Protection of Visual Data by Encryption and Watermarking

Image, video and 3D object

William PUECH

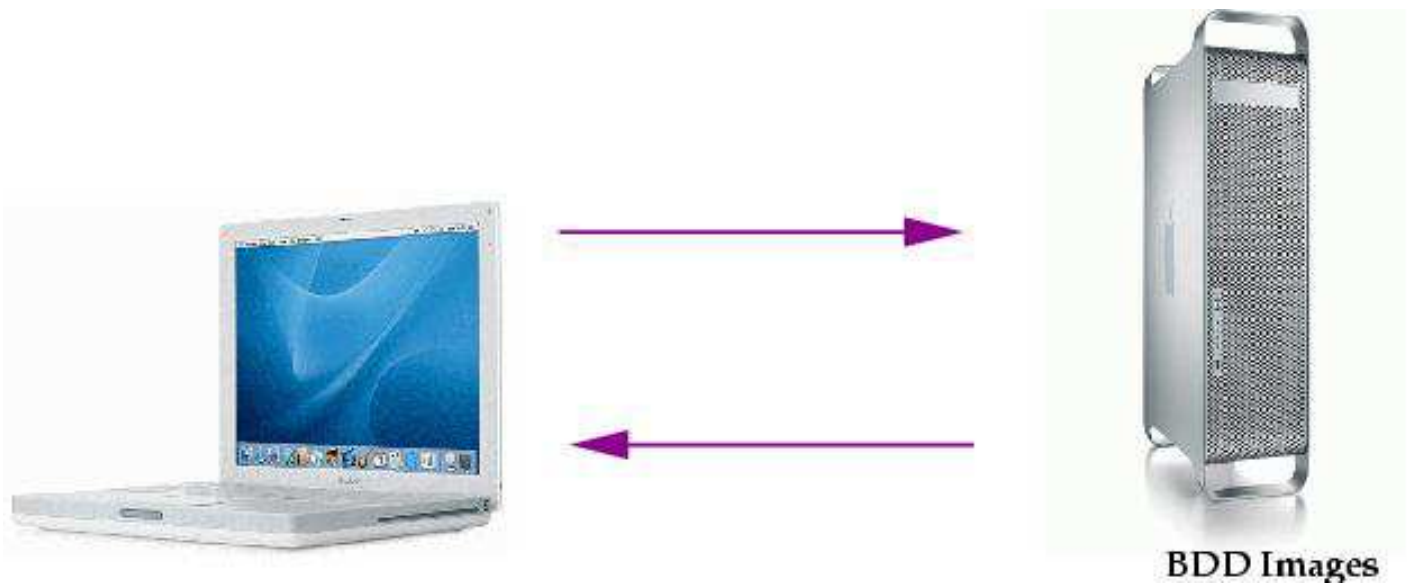
LIRMM
Laboratoire d'Informatique, de Robotique et de Microélectronique de Montpellier
UMR 5506 CNRS, University of Montpellier, France
ICAR Team (Image & Interaction)

Febuary, 19th of 2009

Outline

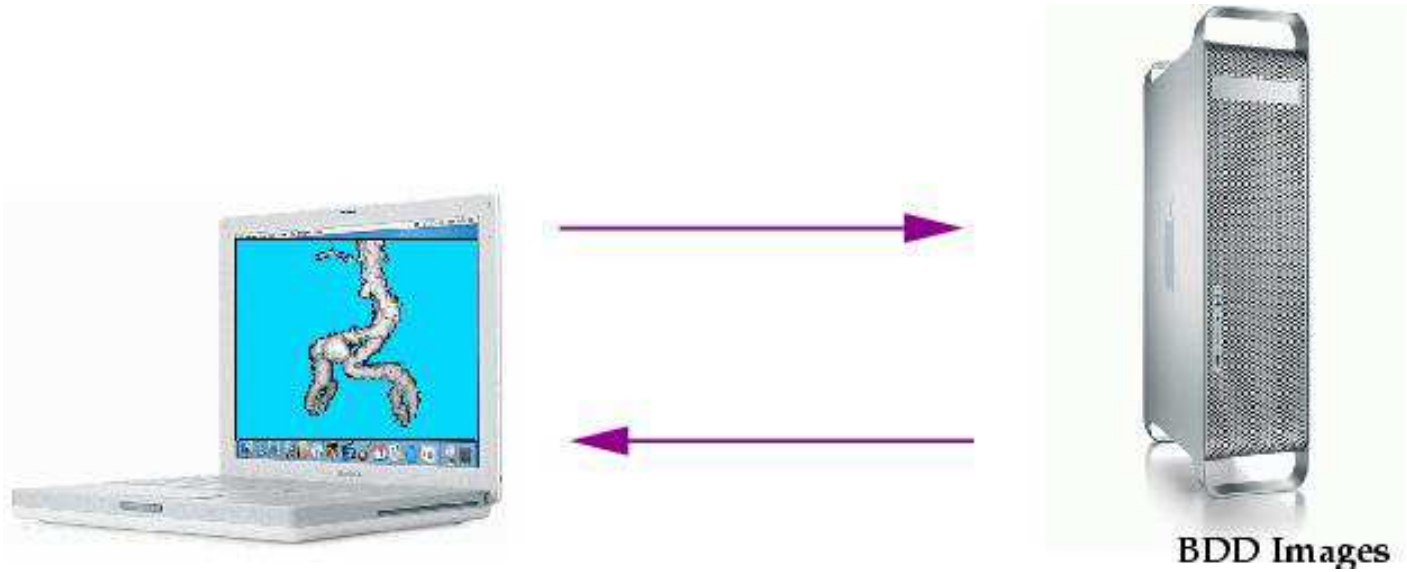
Outline

Safe Image Transfer: the problem



Safe transfer of images with high resolution.

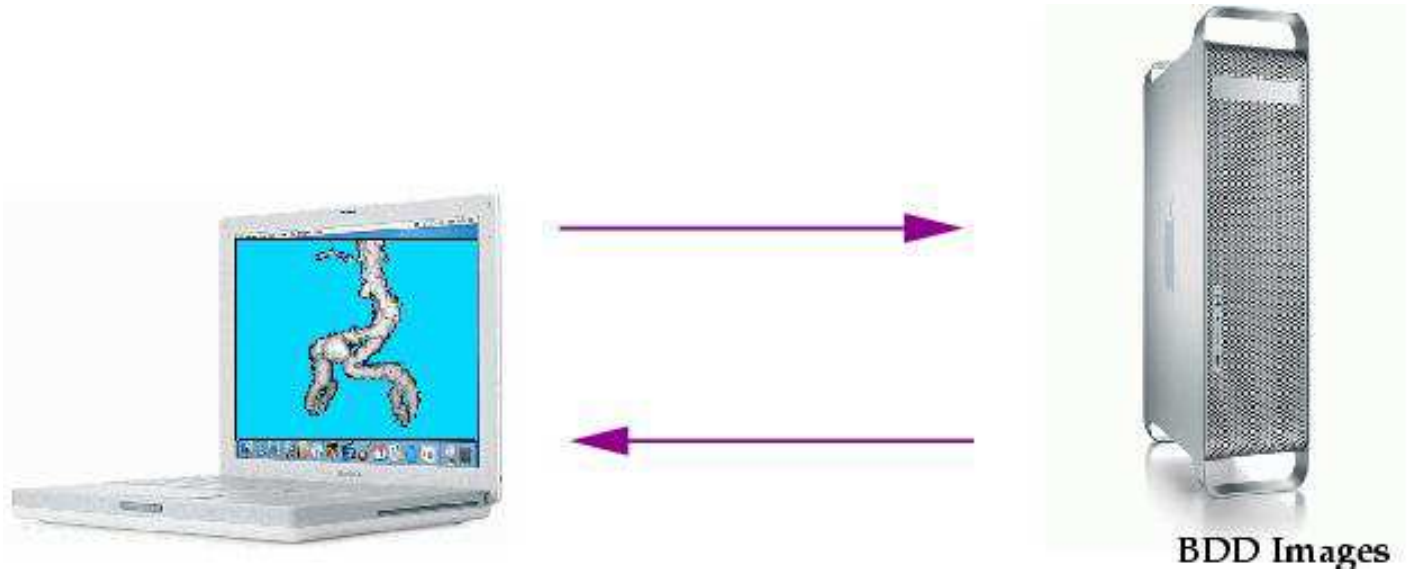
Safe Image Transfer: the problem



3D Visualization 3D on line.

▸ Example

Safe Image Transfer: the problem



3D Visualization 3D on line.

▸ Example

Safe Image Transfer: the problem

Safe Transfer and Visualisation on line in real time for low powered systems (wireless devices).

Safe Image Transfer: the objectives

- To Transfer Safe Images
  - To Have Confidential Image **during** and **after** Transfer
  - To Ensure the Integrity (perceptual) and the Authenticity of Image
  - To Hide associated data (high capacity) in Image
- To Access in different resolution levels of Image
- To Process in Real Time
- To Reduce the Image size.

Safe Image Transfer: the objectives

- To Transfer Safe Images
  - To Have Confidential Image **during** and **after** Transfer
  - To Ensure the Integrity (perceptual) and the Authenticity of Image
  - To Hide associated data (high capacity) in Image
- To Access in different resolution levels of Image
- To Process in Real Time
- To Reduce the Image size.

Safe Image Transfer: the objectives

- To Transfer Safe Images
  - To Have Confidential Image **during** and **after** Transfer
  - To Ensure the Integrity (perceptual) and the Authenticity of Image
  - To Hide associated data (high capacity) in Image
- To Access in different resolution levels of Image
- To Process in Real Time
- To Reduce the Image size.

Possible solution: image encryption

Image encryption for safe image transfer

- Robust to noise
- Compatible with a 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.

Possible solution: image encryption

Image encryption for safe image transfer

- Robust to noise
- Compatible with a 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.

Possible solution: image encryption

Image encryption for safe image transfer

- Robust to noise
- Compatible with a 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.

Possible solution: image encryption

Some Solutions:

- To adapt the encryption algorithms to images
- To develop new methods of encryption
- To combine encryption and watermarking with compression and to be robust to noise.

Possible solution: image encryption

Some Solutions:

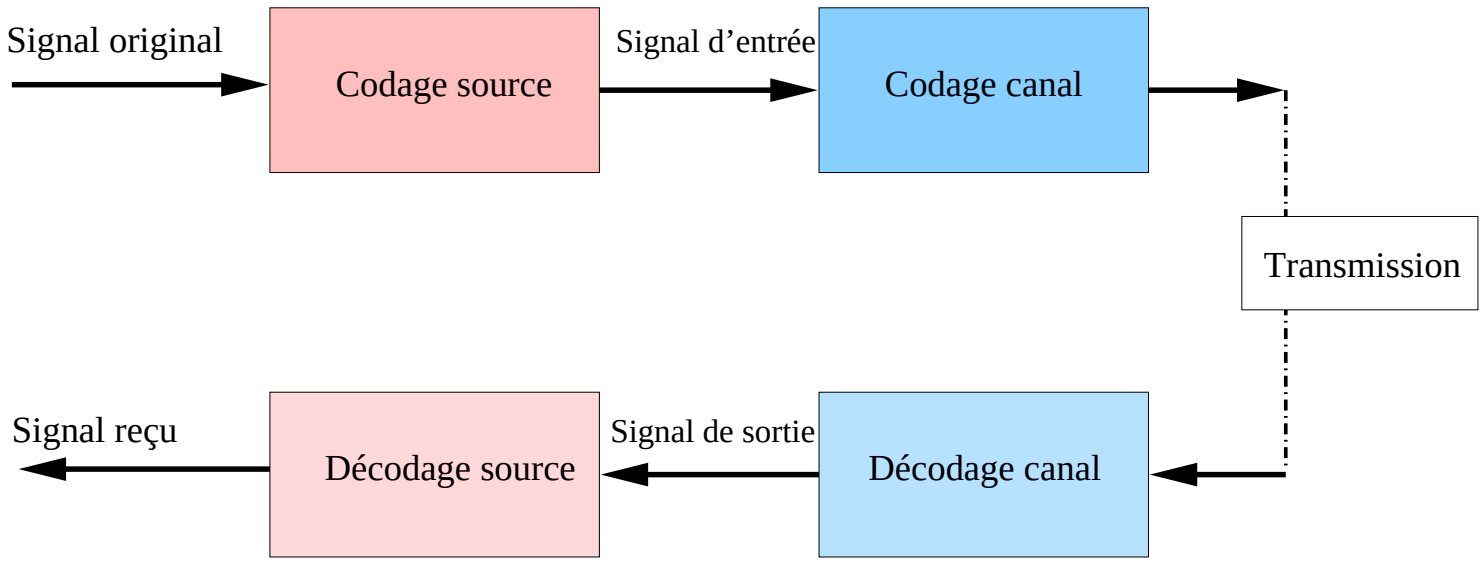
- To adapt the encryption algorithms to images
- To develop new methods of encryption
- To combine encryption and watermarking with compression and to be robust to noise.

Possible solution: image encryption

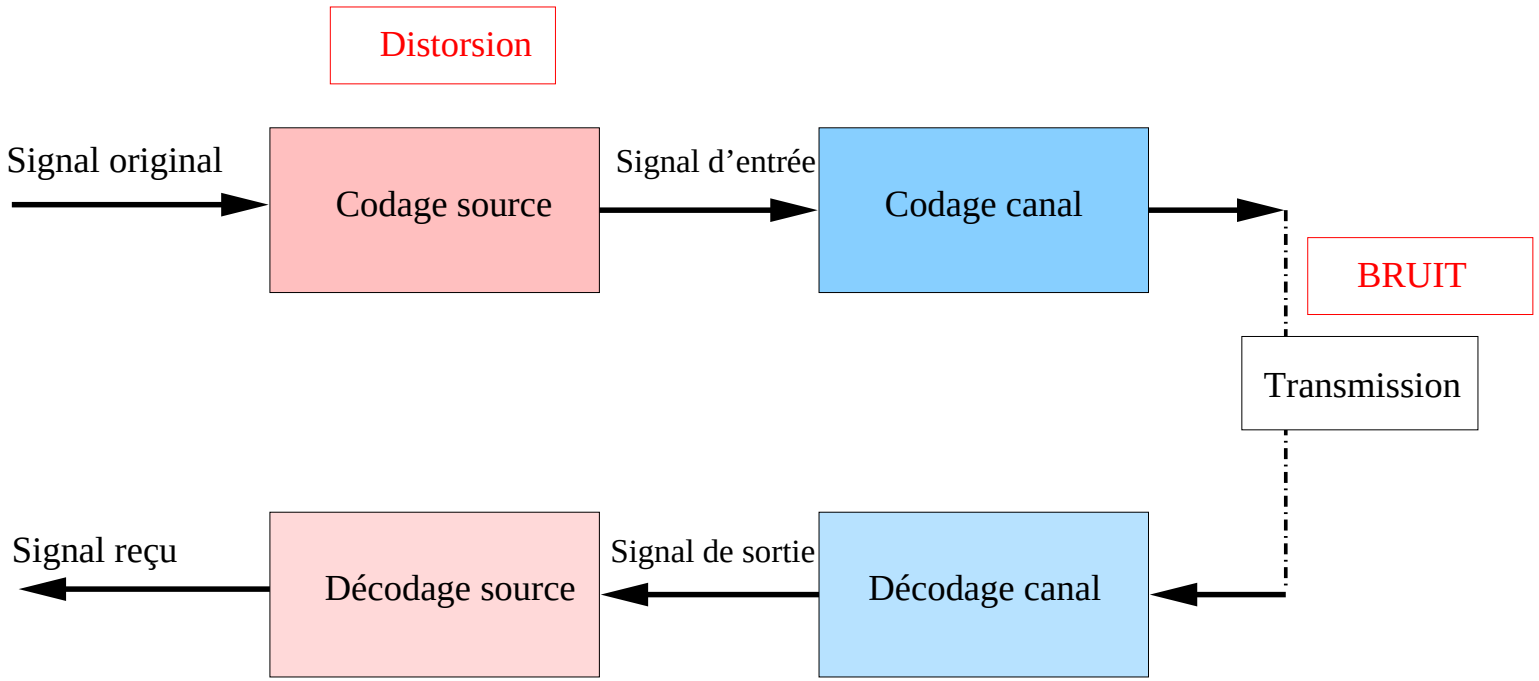
Some Solutions:

- To adapt the encryption algorithms to images
- To develop new methods of encryption
- To combine encryption and watermarking with compression and to be robust to noise.

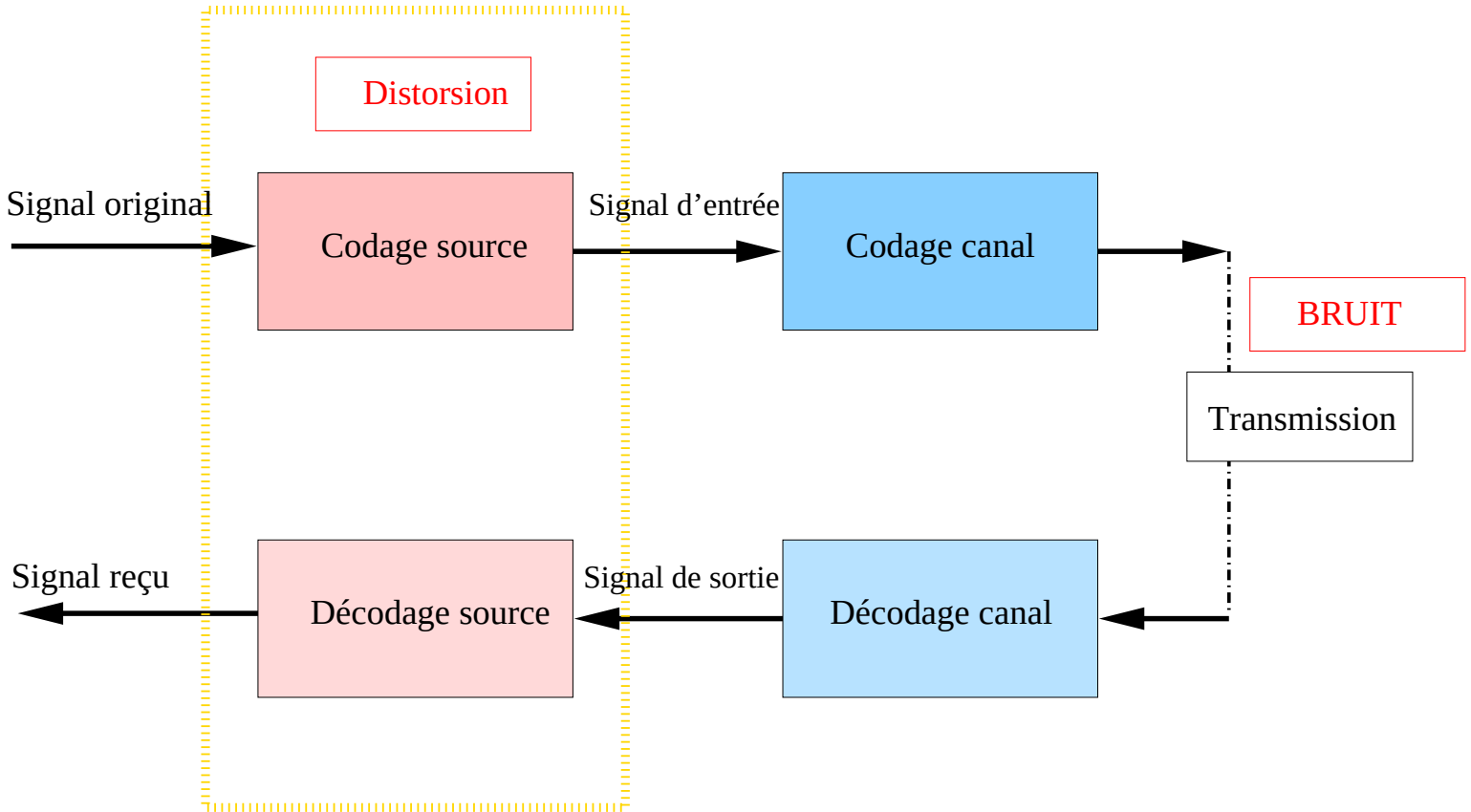
Context of the proposed solution



Context of the proposed solution



Context of the proposed solution



Outline

Data encryption

Data encryption

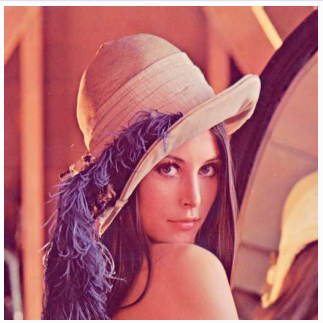
- The art to mask the data:
  - confidentiality : data protection
  - authenticity : emitter and receiver
  - integrity : ensure the totality and the content of the data
  - non repudiation : ACK

