrics.

GT/action Sécurité et données multimédia

Remerciements

Visual data security: quality metric



Visual data security: quality metric

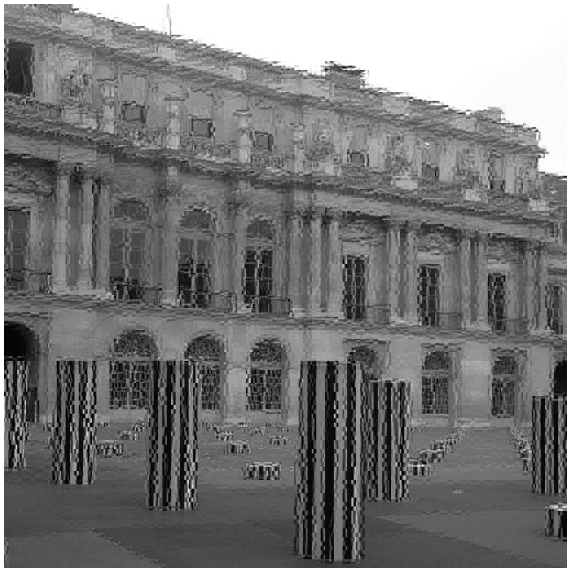
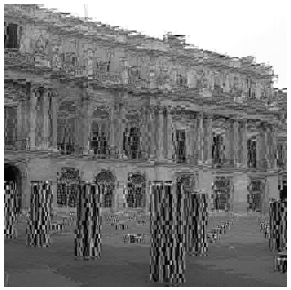
Visual data security: quality metric



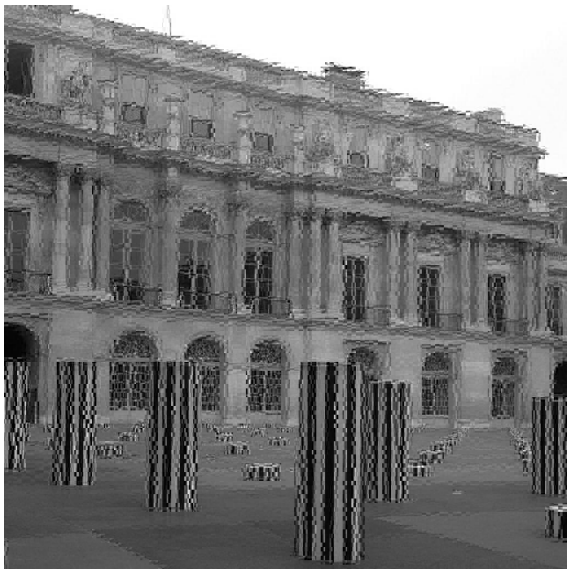
Visual data security: quality metric



Visual data security: quality metric


Visual data security: quality metric



Perceptual signatures: data integrity

Signature of a text

M1 = *“Aujourd’hui il fait beau dans le sud de la France, même si il y a un peu de vent...”*
S1 = `Ox2534A8C08E12F4A8`
M2 = *“Aujourd’hui il fait beau dans le sud de la France, même si il y a un peu de mistral...”*
S2 = `Ox3D68AB9310E38B51`

Signature of an image

S1(original image (760 kB)) = S2(compressed image (224 kB))

back

Perceptual signatures: data integrity

Signature of a text

M1 = *“Aujourd’hui il fait beau dans le sud de la France, même si il y a un peu de vent...”*
S1 = `Ox2534A8C08E12F4A8`
M2 = *“Aujourd’hui il fait beau dans le sud de la France, même si il y a un peu de mistral...”*
S2 = `Ox3D68AB9310E38B51`

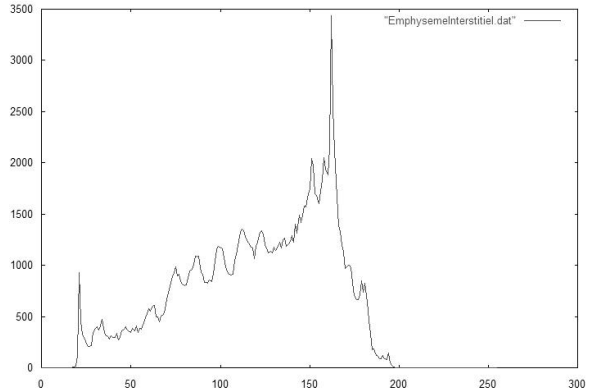
Signature of an image

S1(original image (760 kB)) = S2(compressed image (224 kB))

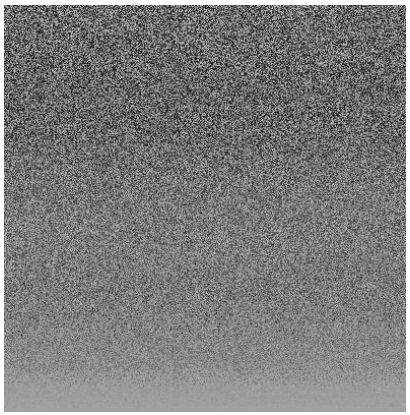
back

Image encryption

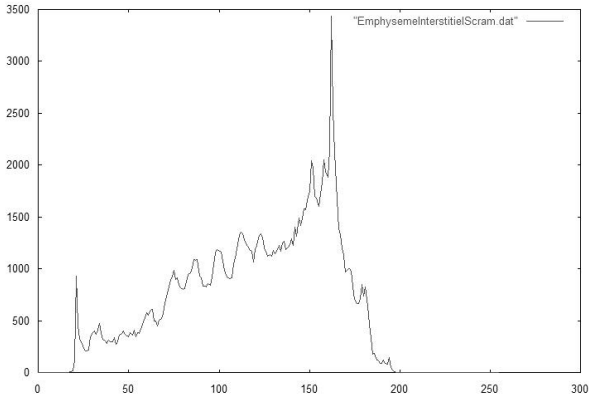
(a)



