Medical image protection (2D/3D) 
data hiding, selective encryption and secret sharing

William PUECH

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

November 14, 2019
During ...

- **Storage**
  - Access control: identification and authorization
  - Availability

- **Transmission**
  - Confidentiality
  - Integrity
  - Authentication

- **Visualization**
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

[Two images side by side: one of a tree, the other of a cat]
Image security

Image forensics
Image security

Biometrics

- Fingerprint
- Iris scan
- Facial recognition
Image security

Image encryption

[Images of original and encrypted images]
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

Original image → Compression → Compressed image

No redundancy, reduce size
Image security

Hybrid coding for safe transmission

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

Image encryption

Original image $\rightarrow$ Encryption $\rightarrow$ Encrypted image

Ke

No redundancy
Original size
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 (secret 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 an 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.
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
  - Image encryption
  - Perceptual signature

I. Cox.
Digital Watermarking and Steganography.
Medical image protection (2D/3D): data hiding, selective encryption and secret sharing

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.
Remerciements
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))
Perceptual signatures: data integrity

Signature of a text

\[ M_1 = \text{“Aujourd’hui il fait beau dans le sud de la France, même si il y a un peu de vent...”}\]
\[ S_1 = \text{0x}2534A8C08E12F4A8 \]
\[ M_2 = \text{“Aujourd’hui il fait beau dans le sud de la France, même si il y a un peu de mistral...”}\]
\[ S_2 = \text{0x}3D68AB9310E38B51 \]

Signature of an image

Original image (760 kB) = Compressed image (224 kB)
a) Original image, b) histogram, c) encrypted image by scrambling, d) histogram of the encrypted image.
a) Original image, b) histogram, c) encrypted image with a stream cipher algorithm, d) histogram of the encrypted image.
Conclusion

Image encryption

\[ E_{K_e}(I_1) \]
\[ E_{K_e}(I_2) \]

\[ I_1 \]
\[ I_2 \]

\[ I_{1e} \]
\[ I_{2e} \]

XOR encryption.