Perceptual signature: 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 visual data



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

Perceptual signature: 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 visual data

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

Watermarking

Watermarking and Data Hiding

- The art to embed message in perceptual data:
  - invisibility: statistically invisible
  - no removable: robust to transformations and attacks
  - payload: size of the hidden message
- Data hiding: large payload
- Steganography: invisibility
- Watermarking: robust to attacks

Watermarking

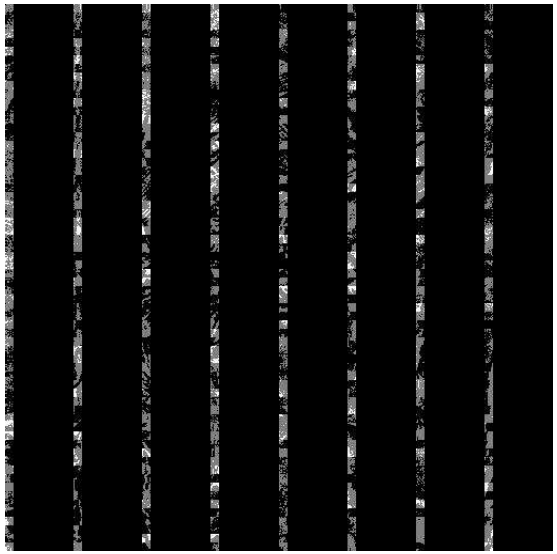
Watermarking and Data Hiding

- The art to embed message in perceptual data:
  - invisibility: statistically invisible
  - no removable: robust to transformations and attacks
  - payload: size of the hidden message
- Data hiding: large payload
- Steganography: invisibility
- Watermarking: robust to attacks

Previous work in the LIRMM: Safe Image Transfer

a)

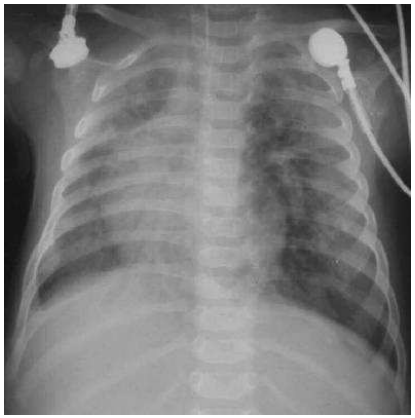
b)



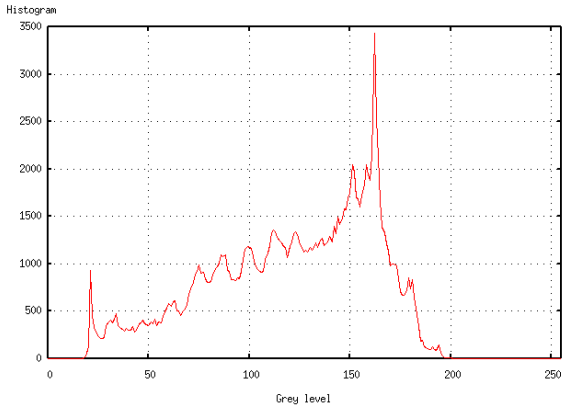
c)

a) Original image.
b) Embedded image with a message of 512 bits using the DCT based data hiding method.
c) Difference between (a) and (b).

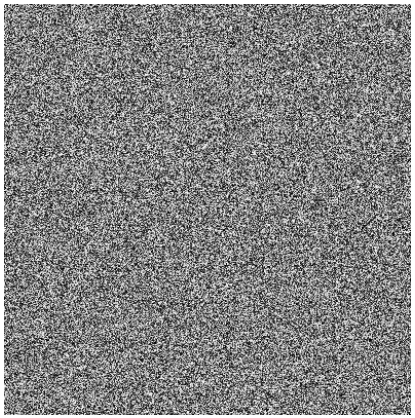
Previous work in the LIRMM: Safe Image Transfer



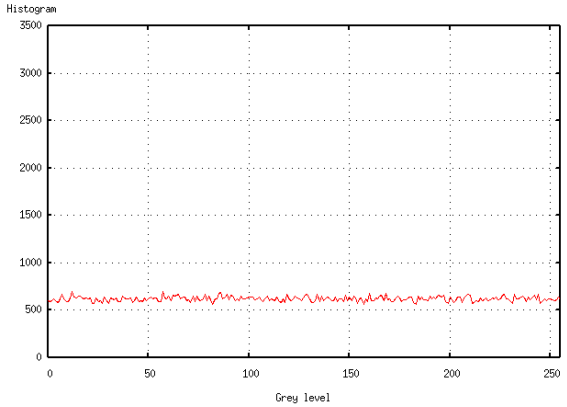
(a)



(b)



(c)



(d)

a) Original image, b) Original image histogram
c) Encrypted image with the stream cipher algorithm, with a key of 128 bits
d) Histogram of the image (c).

Previous work in the LIRMM: Safe Image Transfer

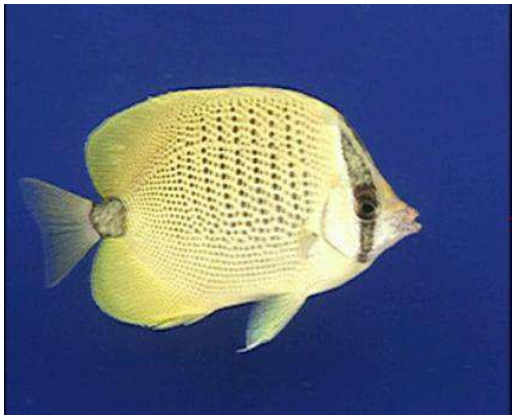
a)

b)

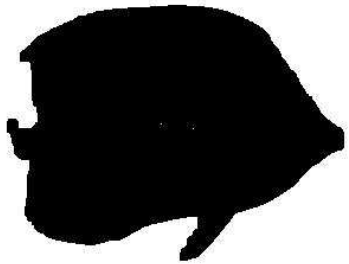
c)

ginal image.
nsfer of compressed Image with a Safe ROI.
construction of the High Resolution Definition of the ROI.

Previous work in the LIRMM: Safe Image Transfer

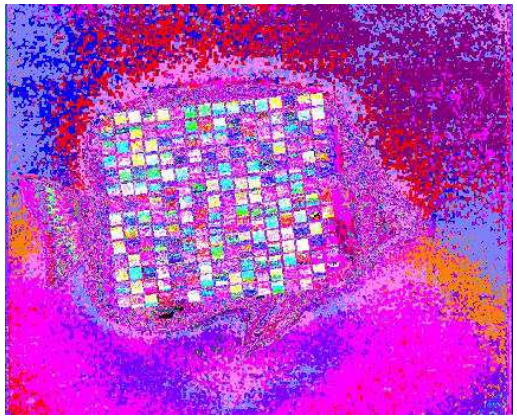


(a)



(b)

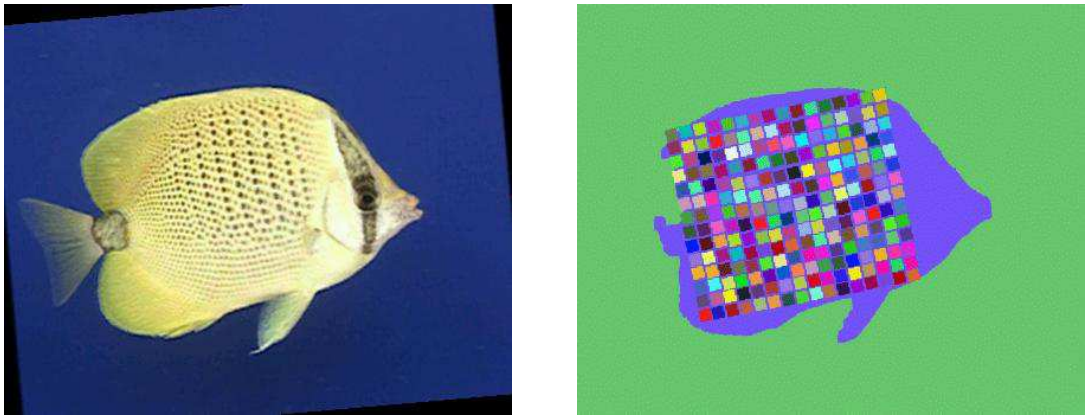
(c)



(d)

a) The original image, b) The associated binary mask, c) Color watermarked image, d) Difference between original color image and color watermarked image.

Previous work in the LIRMM: Safe Image Transfer



(a) (b)

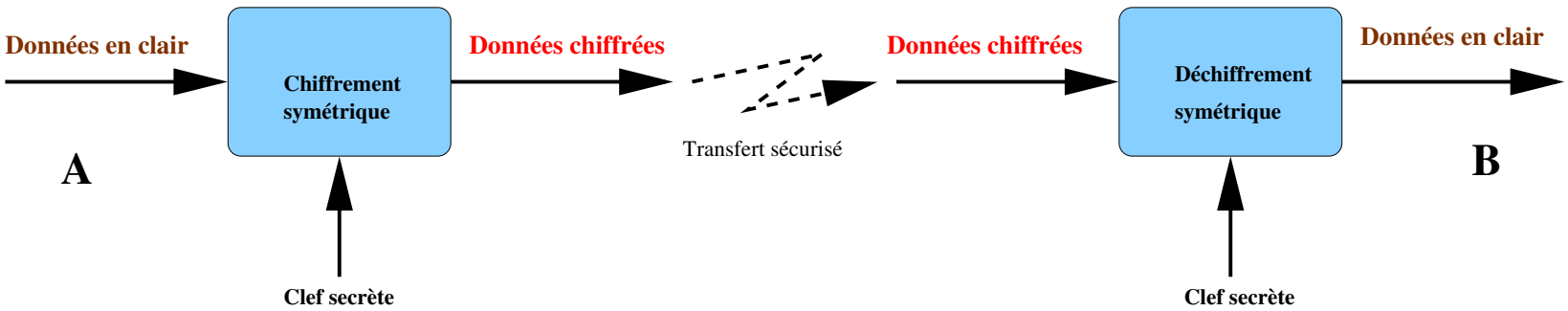
a) 5 degree rotation of color watermarked image "Fish", b) The label of fish color image with watermarked blocks.

Outline

Outline

Standard approaches to encrypt data [SCH 95]

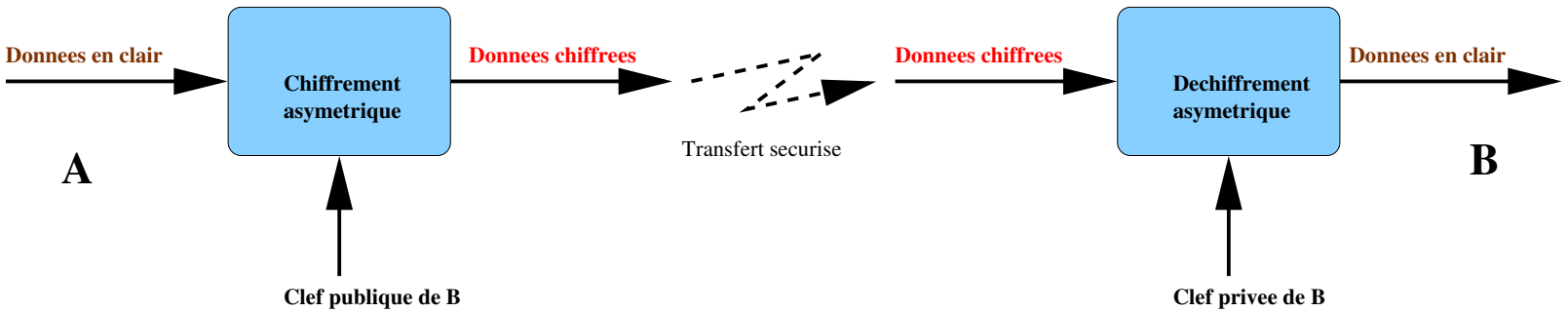
- Symmetric encryption: secret key: DES and AES
  - Transfer of the key by using another canal of transmission
- Asymmetric encryption: public key and a private key: RSA



B. Schneier.
Applied cryptography.
Wiley, 1995.

Standard approaches to encrypt data [SCH 95]

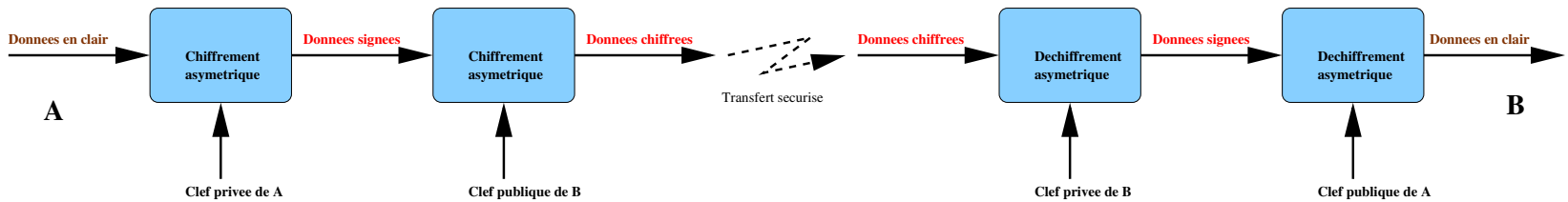
- Symmetric encryption: secret key: DES and AES
  - Transfer of the key by using another canal of transmission
- Asymmetric encryption: public key and a private key: RSA



B. Schneier.
Applied cryptography.
Wiley, 1995.

Standard approaches to encrypt data [SCH 95]

- Symmetric encryption: secret key: DES and AES
  - Transfer of the key by using another canal of transmission
- Asymmetric encryption: public key and a private key: RSA



B. Schneier.
Applied cryptography.
Wiley, 1995.

Standard approaches to encrypt data [SCH 95]

- Symmetric encryption: secret key: DES and AES
  - Transfer of the key by using another canal of transmission
- Asymmetric encryption: public key and a private key: RSA

- Block encryption:
  - The size of the blocks is static
  - The size is big: between 128 and 256 bits
- Stream cipher:
  - Variable length coding
  - The size is relatively small: 1 bit or 1 byte

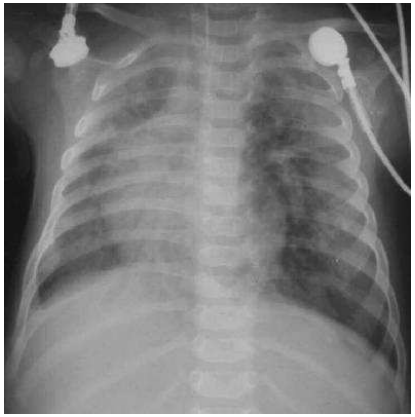
Standard approaches to encrypt data [SCH 95]

- Symmetric encryption: secret key: DES and AES
  - Transfer of the key by using another canal of transmission
- Asymmetric encryption: public key and a private key: RSA

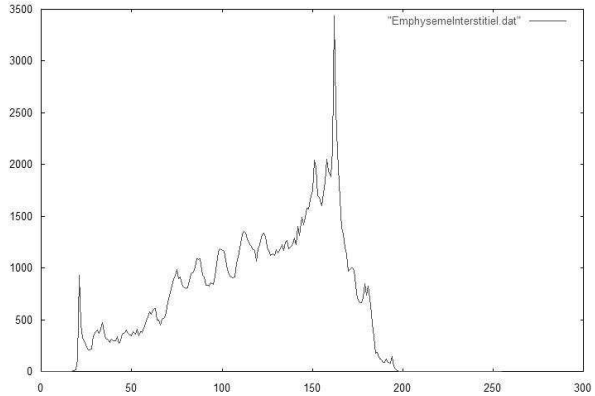
- Block encryption:
  - The size of the blocks is static
  - The size is big: between 128 and 256 bits
- Stream cipher:
  - Variable length coding
  - The size is relatively small: 1 bit or 1 byte

Outline

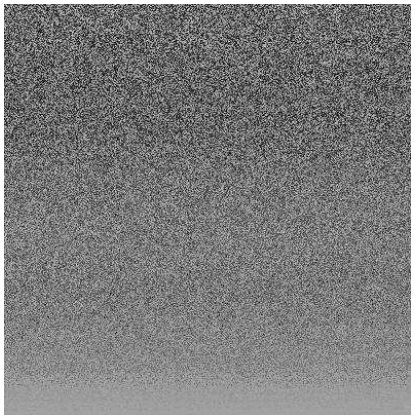
Method based on scrambling



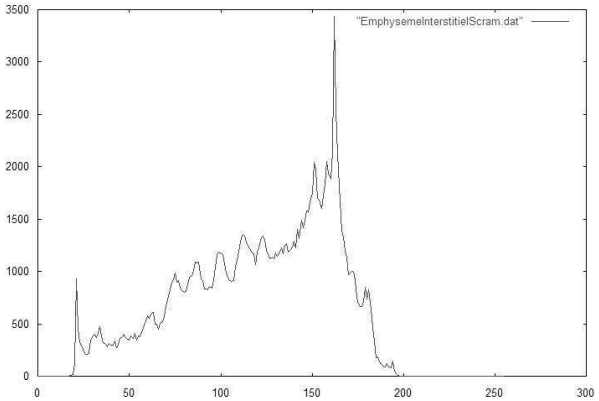
(a)



(b)



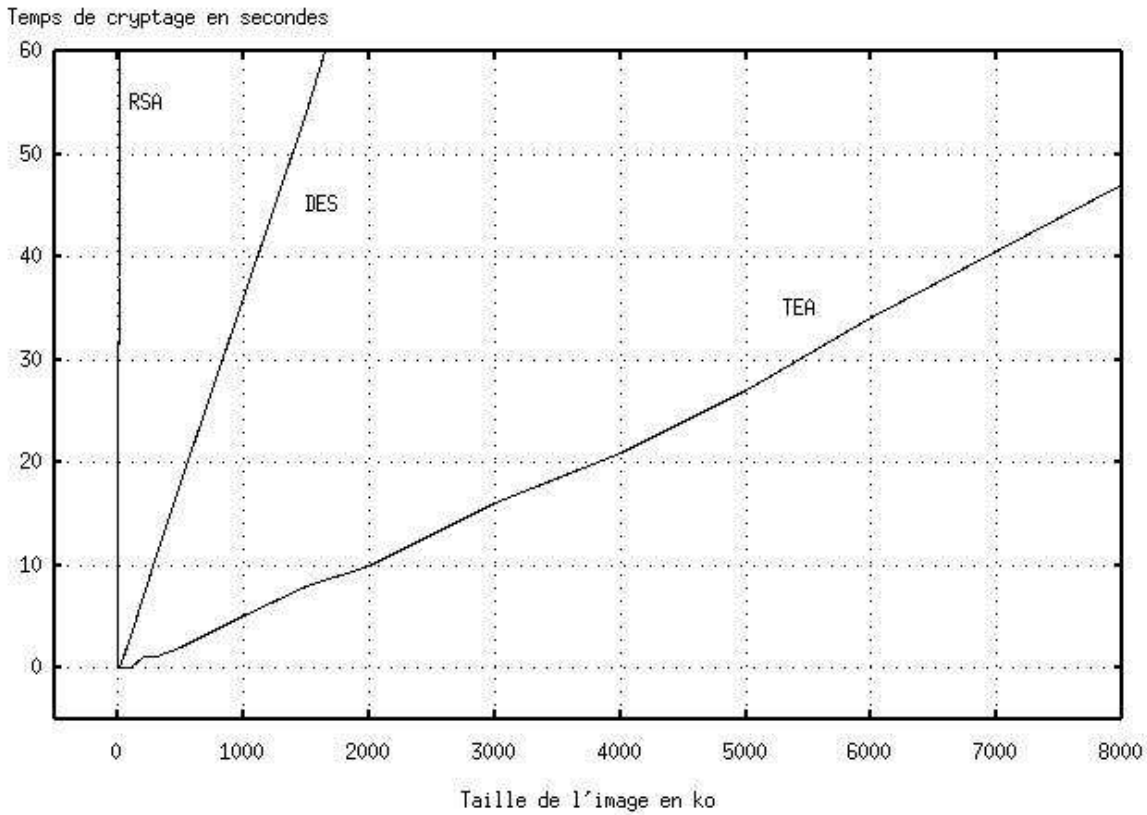
(c)



(d)

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

Asymmetric encryption (RSA)



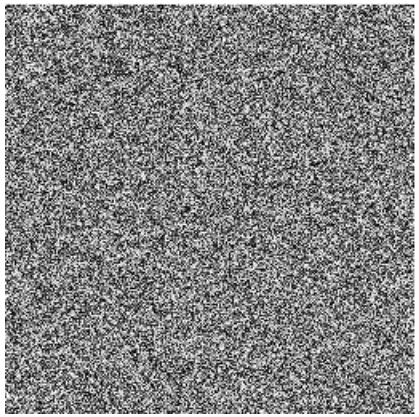
Encryption time for RSA compared to symmetric encryption.