(b)



(c)

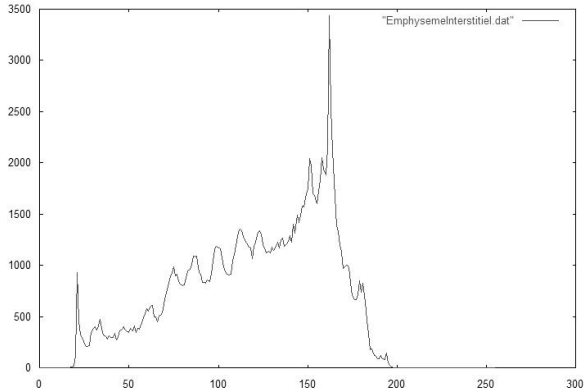


(d)

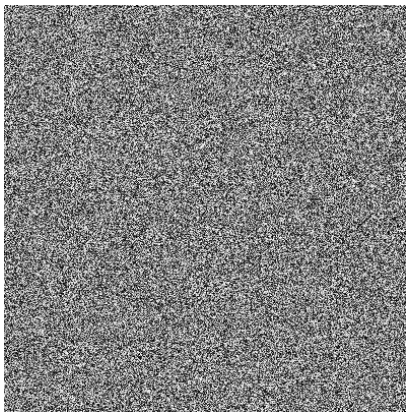
a) Original image, b) histogram, c) encrypted image by scrambling, d) histogram of the encrypted image.

Image encryption

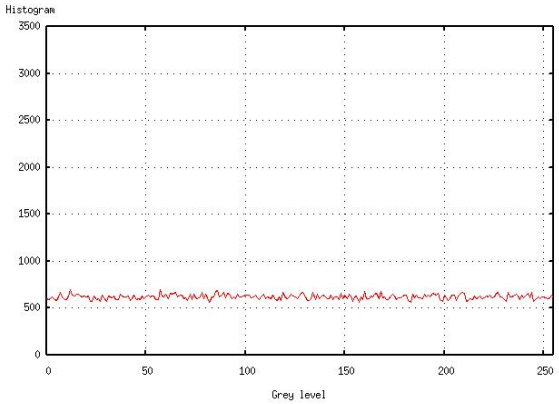
(a)



(b)



(c)

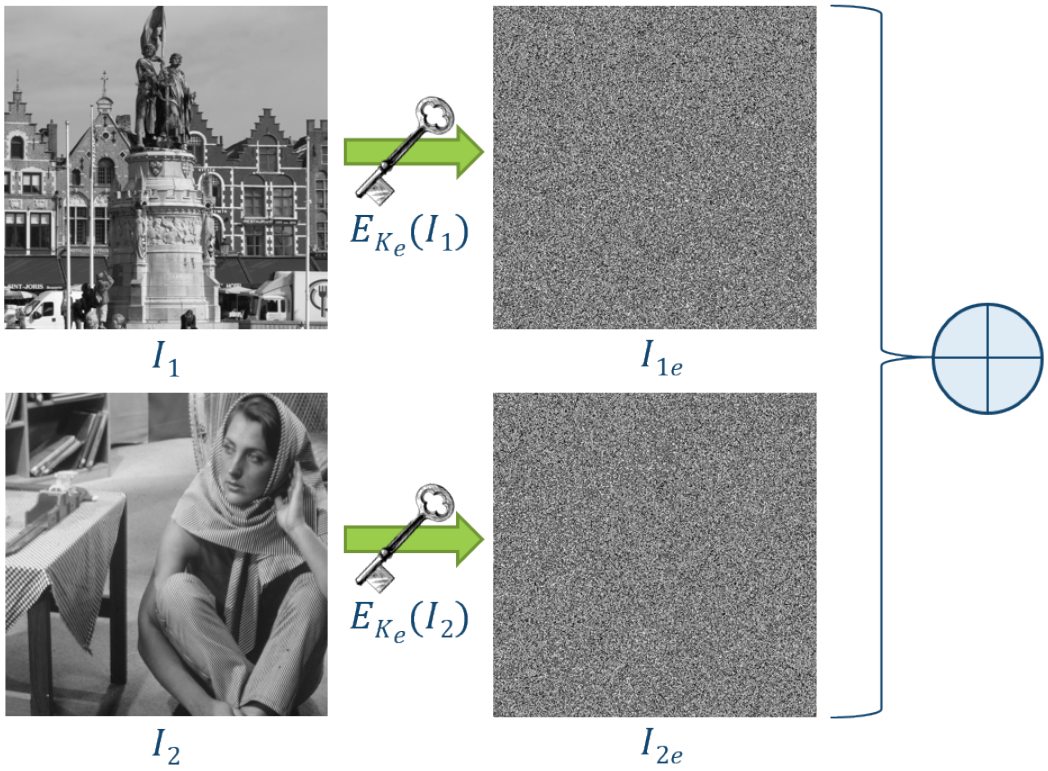


(d)

a) Original image, b) histogram, c) encrypted image with a stream cipher algorithm, d) histogram of the encrypted image.

back

Image encryption



XOR encryption.

back