J.C. Borie, W. Puech and M. Dumas.

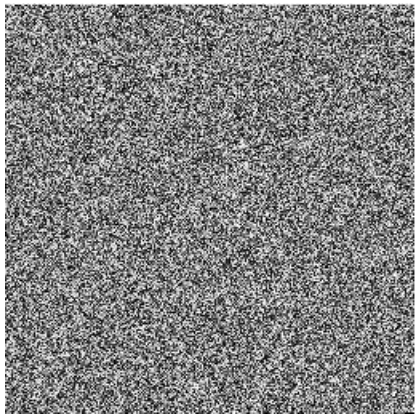
Encrypted Images for Secure Transfer with RSA Algorithm.
IEEE Communication 2002, Bucharest, Romania, 2002.

Symmetric encryption by block (DES, TEA, AES)

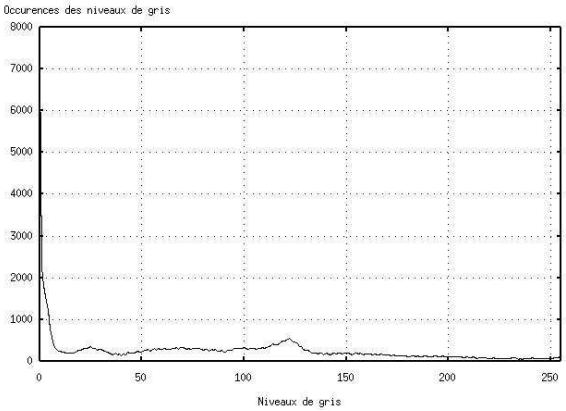
Original image

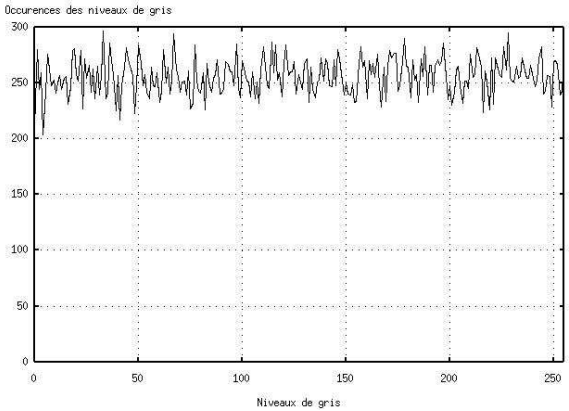


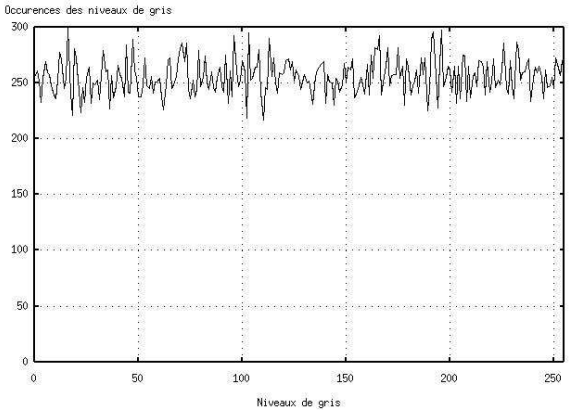
Encrypted Image with DES or AES



Encrypted Image with TEA



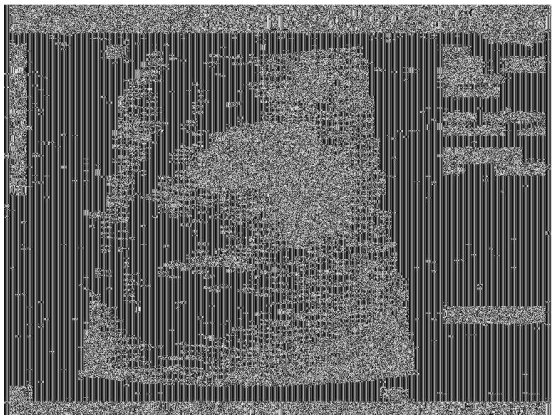




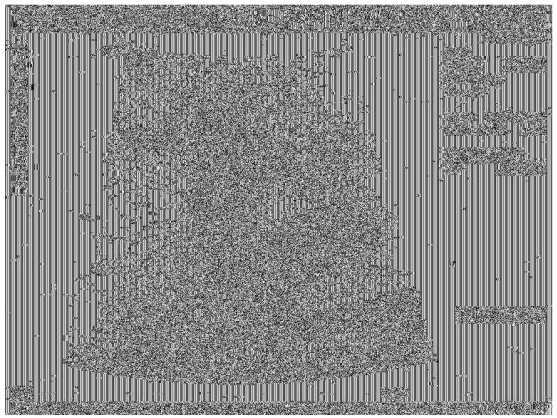
Histograms

Symmetric block encryption (DES, TEA, AES)

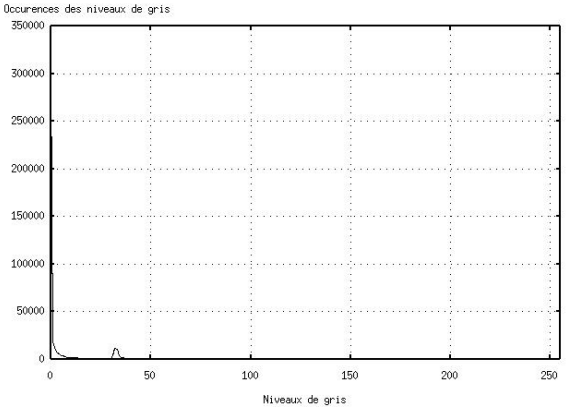
Original Image

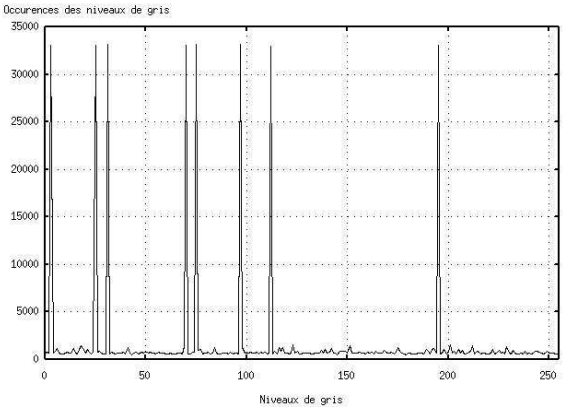


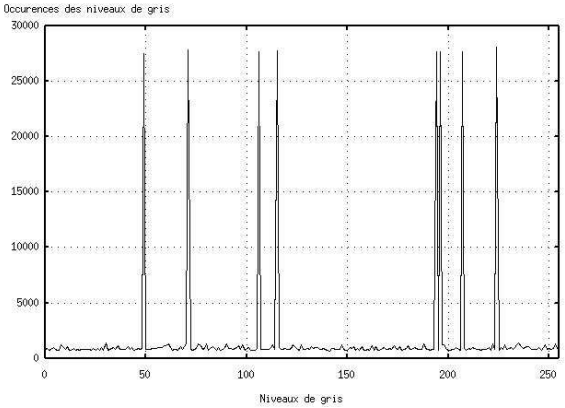
Encrypted Image with DES or AES



Encrypted Image with TEA

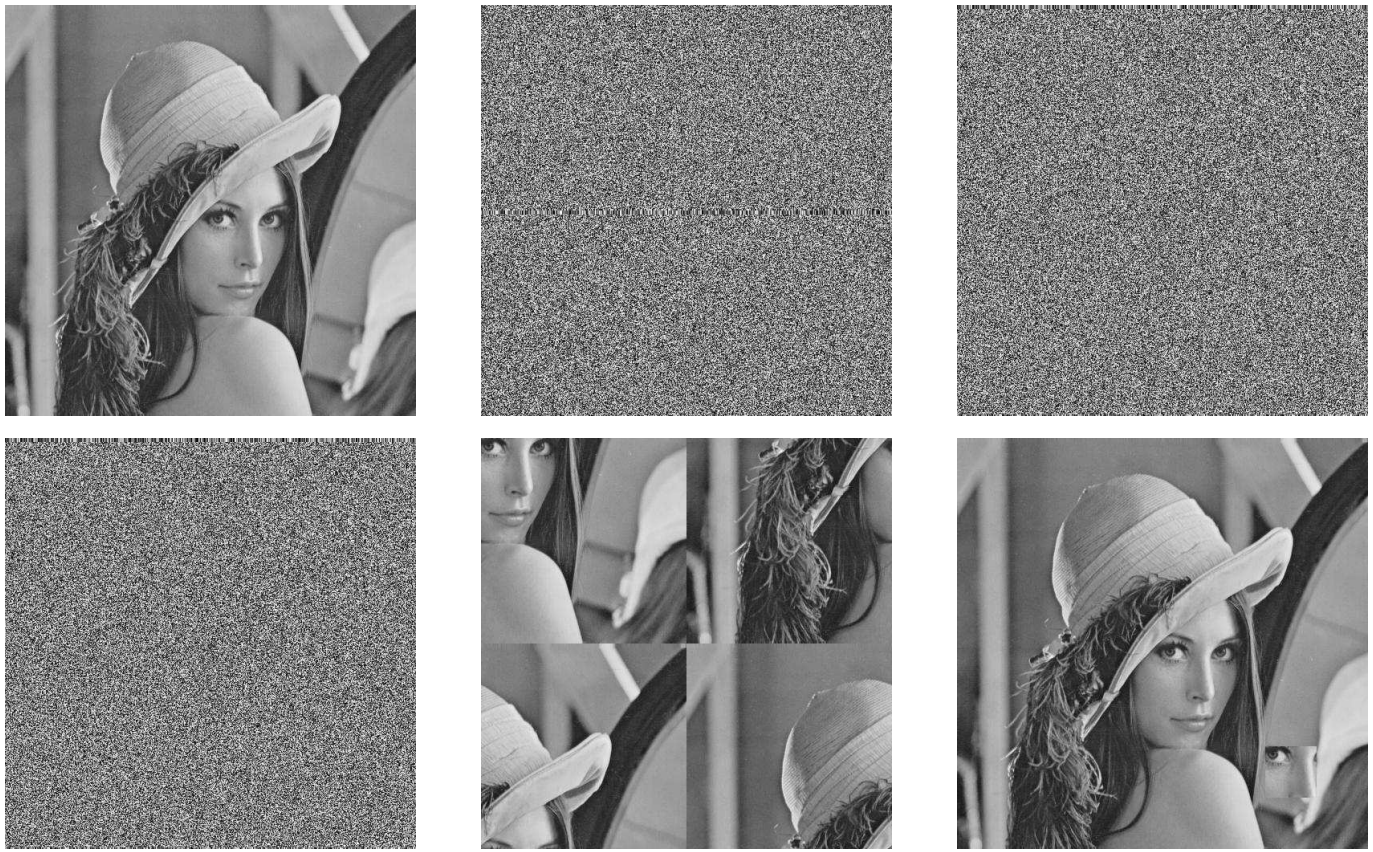






Histograms

Data integrity



"Permutation" and "cut and copy".

Stream cipher

- Encryption for each bit or for each byte
- Very fast
- Dynamic encryption for each symbol of the original message
- Need of memory
- Two steps
  - To generate a Keystream (dynamic key)
  - Encryption of the output function of the keystream

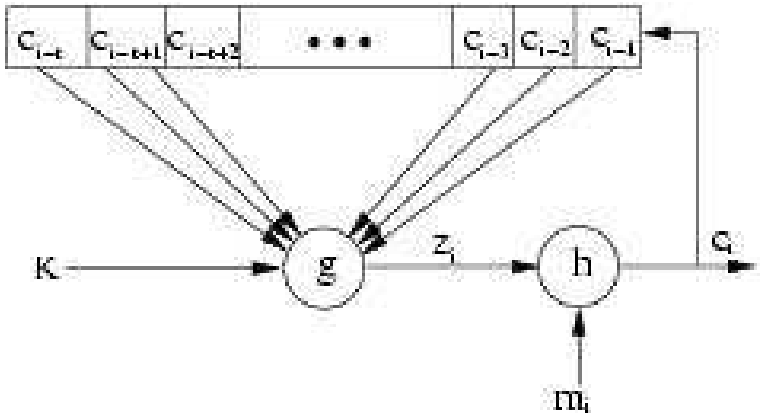
- Synchronous : if the keystream does not depend to the cleartext and the ciphertext
- Asynchronous : if the key is based on some previous ciphertext

Stream cipher

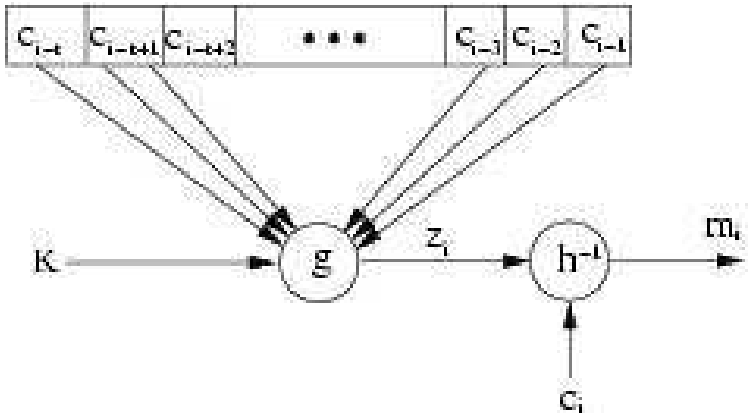
- Encryption for each bit or for each byte
- Very fast
- Dynamic encryption for each symbol of the original message
- Need of memory
- Two steps
  - To generate a Keystream (dynamic key)
  - Encryption of the output function of the keystream

- Synchronous : if the keystream does not depend to the cleartext and the ciphertext
- Asynchronous : if the key is based on some previous ciphertext

Asynchronous stream cipher



a) Asynchronous stream cipher,



b) Decryption.

Calculus of z_i and c_i from m_i and K :

$$\begin{cases} z_i &= g(K, c_{i-t}, c_{i-t+1}, \ldots, c_{i-2}, c_{i-1}) \\ c_i &= h(z_i, m_i), \end{cases}$$

where K is the secret key, $g()$ the function to generate the keystream and $h()$

Outline

Outline

Asynchronous stream cipher for image encryption

- K: key of length k bits b_i ($K = b_1 b_2 ... b_k$).
- Encryption unit: the pixel (1 byte).
- For each pixel p_i of the original image, the encryption (p'_i) depends of the current original pixel, of the secret key K, and of the $k/2$ previously encrypted pixels ($k/2 = t$).

$$\begin{cases} z_i & = & (\sum_{j=1}^{k/2} \alpha_j p'_{i-j}) mod\ 256 \\ p'_i & = & (z_i + p_i) mod\ 256, \end{cases}$$

with $i \in [0, \ldots, N-1]$, where N is the number of pixel of the image, k is the length of the key, $k \in [1, N]$, and α_j is a sequence of $k/2$ coefficients generated from the secret key K.

Asynchronous stream cipher for image encryption

Coefficients α_j: initialization vector (*VI*)

The coefficients α_j : integers between -2 $+2$ such as:

$$\begin{cases} \alpha_j = \beta_j - 1 & \text{si } \beta_j \in \{0, 1, 2\}, \\ \alpha_j = \pm 2 & \text{si } \beta_j = 3, \end{cases}$$

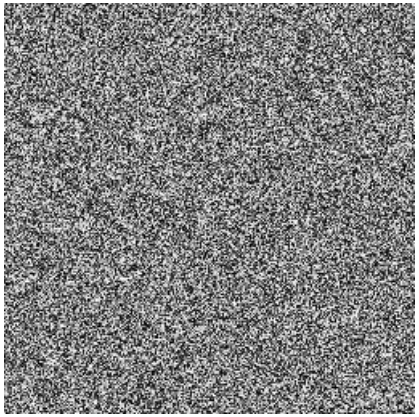
with $\beta_j = 2b_{2j-1} + b_{2j}$, where b_{2j-1} and b_{2j} two neighbouring bits of the secret key K.

The sign before 2 depends of the sum of the coefficients α_j in order to:

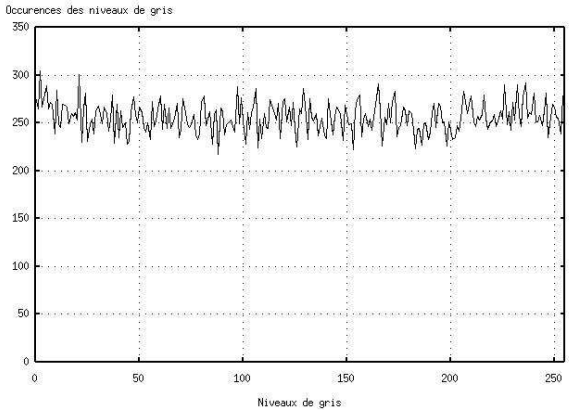
$$\frac{1}{k/2} \sum_{j=1}^{k/2} \alpha_j \simeq 0.$$

Asynchronous stream cipher for image encryption

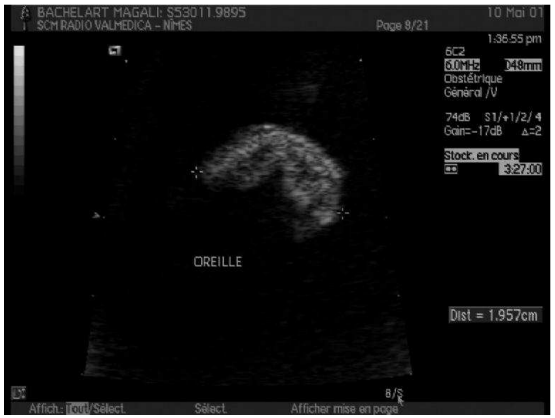
Original Image



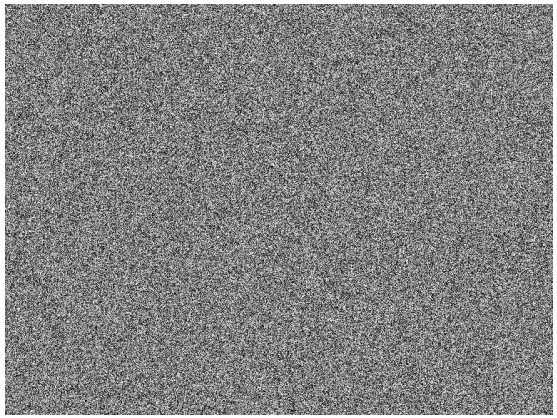
Encrypted Image



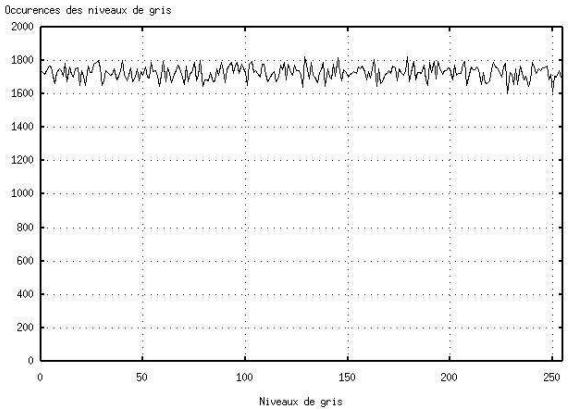
Histogram of the encrypted image



Medical Image

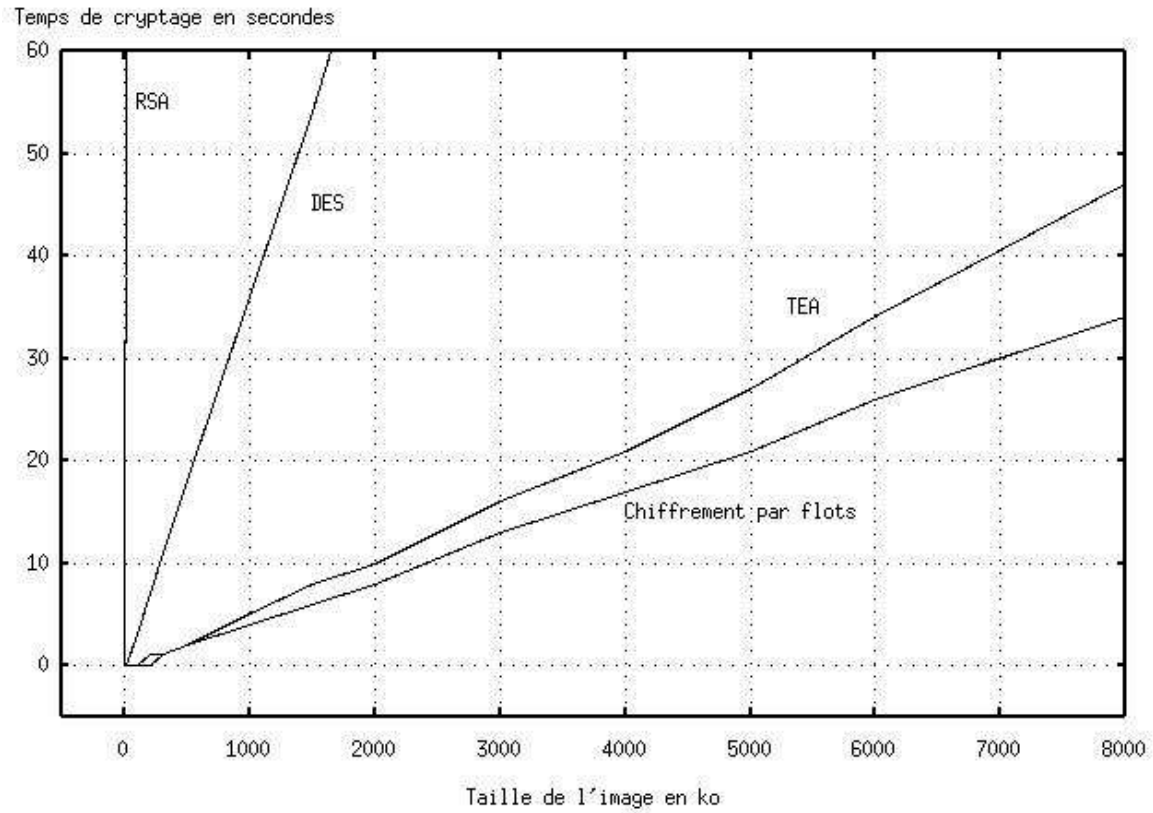


Encrypted Image



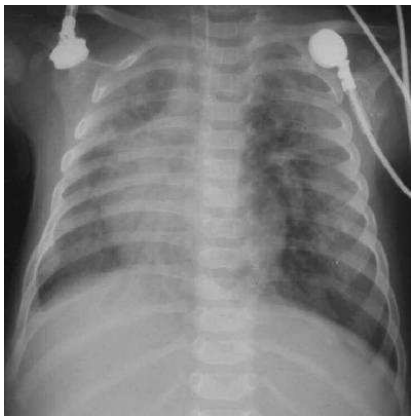
Histogram of the encrypted image

Asynchronous stream cipher for image encryption



Encryption time for the proposed stream cipher.

Asynchronous stream cipher for image encryption



Original Image

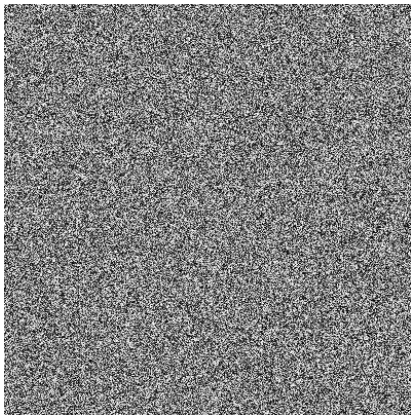
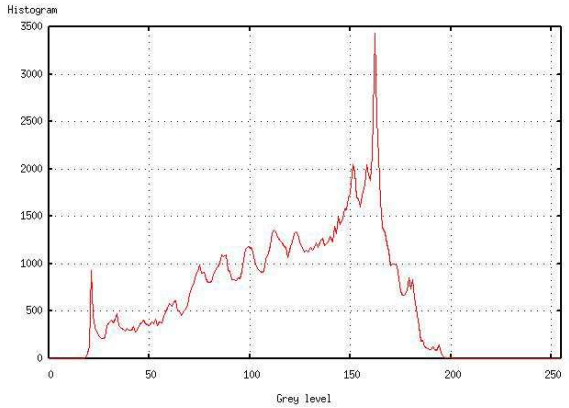
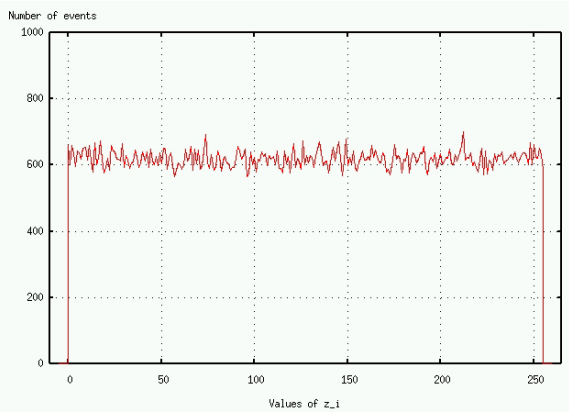


Image of the keystreams

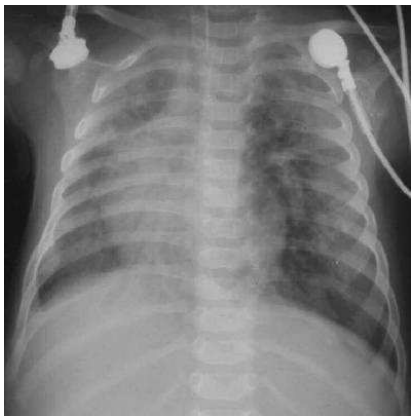


Histogram of the original image.

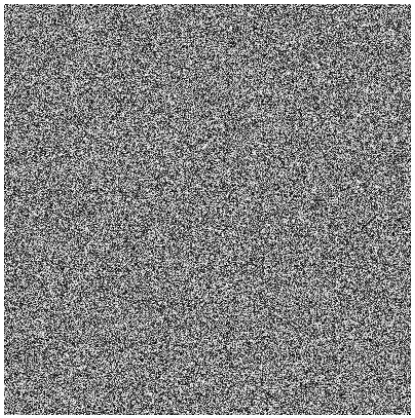


Histogram of the keystreams.

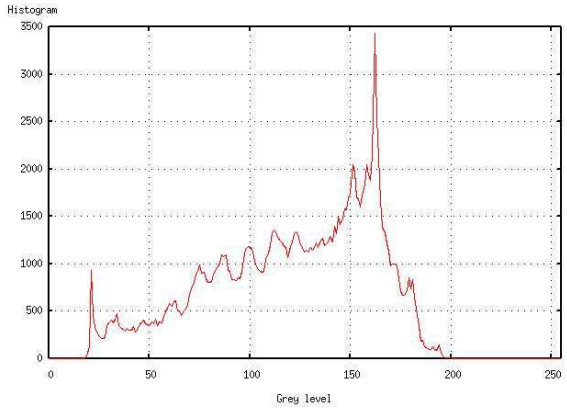
Asynchronous stream cipher for image encryption



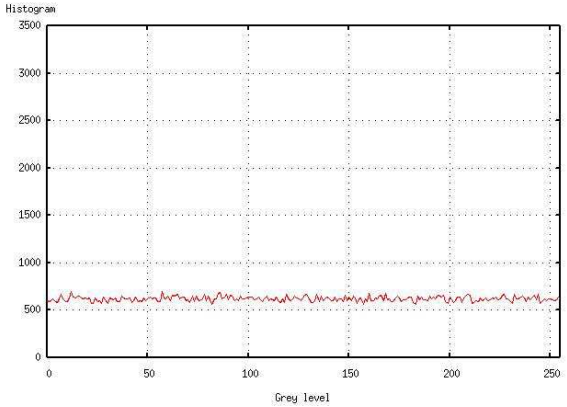
Original Image



Encrypted Image, $k = 128$ bits

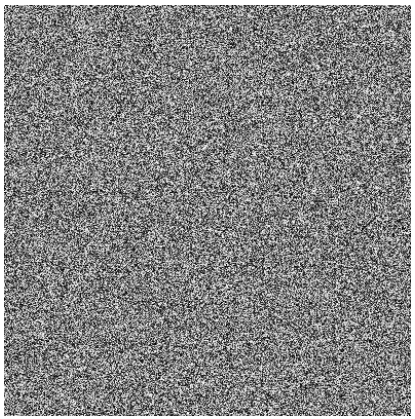


Histogram of the original image.

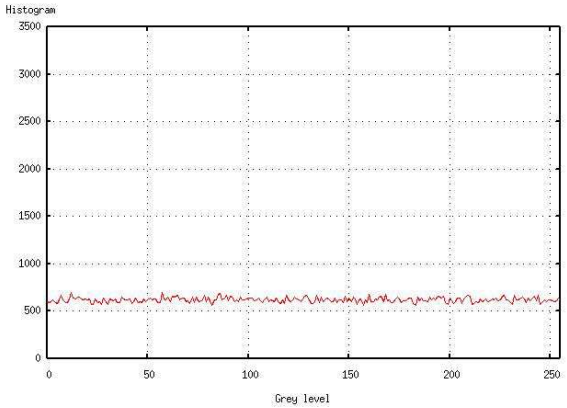


Histogram of the encrypted image.

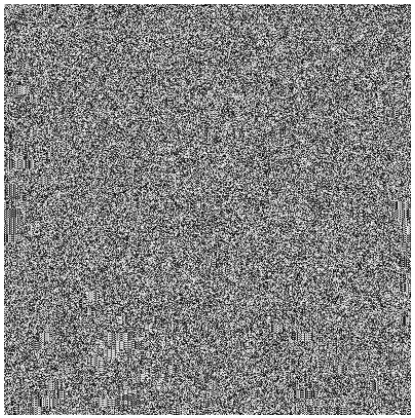
Asynchronous stream cipher for image encryption



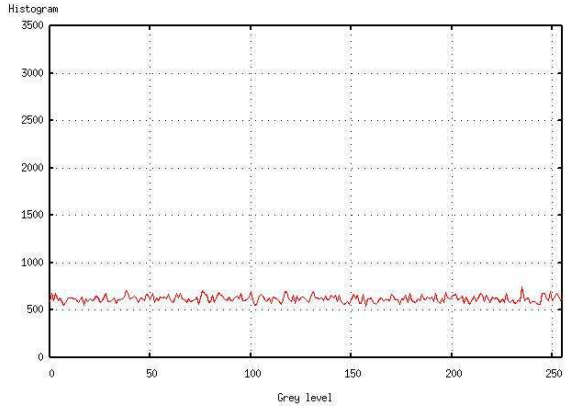
Encrypted Image, $k = 128$ bits



Histogram of the encrypted image.

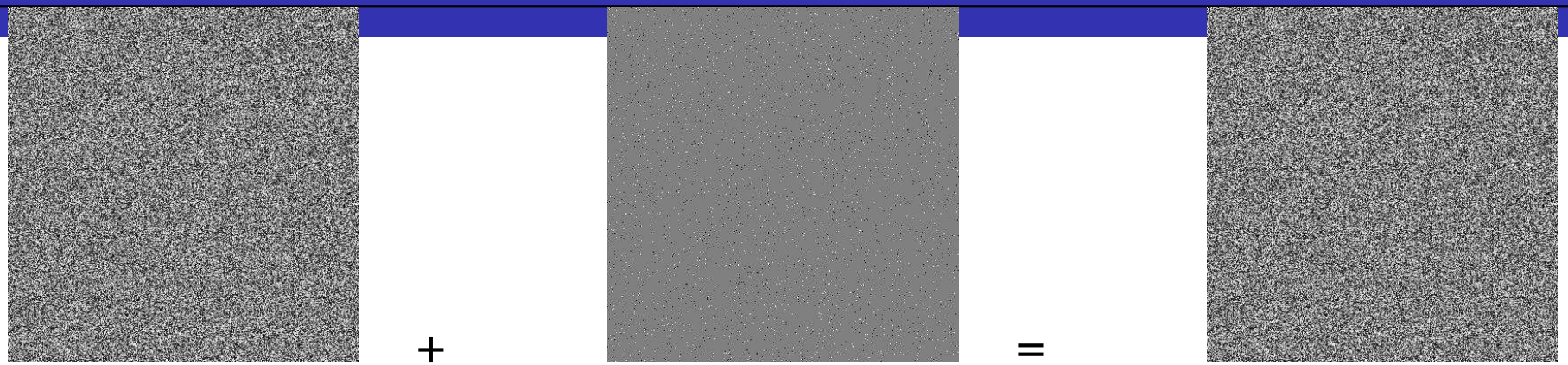


Encrypted Image with AES $k = 128$ bits

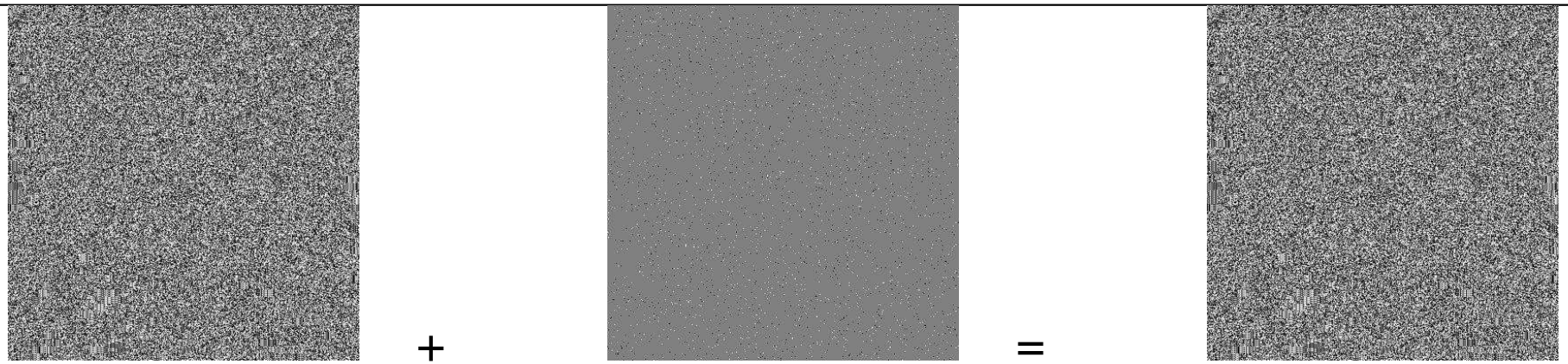


Histogram of the encrypted image.

Robustness to noise (BER =1.95 10^{-3})



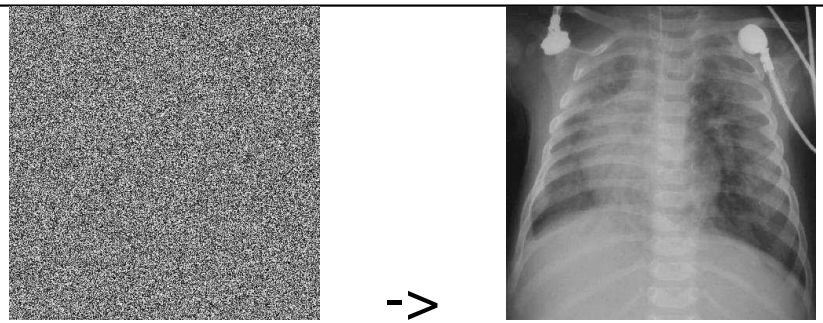
Stream cipher, $k = 128$ bits, $PSNR = 66.15$ dB



Encryption with AES, $k = 128$ bits, $PSNR = 66.15$ dB

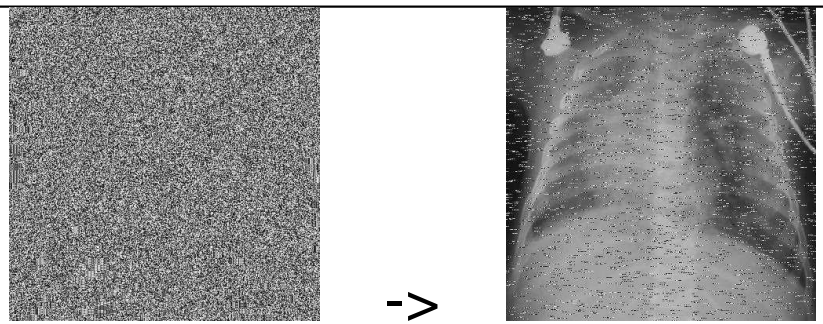
W. Puech and J.M. Rodrigues.
A New Crypto-Watermarking Method for Medical Images Safe Transfer.
EUSIPCO'04, Vienna, Austria, 2004.

Robustness to noise (BER =1.95 10^{-3})



-> $PSNR = 48.13\ dB$

Stream cipher $k = 128$ bits : decryption



-> $PSNR = 25.71\ dB$

Encryption with AES $k = 128$ bits : decryption

W. Puech and J.M. Rodrigues.
A New Crypto-Watermarking Method for Medical Images Safe Transfer.
EUSIPCO'04, Vienna, Austria, 2004.

Security level analysis

The entropy $H(S)$:

$$H(S) = -\sum_{j=0}^{M-1} P(\alpha_j) log_2(P(\alpha_j)). \quad (1)$$

Information redundancy r:

$$r = b - H(S), \quad (2)$$

The order-n entropy $H(S')$:

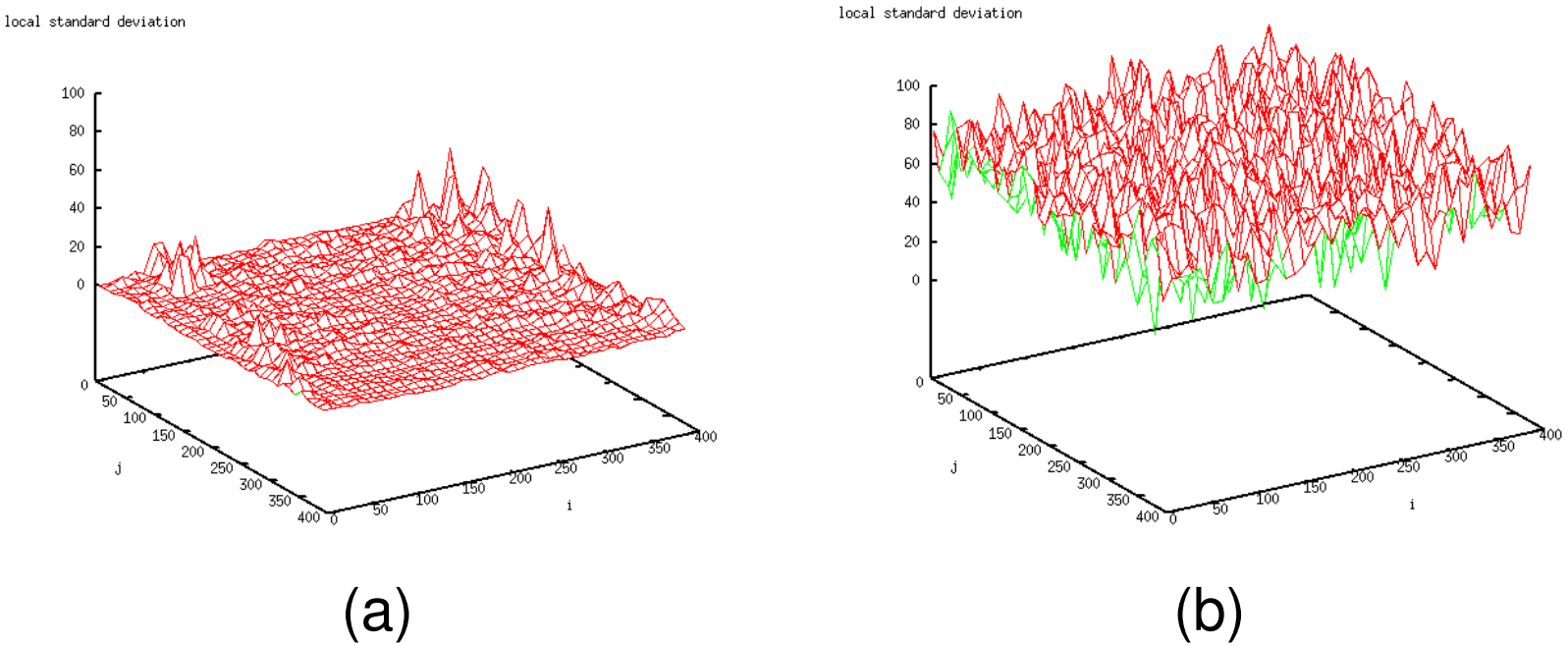
$$H(S') = H(S^n) = -\sum_{j=0}^{M^n-1} P(\beta_j) log_2(P(\beta_j)). \quad (3)$$

Security level analysis

The local standard deviation σ:

$$\sigma = \sqrt{\frac{1}{m}\sum_{i=1}^{m}(p_i - \overline{p_i})^2}, \tag{4}$$

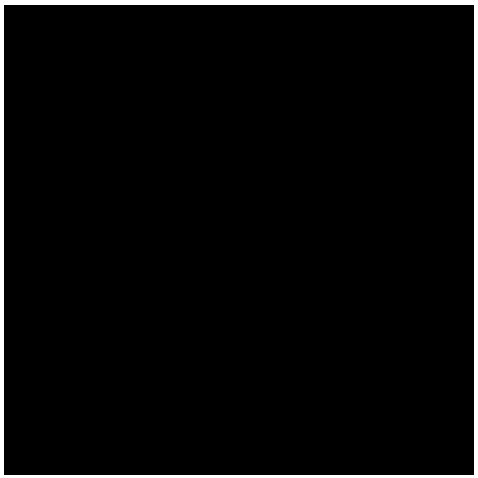
Security level analysis



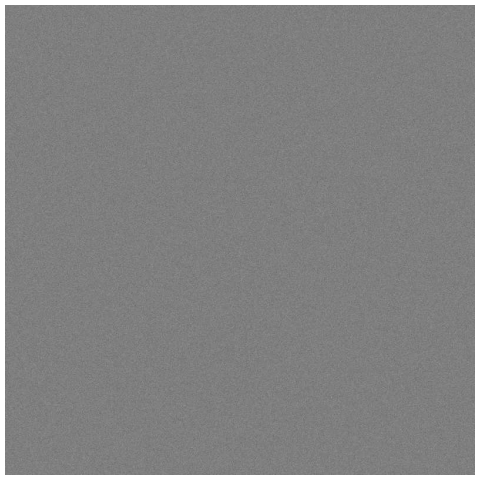
(a) (b)

Figure: Local standard deviation: a) Original medical image, b) Encrypted image.

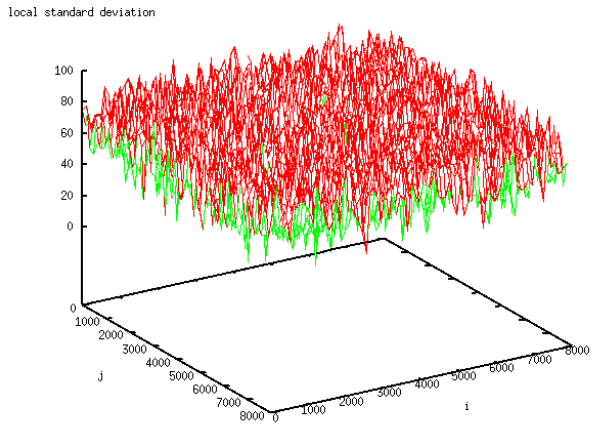
Security level analysis



(a)



(b)



(c)

Figure: a) Original black image, b) Encrypted image with the proposed asynchronous stream cipher algorithm for $k = 128$ bits, c) Local standard deviation of the encrypted image.

Security level analysis

Average value results of the entropy for 100 various images. We can remark, from the standard deviations in this table, that the variations are very small.

H1 (bit/pixel)	σ	H2 (bits/block)	σ	H3 (bits/block)	σ
8.000	0.000	15.999	0.000	23.770	0.072

Table: Mean value and standard deviation for the entropies of 100 encrypted images.

Outline

keywords

- Selective encryption,
- Partial encryption,
- JPEG compression,
- Huffman coding,
- AES algorithm,
- Stream cipher mode,
- Variable Length Coding,
- Privacy protection.

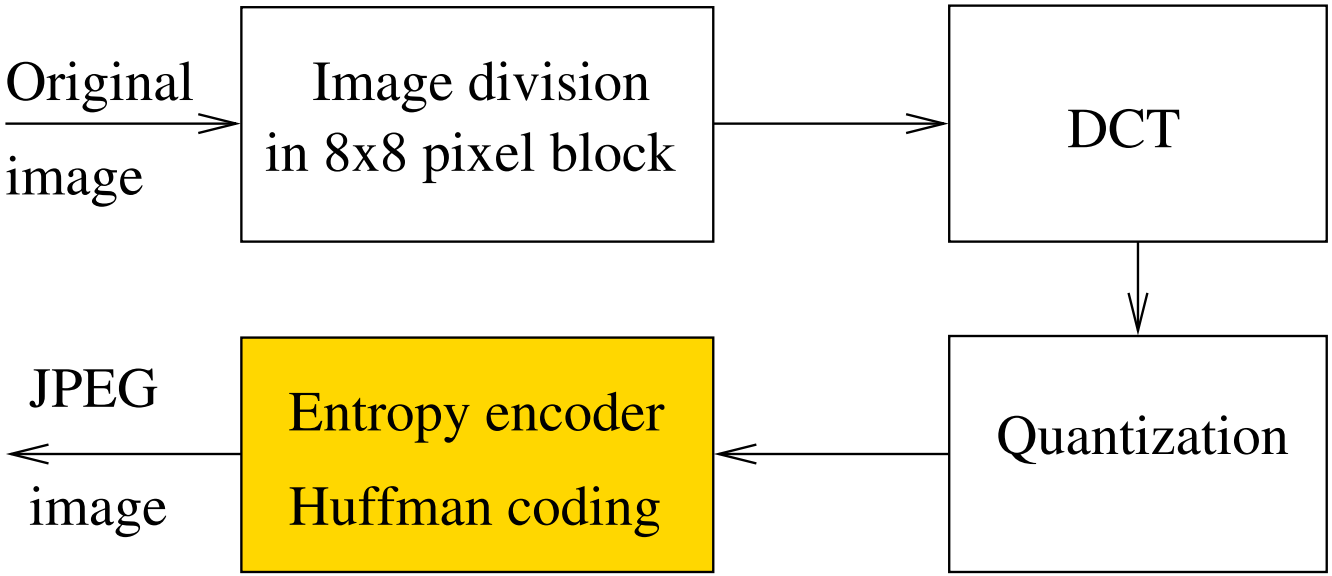


Figure: JPEG algorithm.

Global overview of the proposed method

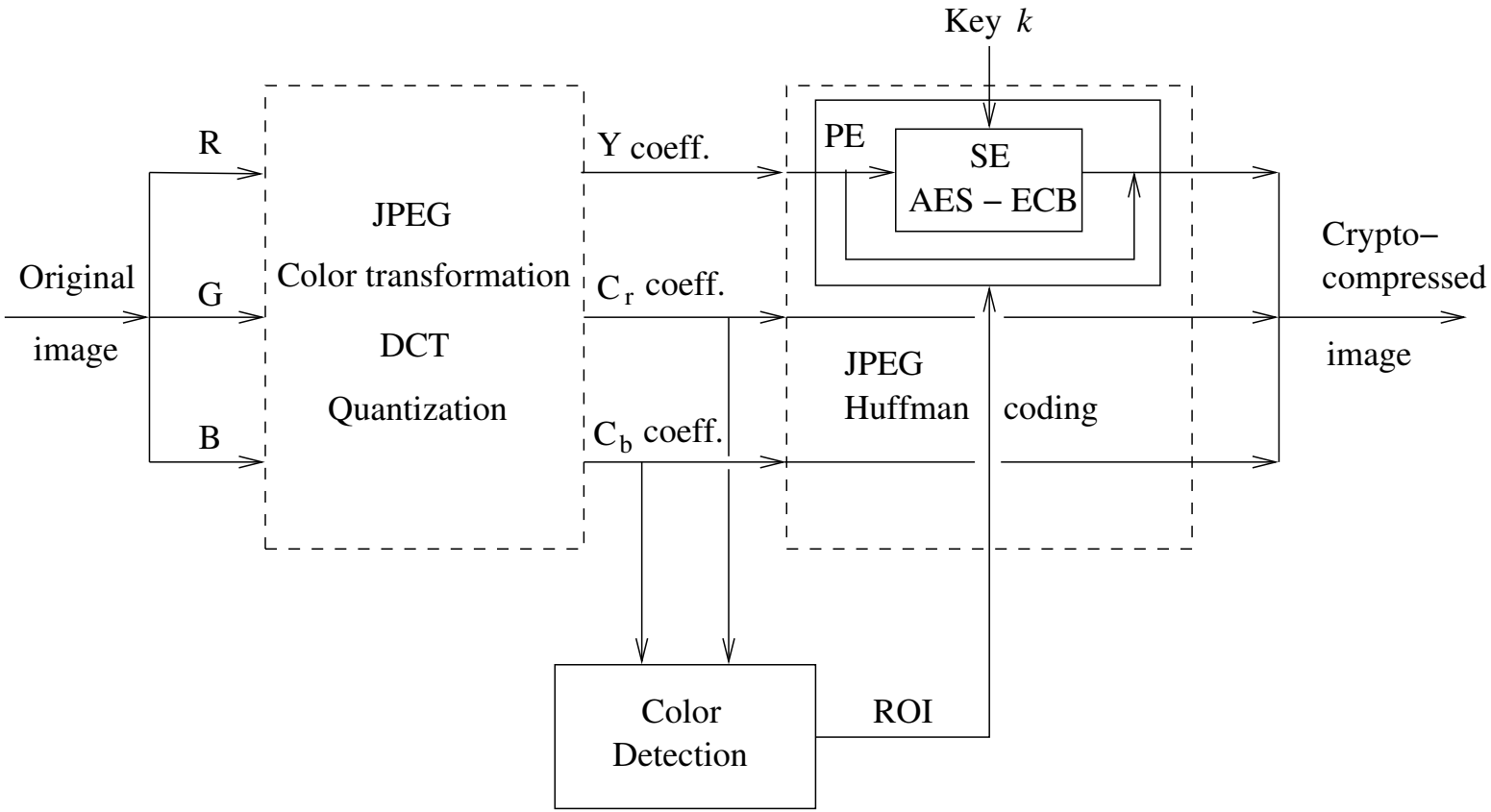


Figure: Global overview of the proposed method.

Global overview of the proposed SE method

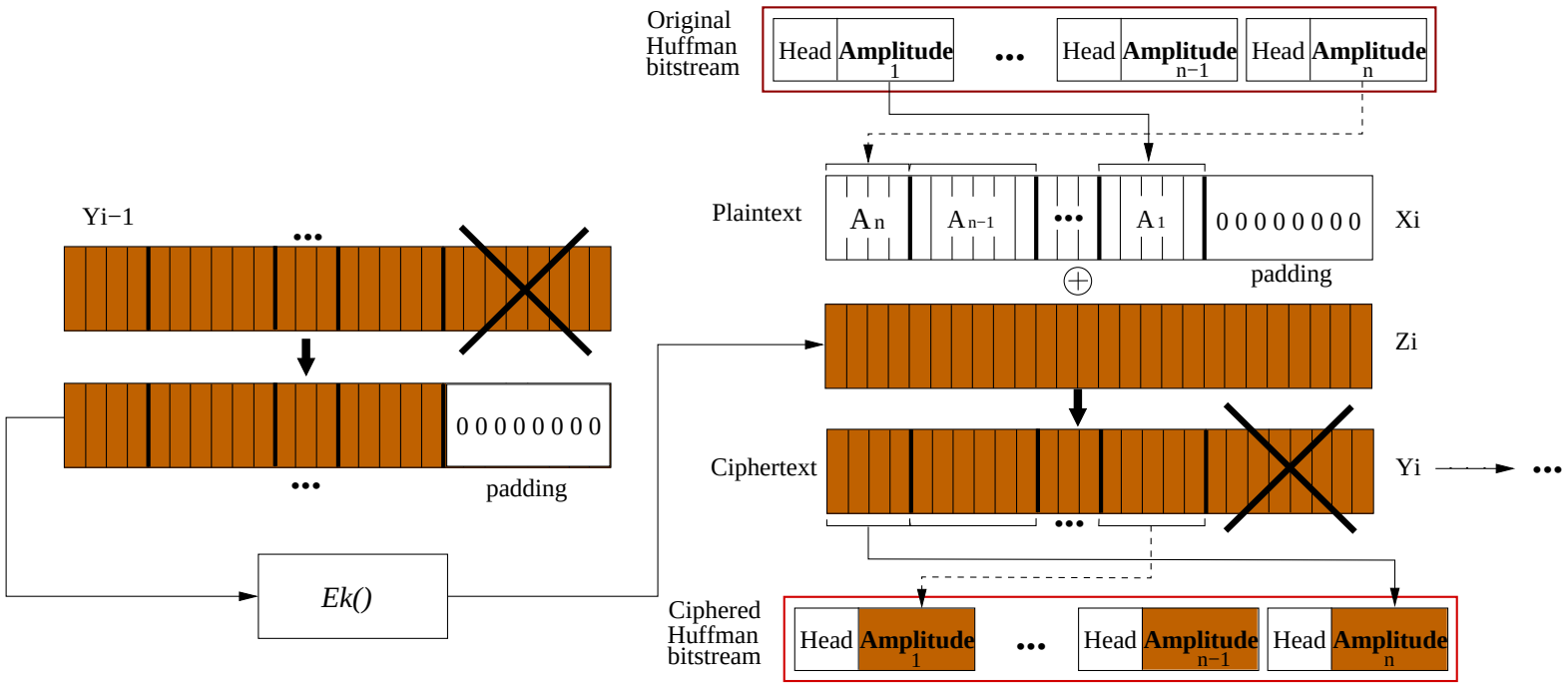


Figure: Global overview of the proposed SE method.

Global overview of the proposed decryption

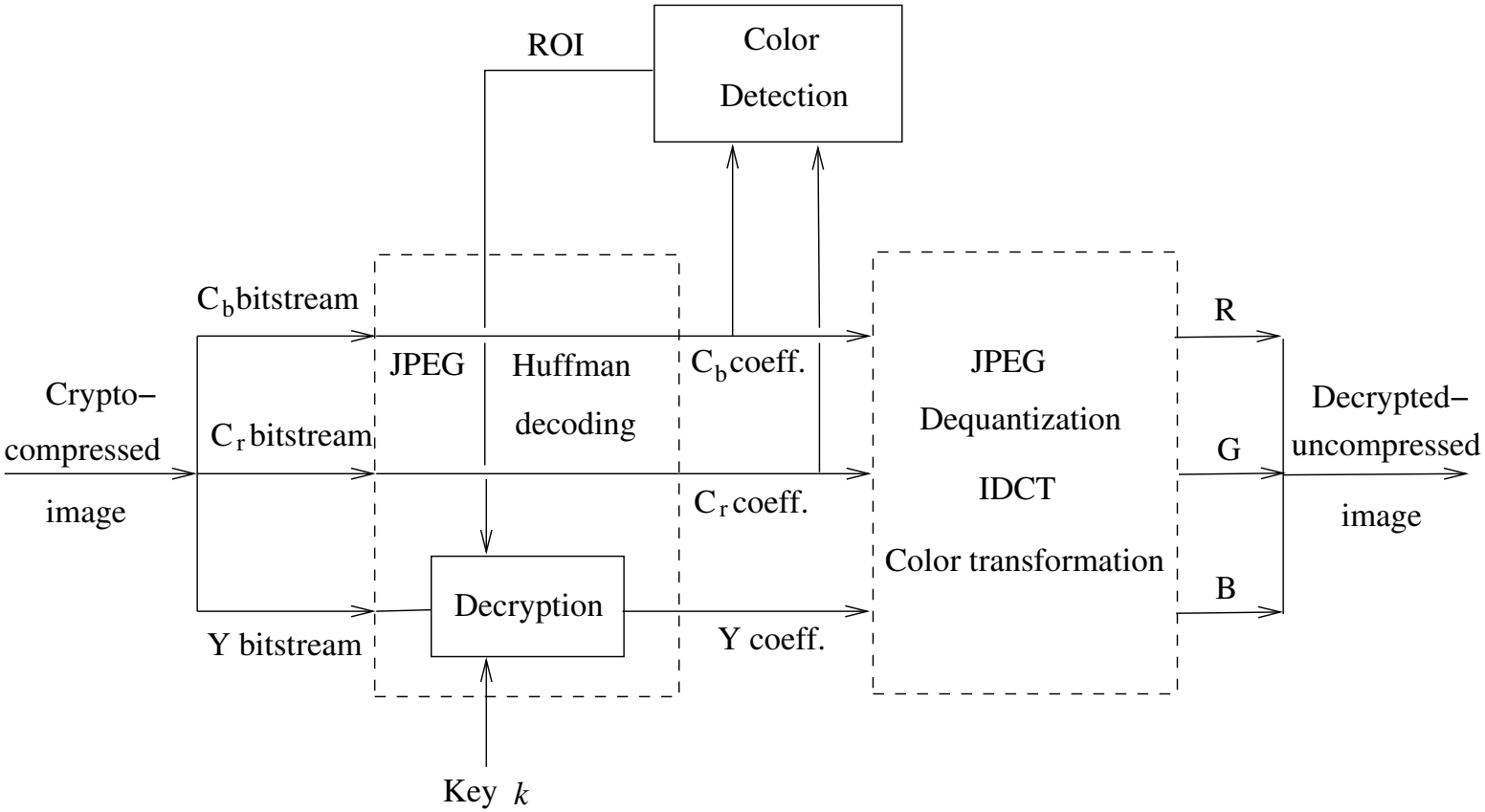


Figure: Global overview of the decryption.

Experimental results

(a) 37.49 *dB*

(b) 20.43 *dB*

(c) 25.46 *dB*

(d) 27.53 *dB*

(e) 20.31 *dB*

(f) 20.60 *dB*

a) JPEG compressed image with QF=100%, b) Image (a) with $C = 128$ bits/block, c) Image (a) with $C = 8$ bits/block, d) JPEG compressed image with QF=10%, e) Image (d) with $C = 128$ bits/block, f) Image (d) with $S = 8$ bits/block.

Experimental results

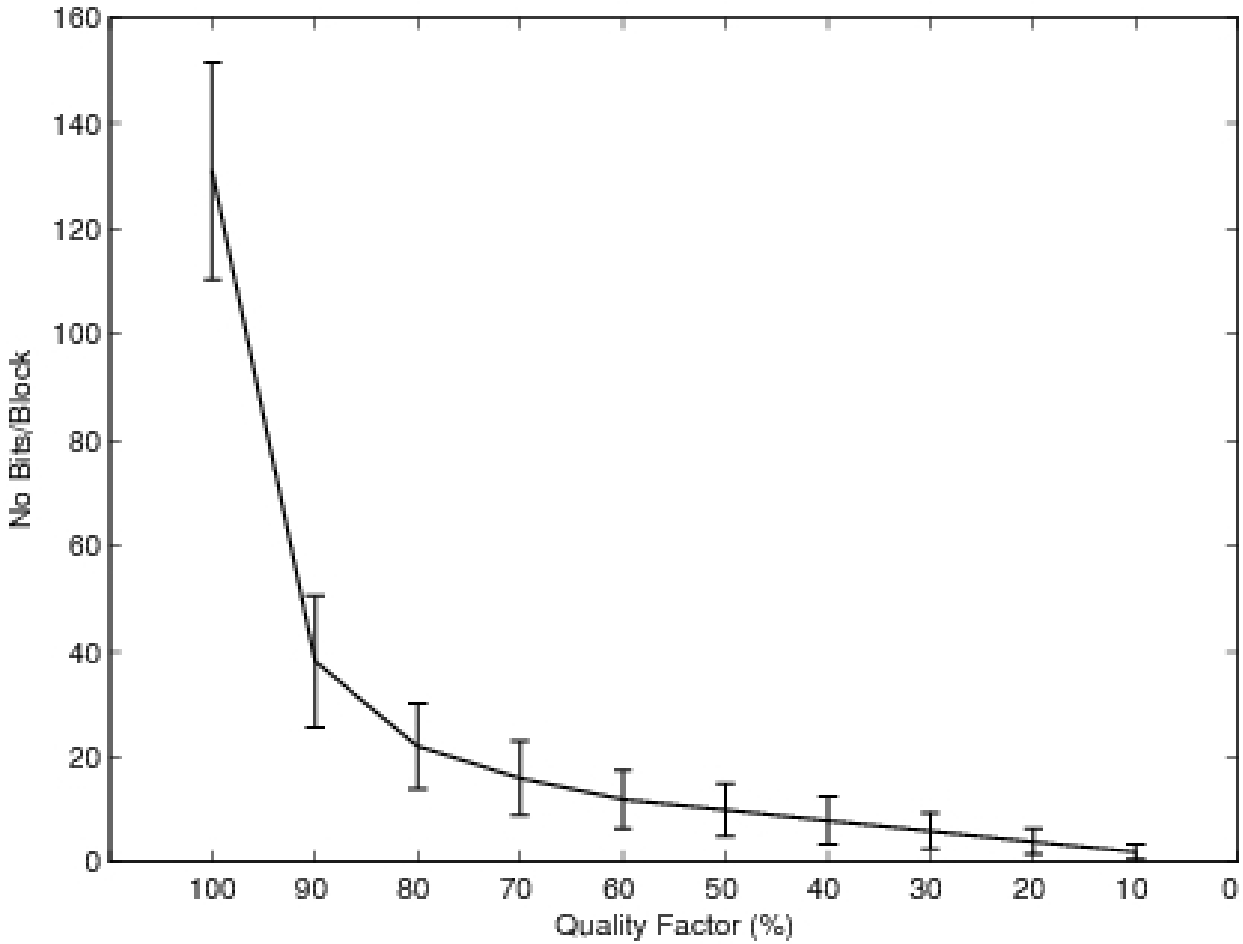


Figure: Ratio between the average number of bits available for SE and the block size.

Experimental results

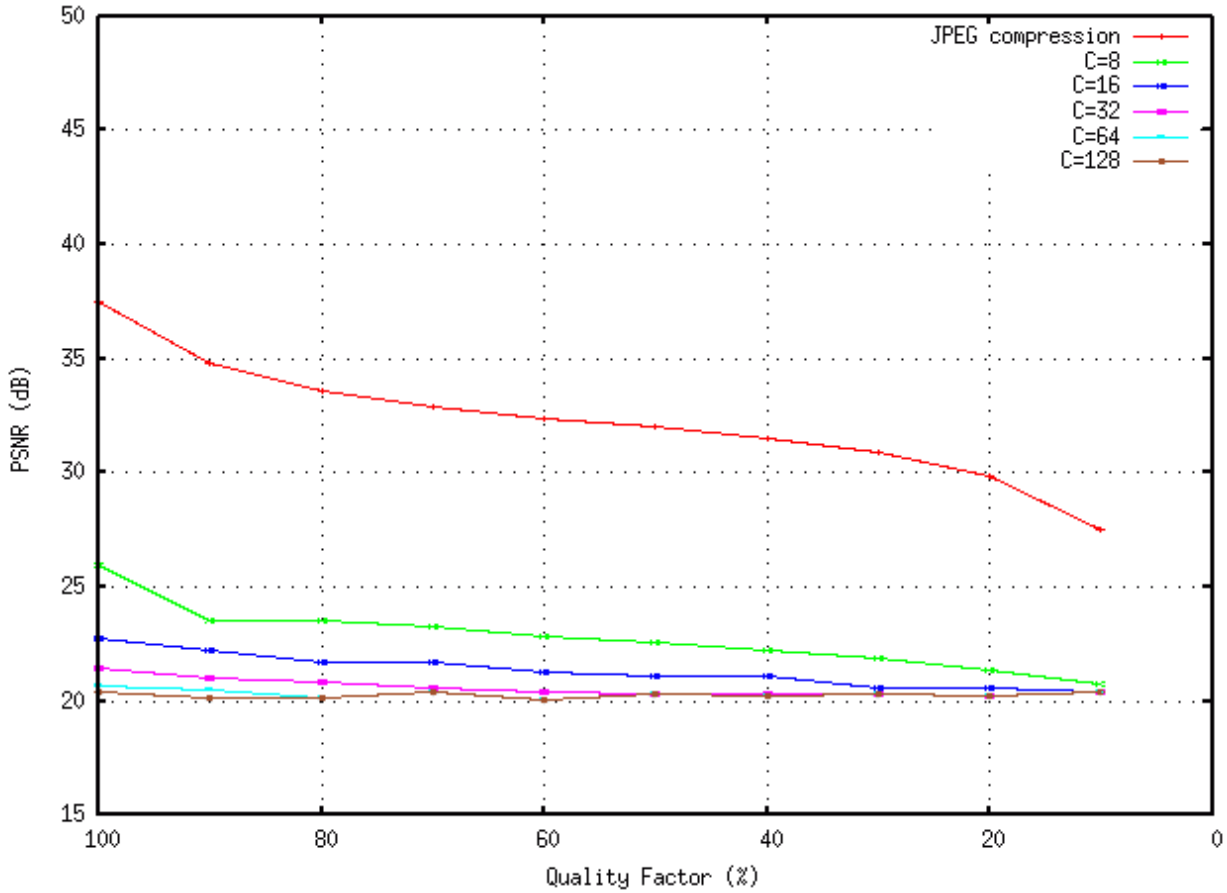


Figure: PSNR of crypto-compressed Lena image for various quality factors and constraints.

Experimental results: a first attack

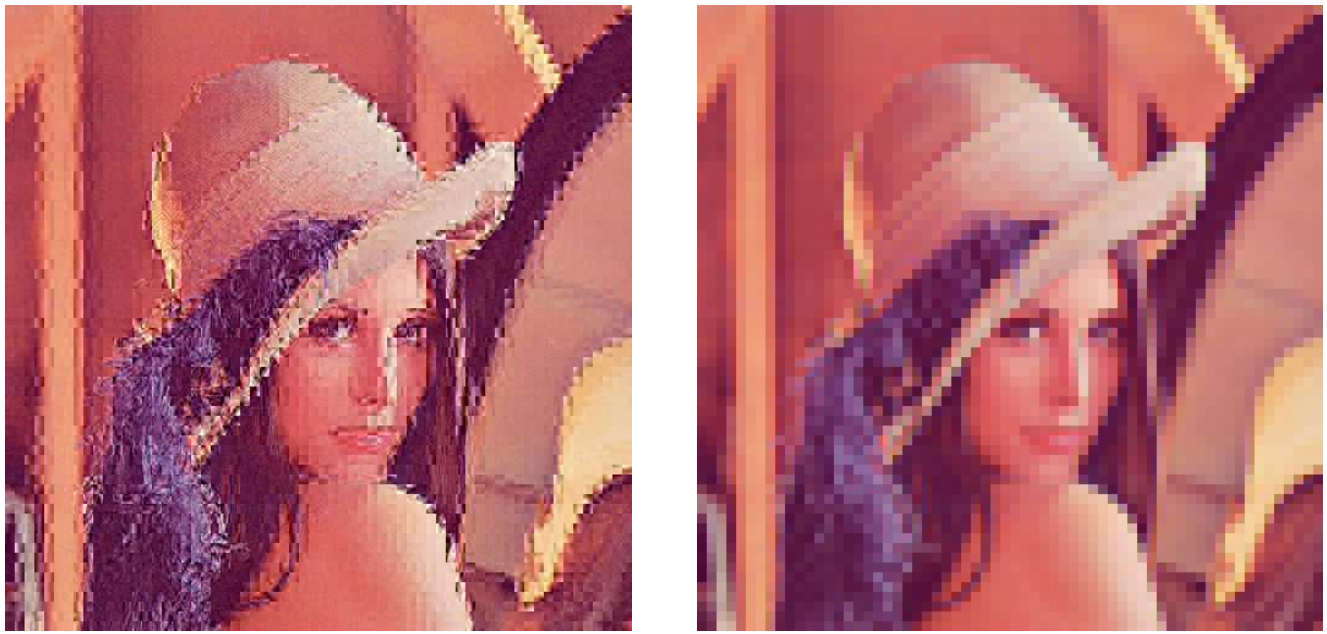
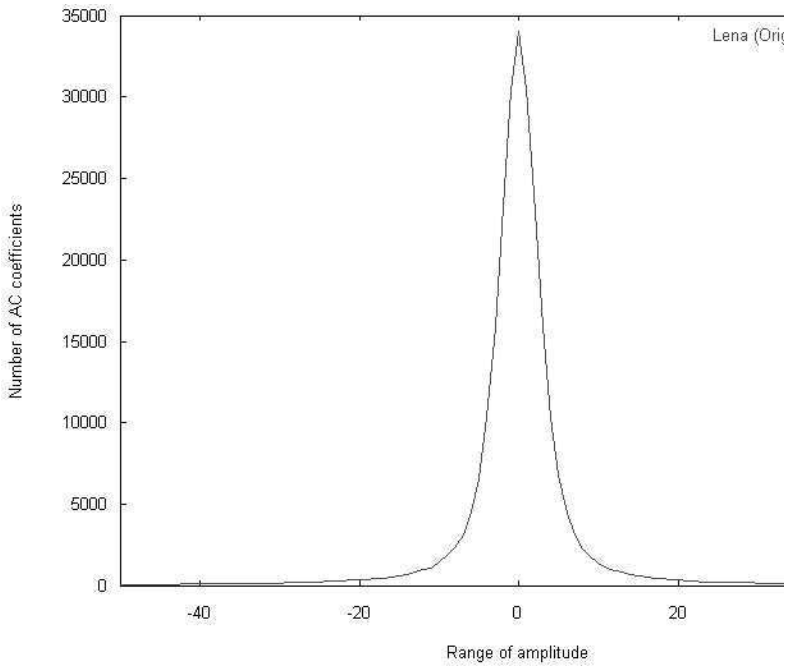
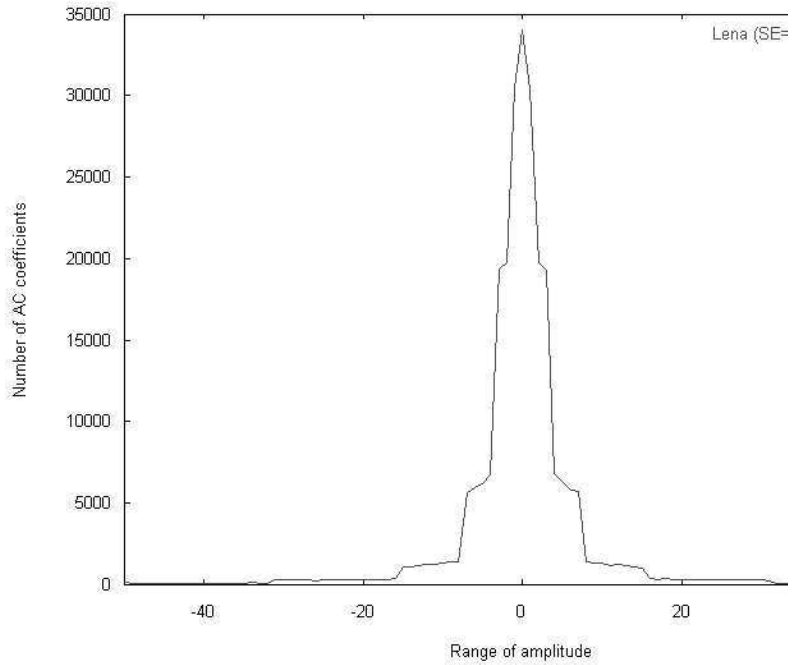


Figure: a) Selectively encrypted image with $C = 128$ bits/block, b) Attack in the selectively encrypted image by removing the encrypted data (23.44 *dB*).

Experimental results: a second attack





Experimental results: face protection

(a)

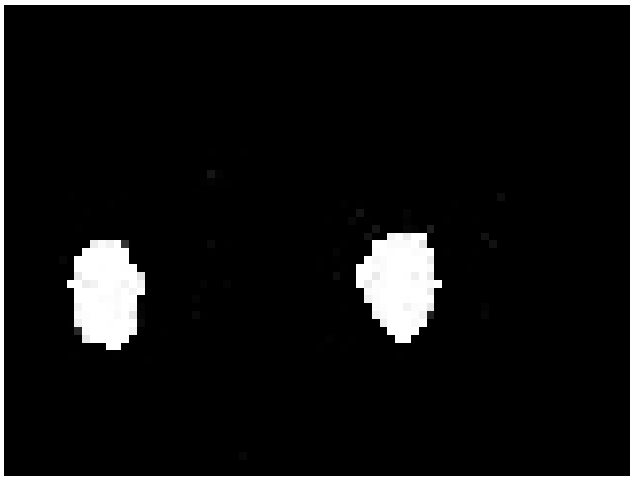
(b)

Figure: Detail resulting from cropping the image: a) Original sub-image, b) SE encrypted sub-image.

Experimental results: face protection

a)

b)



c)

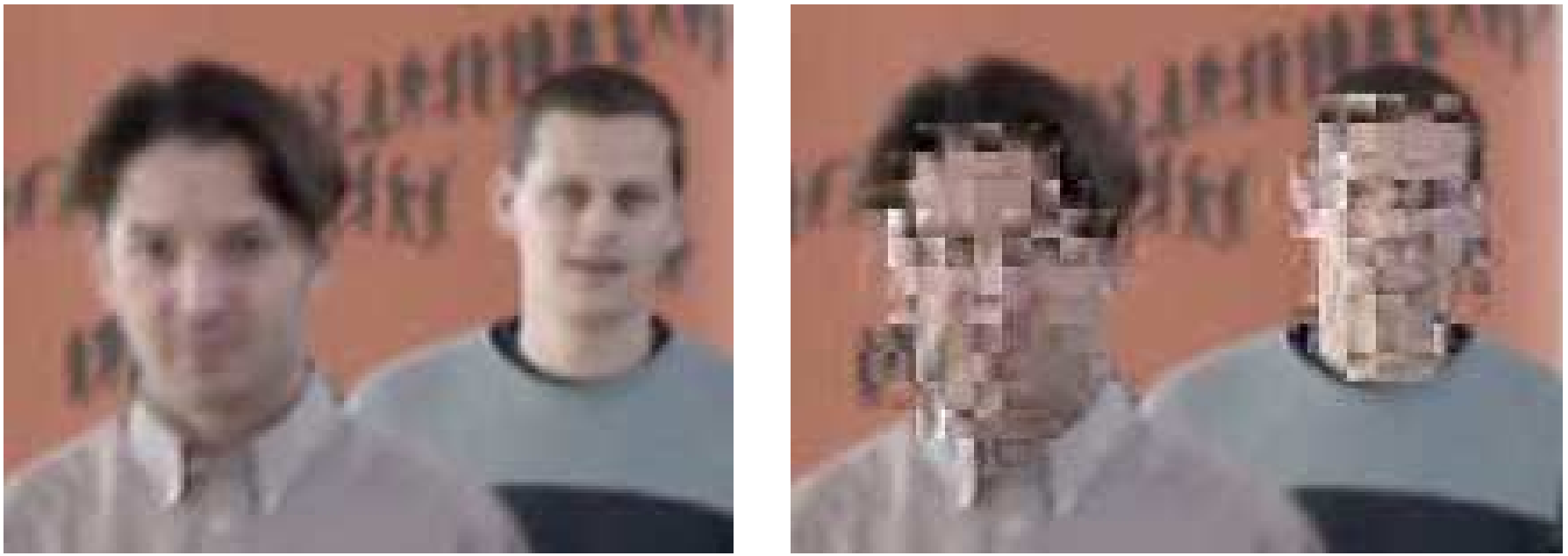
Figure: a) original image of a sequence, b) Detection of the ROI representing the skin, c) Selectively encrypted image.

Experimental results: face protection

	Total ciphered			
Image	Quant. Blocks	Coeff.	Bits	Blocks %
083	79	2547	10112	1.65
123	113	3042	14464	2.35
135	159	4478	20352	3.31
147	196	5396	25088	4.08

Table: Results of PE and SE in a sequence of images acquired with a surveillance video-camera

Experimental results: face protection



(a) (b)

Figure: Region of 216 $\times$ 152 pixels from frame #123: a) Original image, b) Protected image.

Original Image

Encrypted Image, $C = 8$

2.88 % *bits*, $PSNR = 25.87$ *dB*.

H. Cheng and X. Li.

Partial Encryption of Compressed Images and Videos.
IEEE Transactions on Signal Processing, 48(8), pp. 2439-2451, 2000.

A. Said.

Measuring the Strength of Partial Encryption Scheme.
IEEE ICIP International Conference in Image Processing, pp. 1126-1129, Genova, Italy, 2005.

Original Image

Encrypted Image, $C = 128$

34.70 % *bits*, $PSNR = 19.31$ *dB*.

H. Cheng and X. Li.

Partial Encryption of Compressed Images and Videos.
IEEE Transactions on Signal Processing, 48(8), pp. 2439-2451, 2000.

A. Said.

Measuring the Strength of Partial Encryption Scheme.
IEEE ICIP International Conference in Image Processing, pp. 1126-1129, Genova, Italy, 2005.

Substitution of the encrypted AC by 0

$PSNR = 19.20\ dB$

Encrypted Image, $C = 128$

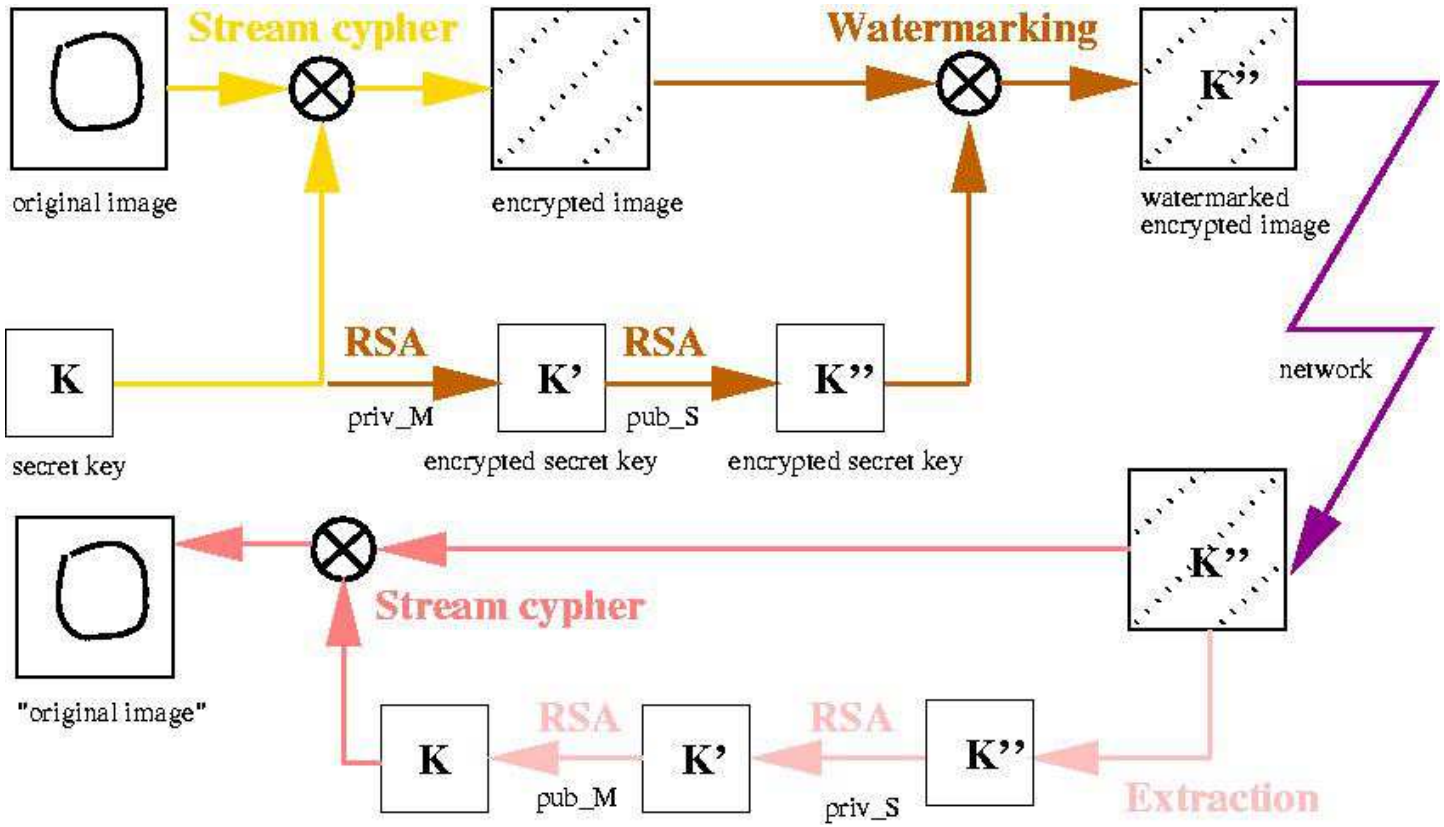
34.70 % *bits*, $PSNR = 19.31\ dB$.

J. Rodrigues, W. Puech and A. Bors.
Selective and Partial Encryption Method in JPEG Color Image Sequences for People Privacy Protection.
Pattern Recognition, Elsevier, submitted.

Outline

Outline

The method



Combination of public key encryption, secret key stream cipher, and data hiding method.

Combination of encryption and watermarking algorithms

DCT-based Data Hiding

- To embed a message M made up of k bits b_i ($M = b_1 b_2 ... b_k$).
- Square blocks made up of n^2 pixels p_i of the image of N pixels.
- We calculate the DCT continuous component $F(0,0)$ of this block:

$$F(0,0) = \frac{1}{n} \sum_{i=0}^{n^2-1} p_i. \tag{5}$$

where n is the side of the block of pixels.

- $$F'(0,0) = [F(0,0)/Q(0,0)], \tag{6}$$

where $Q(0,0)$ is the quantization value.

- To embed a bit before the quantization ($F(0,0)$ by $F_w(0,0)$):

$$F_w(0,0) = \begin{cases} \lfloor \frac{F(0,0)}{Q(0,0)} \rfloor \times Q(0,0) & \text{if } \lfloor \frac{F(0,0)}{Q(0,0)} \rfloor \%2 = b_i, \\ \lceil \frac{F(0,0)}{Q(0,0)} \rceil \times Q(0,0) & \text{if } \lceil \frac{F(0,0)}{Q(0,0)} \rceil \%2 = b_i, \end{cases} \tag{7}$$

- After quantization :

$$F'_w(0,0) = F_w(0,0)/Q(0,0). \tag{8}$$

$$d = F(0,0) - F_w(0,0). \tag{9}$$

$$n_w = \left[\frac{|d| \times n}{Q(0,0)} \right]. \tag{10}$$

- Modification of the value of n_w pixels of the block of n^2 pixels to get new pixel's value $p_w(i)$:

$$p_w(i) = p(i) - sign(d), \tag{11}$$

- The modified pixels are chosen in function of a criterion
- For the DC component after quantization, we have for each block that embed a bit of the message:

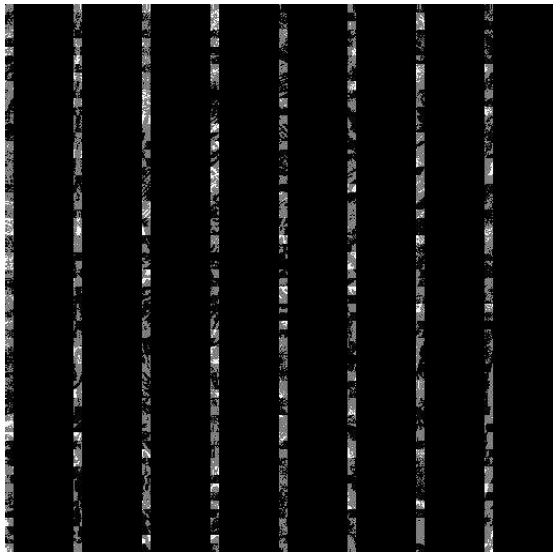
$$F'_w(0,0) = \frac{1}{n \times Q(0,0)} \Big(\sum_{i=0}^{n_w-1} p_w(i) + \sum_{i=n_w}^{n^2-1} p(i) \Big). \tag{12}$$

- We calculate an embedding factor

Combination of encryption and watermarking algorithms

a)

b)

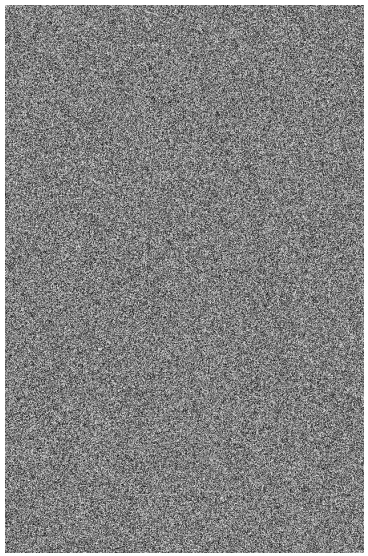


c)

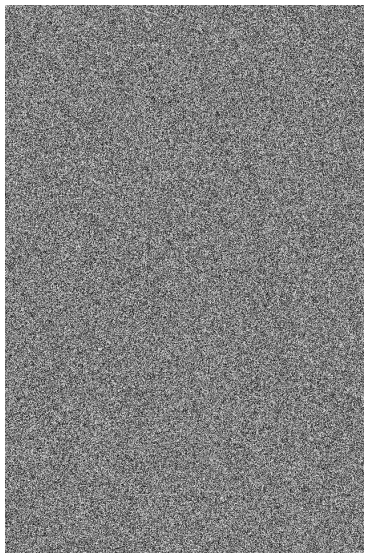
a) Original image.
b) Embedded image with a message of 512 bits using the DCT based data hiding method.
c) Difference between (a) and (b).

Results of the combination

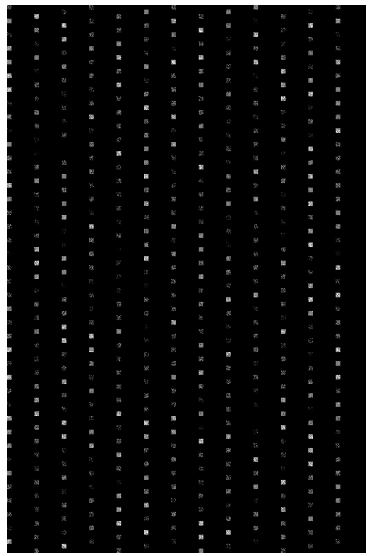
(a)



(b)



(c)



(d)

a) Original image, b) Stream cipher encrypted image 128-bit key, c) DCT based embedded encrypted image with 512-bit key, d) Difference between the encrypted image and the DCT based embedded encrypted image.

Combination of encryption and watermarking algorithms

Decryption

(a) (b) (c)

a) Original image, b) Decryption of the DCT based embedded encrypted image, c) Difference between original image and the decrypted DCT based embedded one.

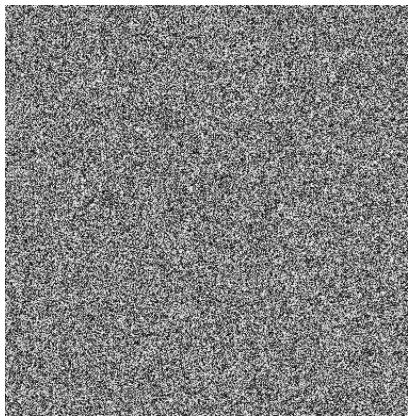
Transmission on a noised network

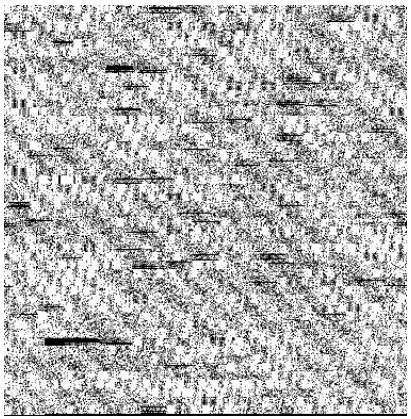
(a) (b) (c)

a) original image, b) Decryption of the noisy encrypted image with the extracted key with the DCT based data hiding method c) Decryption of the noisy encrypted image with the extracted key with a spatial data hiding method.

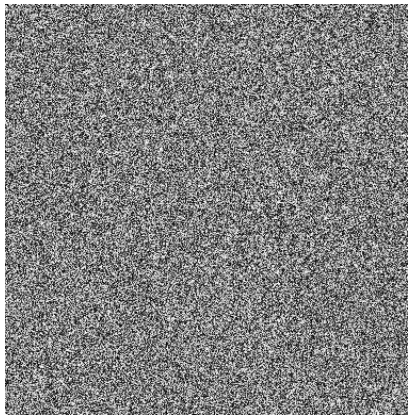
Comparison with AES in OFB mode (synchronous stream) and in CFB mode (asynchronous stream)

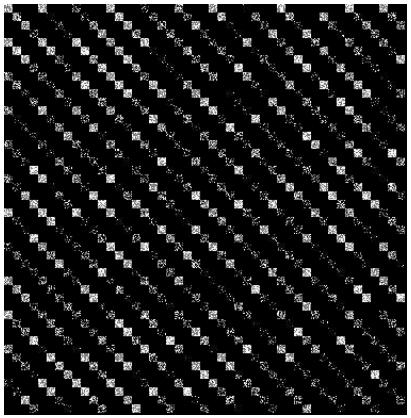
a)





b)





a) Encrypted image with our method (with a key of 512 bits),

b) Encrypted image with AES in OFB mode, and watermarked (with a key of 512 bits).

Outline

Outline

The idea

- To embed data in encrypted images
- To analyze the local standard deviation of the marked encrypted images:
  - In order to remove the embedded data,
  - During the decryption step.

Image encryption

AES algorithm with ECB mode [AES]

- Encryption by block X_i of 128 bits:
  - $n = 16$ gray level pixels.
- With the ECB mode:
  - Each plaintext block X_i is encrypted with the same secret key k producing the ciphertext block Y_i:

$$Y_i = E_k(X_i). \tag{13}$$

J. Daemen and V. Rijmen.
AES Proposal: The Rijndael Block Cipher.
Proton World Int.l, Katholieke Universiteit Leuven, ESAT-COSIC, Belgium, 2002.

Security level analysis

The entropy $H(S)$:

$$H(S) = -\sum_{j=0}^{M-1} P(\alpha_j) log_2(P(\alpha_j)). \quad (14)$$

Information redundancy r:

$$r = b - H(S), \quad (15)$$

The order-n entropy $H(S')$:

$$H(S') = H(S^n) = -\sum_{j=0}^{M^n-1} P(\beta_j) log_2(P(\beta_j)). \quad (16)$$

Theoretically, for an encrypted image:

- The information redundancy r equals to zero,
- The entropy is greater than the entropy of the original image,
- The local standard deviation is higher than for the original image:
- For each block, the local standard deviation $\sigma(X_i)$:

$$\sigma(X_i) = \sqrt{\frac{1}{n}\sum_{j=1}^{n}(p_j - \overline{X_i})^2}, \tag{17}$$

Global overview of the Encoding algorithm

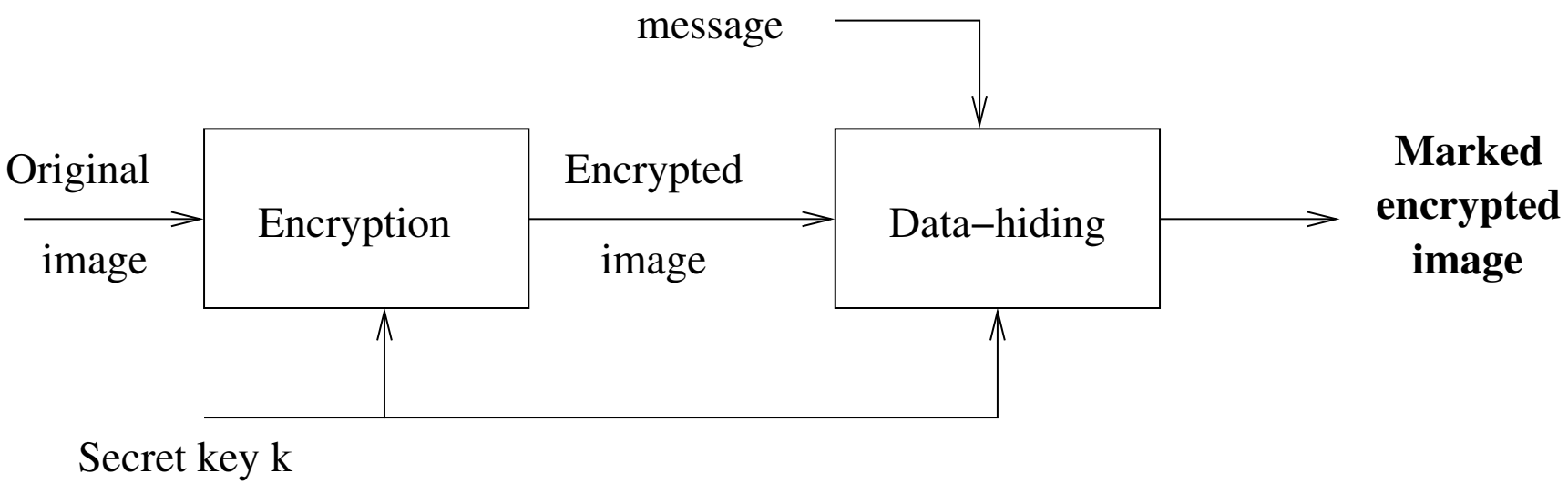


Figure: Overview of the encoding method.

Encoding algorithm

Two steps:

- The encryption: for each block X_i composed of n pixels p_j of an image of N pixels, we apply the AES encryption algorithm by block:

$$Y_i = E_k(X_i). \tag{18}$$

- The data hiding: in each cipher-text we modify only one bit of one encrypted pixel of Y_i:

$$Yw_i = DH_k(Y_i). \tag{19}$$

  - We used bit substitution-based data hiding method in order to embed the bits of the hidden message.
  - Since we embed 1 bit in each block of n pixels, the embedding factor is equal to $1/n$ bit per pixel.

Global overview of the decoding method

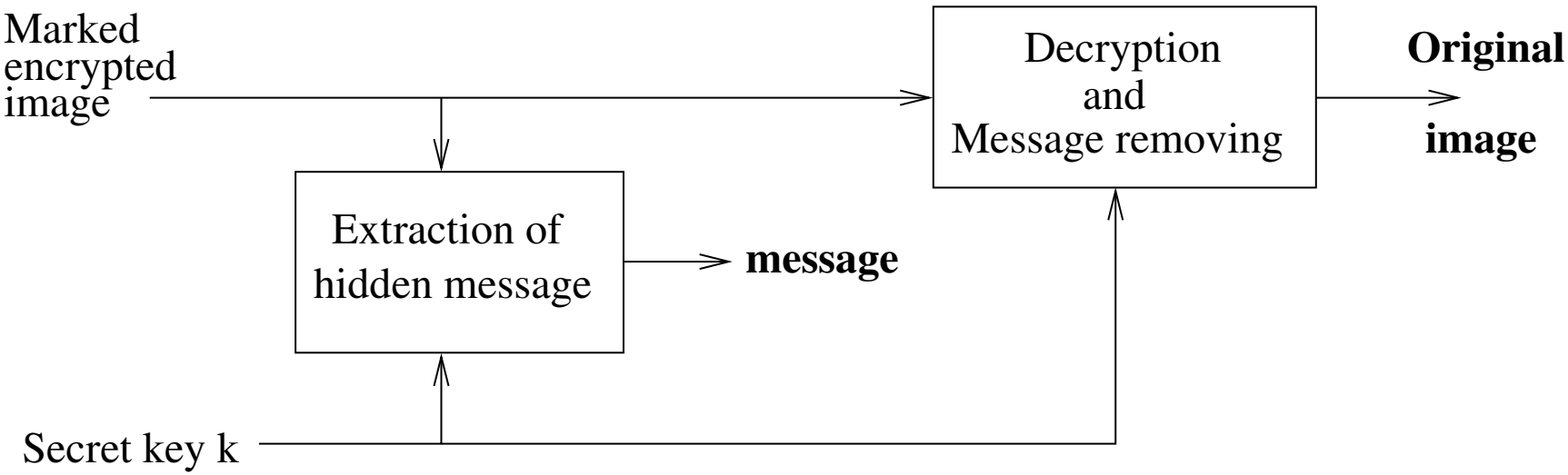


Figure: Overview of the decoding method.

Decoding algorithm

Two steps:

- The extraction of the message,
- The decryption and message removing step by analyzing the local standard deviation:
  - For each marked cipher-text Yw_i we apply the decryption function $D_k()$ for the two possible values of the hidden bit (0 or 1),
  - For each block, we compare the local standard deviation of the two decrypted blocks $X0_i$ with $X1_i$ and we select the bit value where the local standard deviation is the smaller:

$$\begin{cases} X_i & = & D_k(Y0_i) \text{ if } \sigma(D_k(Y0_i)) < \sigma(D_k(Y1_i)) \\ & = & D_k(Y1_i) \text{ else.} \end{cases} \quad (20)$$

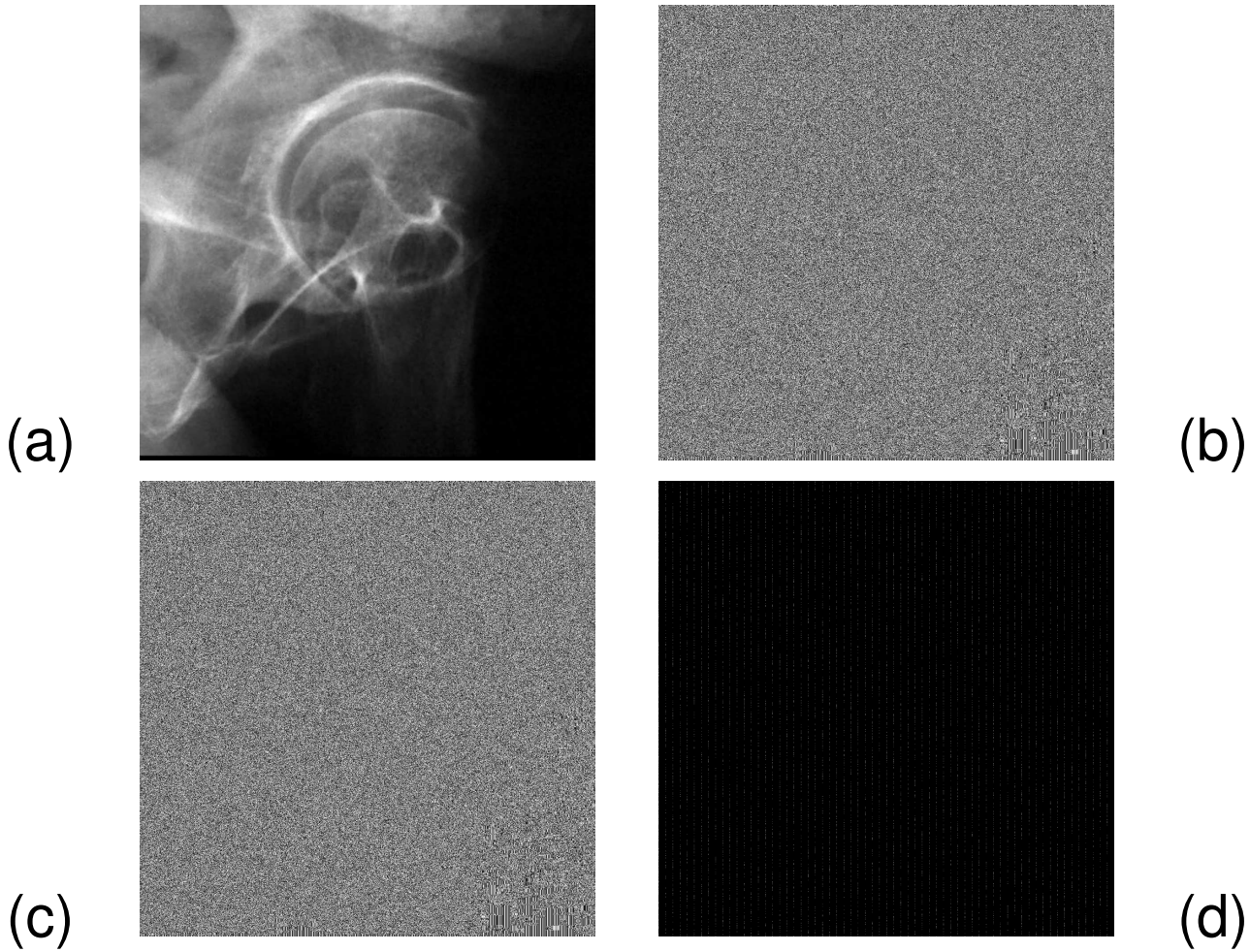
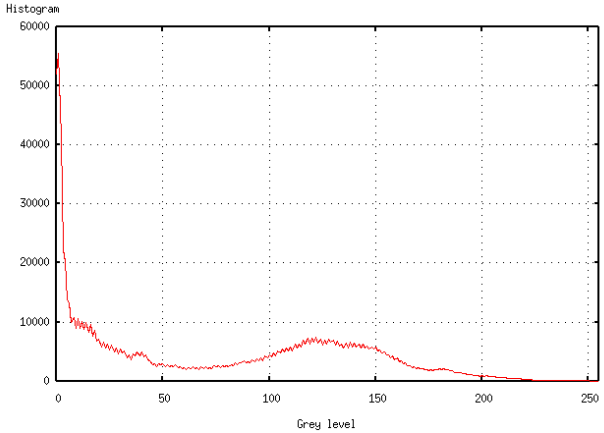
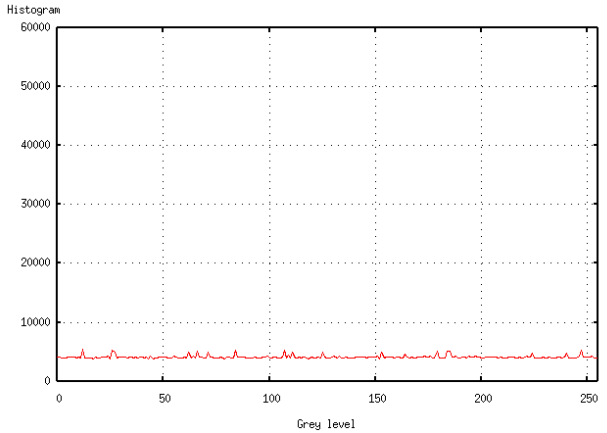


Figure: a) Original medical image of 1024 $\times$ 1024 pixels, b) Encrypted image with AES in ECB mode, c) Encrypted and marked image with 65536 hidden bits, d) Difference between b) and c).

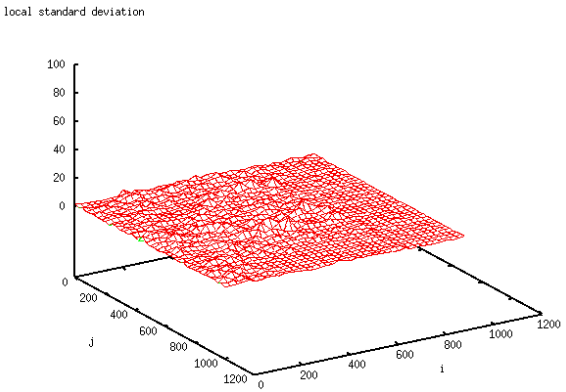
(a)

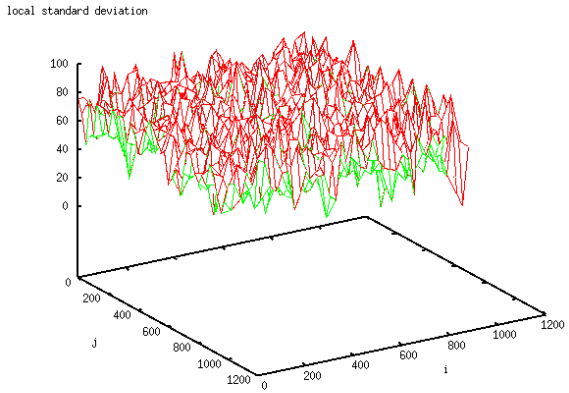




(b)

(c)

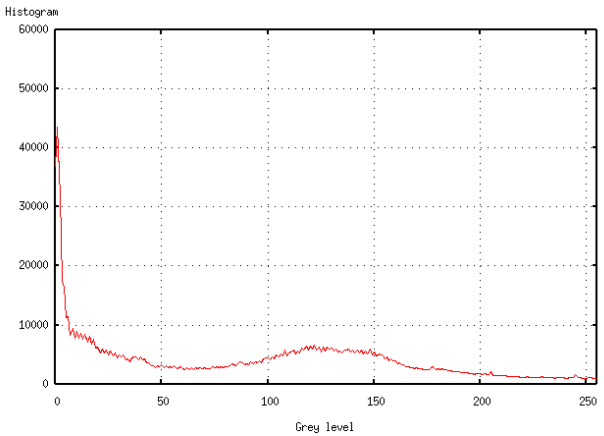




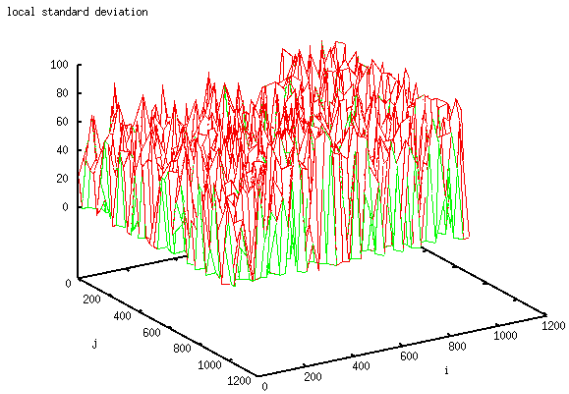
(d)

Figure: Histogram of: a) The original image, b) The marked encrypted image, Local standard deviation of: c) The original image, d) The marked encrypted image.

(a)

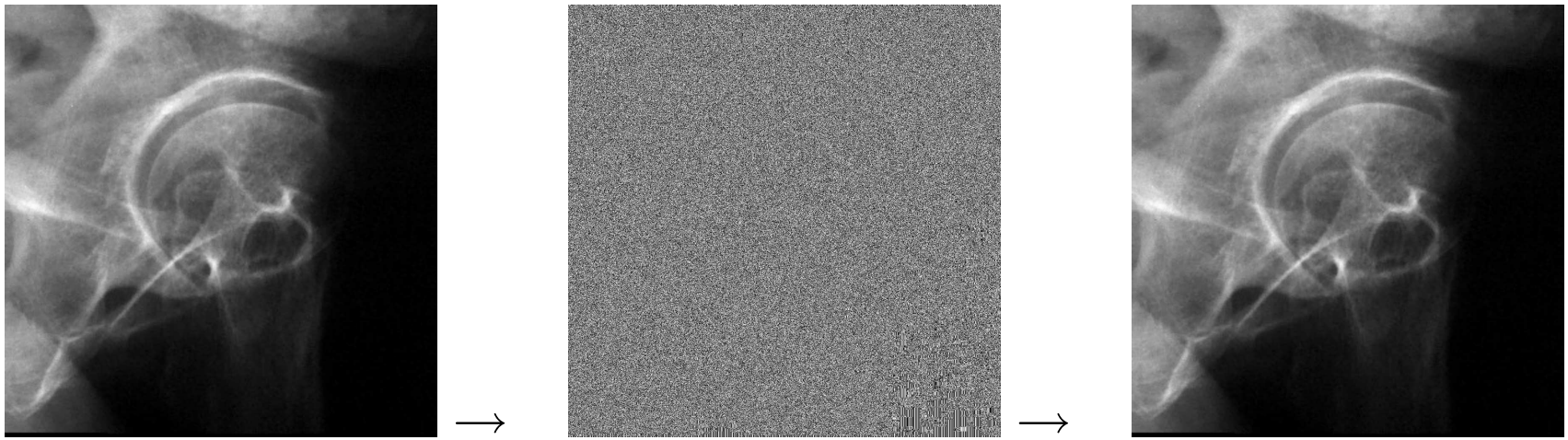


(b)



(c)

Figure: a) Extraction of the message and decryption of the marked encrypted image, b) Histogram of the decrypted marked image, c) Local standard deviation of the decrypted marked image.

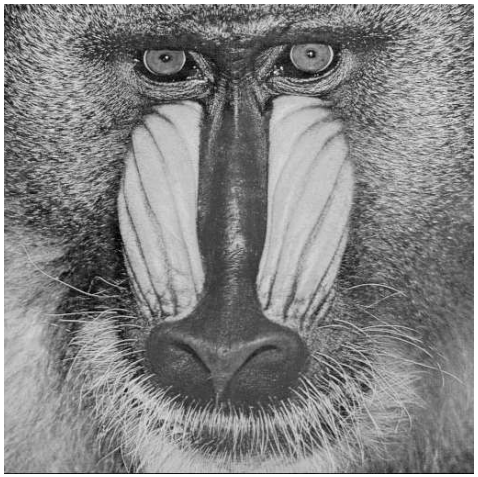


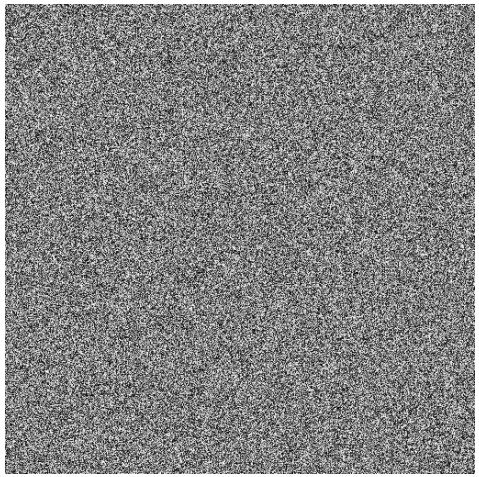
(a) (b) (c)

Figure: a) Original image, b) Encrypted and marked image with 65536 hidden bits, c) Decryption and deleting of the message by using the proposed method.

Comparison with a standard reversible approach

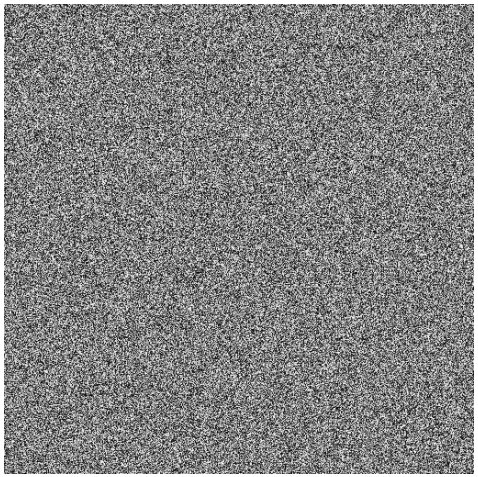
(a)

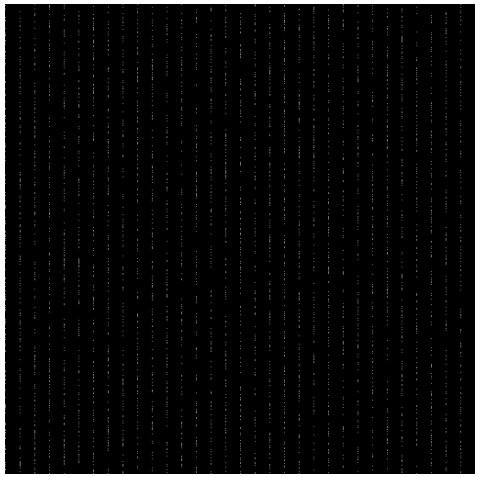




(b)

(c)





(d)

Figure: a) Original image of 512×512 pixels, b) Encrypted image with AES in ECB mode, c) Encrypted and marked image with 16384 hidden bits, d) Difference between b) and c)

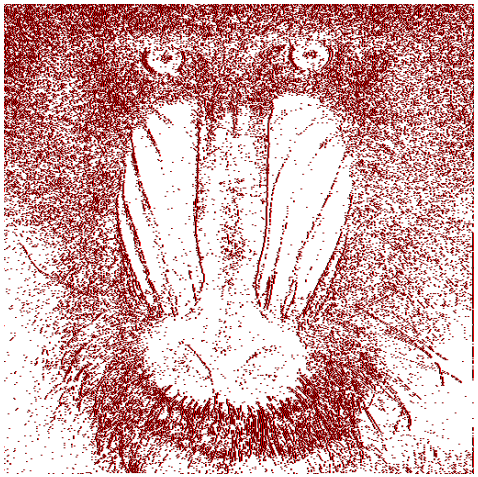
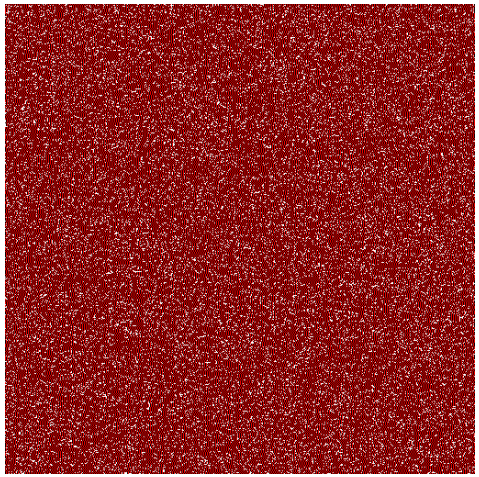
(a)   (b)

Figure: Application of a reversible data hiding method [COLTUC 06]: a) On the original image of Baboon, b) On the encrypted image of Baboon with AES.

On the original image: 170914 white pixels, 2 or 3 bits per pixel and few correctives codes.
On the encrypted image: 28352 white pixels but 116896 correctives codes are necessary.
The data hiding is not possible on the encrypted image.

D. Coltuc and J-M. Chassery.
High Capacity Reversible Watermarking.
Proc. IEEE Int. Conf. on Image Processing, Atlanta, USA, Oct. 2006.

With our approach

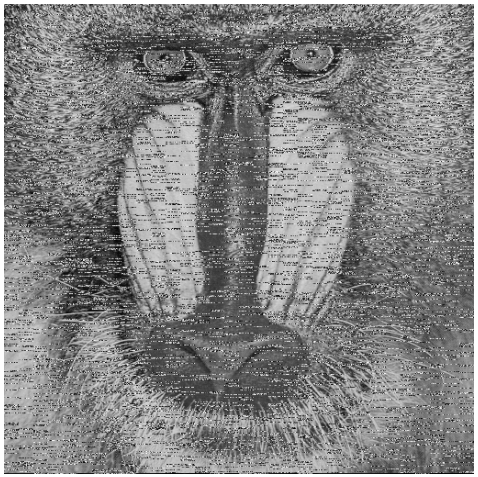
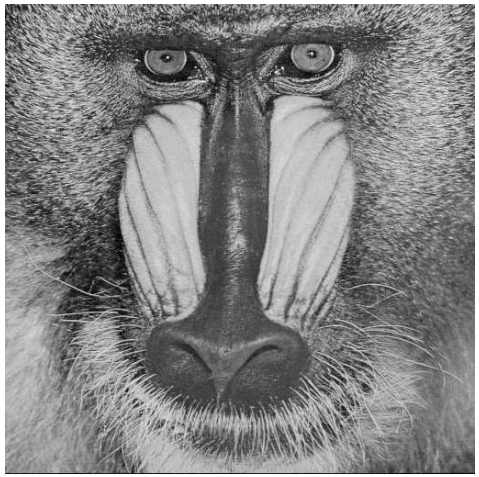
(a)   (b)

Figure: a) Extraction of the message (16384 bits) and decryption of the marked image, b) Decryption and deleting of the message by using the proposed method.

Conclusions

With our proposed reversible data hiding method for encrypted images:

- We are able to embed data in encrypted images,
- We can decrypt the image and rebuild the original image by removing the hidden data.

In this presentation:

- We detailed all the steps of the proposed method,
- We presented and analyzed various results.
- We compared with a standard reversible approach.

Outline

Outline

Image watermarking: LSB substitution

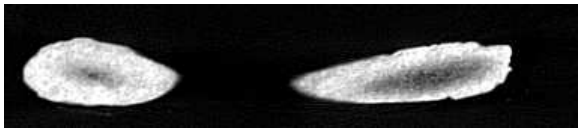
#17

#54

#83

Figure: 125 original slides of “Baton Percé”

#17



#54

#83

Figure: 125 watermarked slides of “Baton Percé”

Image watermarking: LSB substitution

Analyze

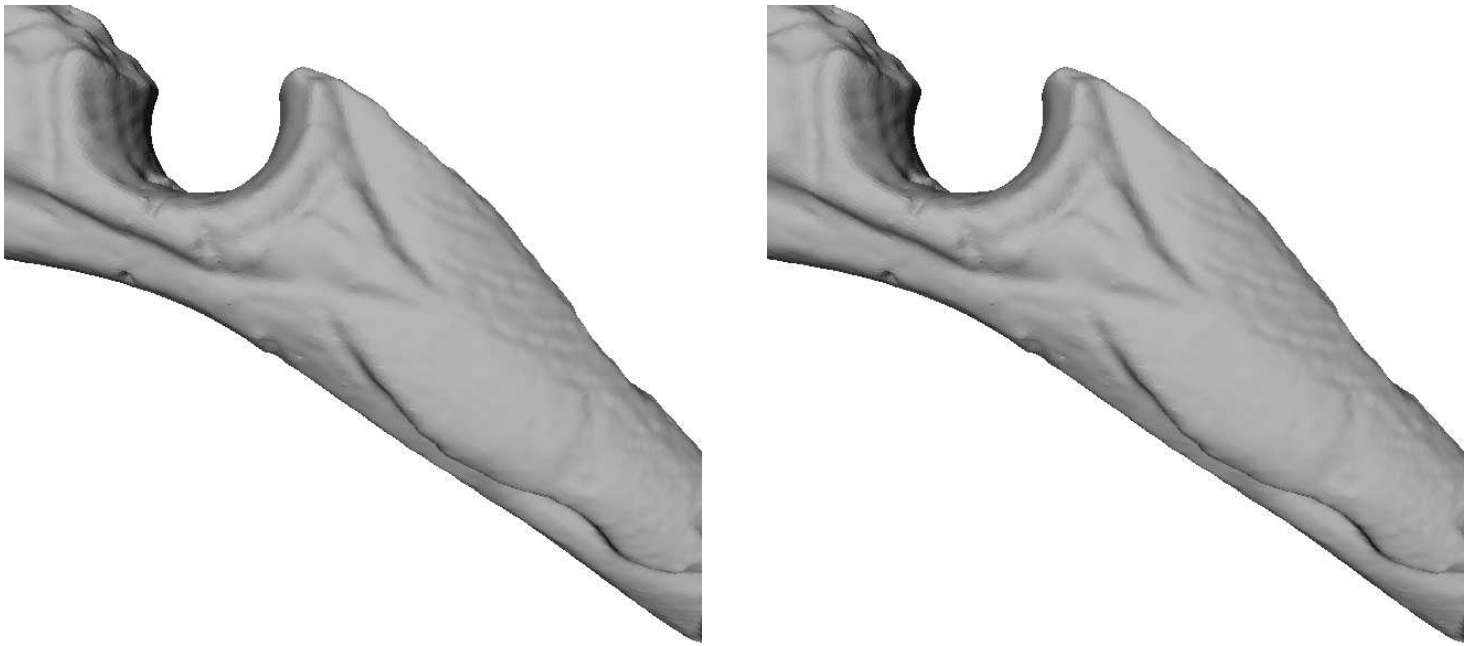
- original size: 125 slides 382 $\times$ 82 pixels
- watermarking with a text file: 5.4 kBytes: PNSR = 70.5 dB
- watermarking with an image of 25.8 kBytes: PNSR = 63.8 dB
- watermarking with a 3D file of 472.4 kBytes: PNSR = 51.2 dB

Original #17

Watermarked #17

Difference.

Image watermarking: LSB substitution



(a) (b)

Figure: 3D Reconstruction: a) From the original data, b) From the watermarked data.

Outline

3D watermarking based on MST

References

P. Amat, W. Puech, S. Druon and J.P. Pedeboy
Lossless Data Hiding Method Based on MST and Topology Changes of 3D Triangular Mesh
Proceedings of the 16th European Signal Processing Conference, Lausanne, Switzerland, 2008

Algorithm

- MST construction,
- Search of quadruples,
- Selection of quadruples based on coplanarity and convexity,
- Embed one bit in each selected quadruple.

3D watermarking based on MST

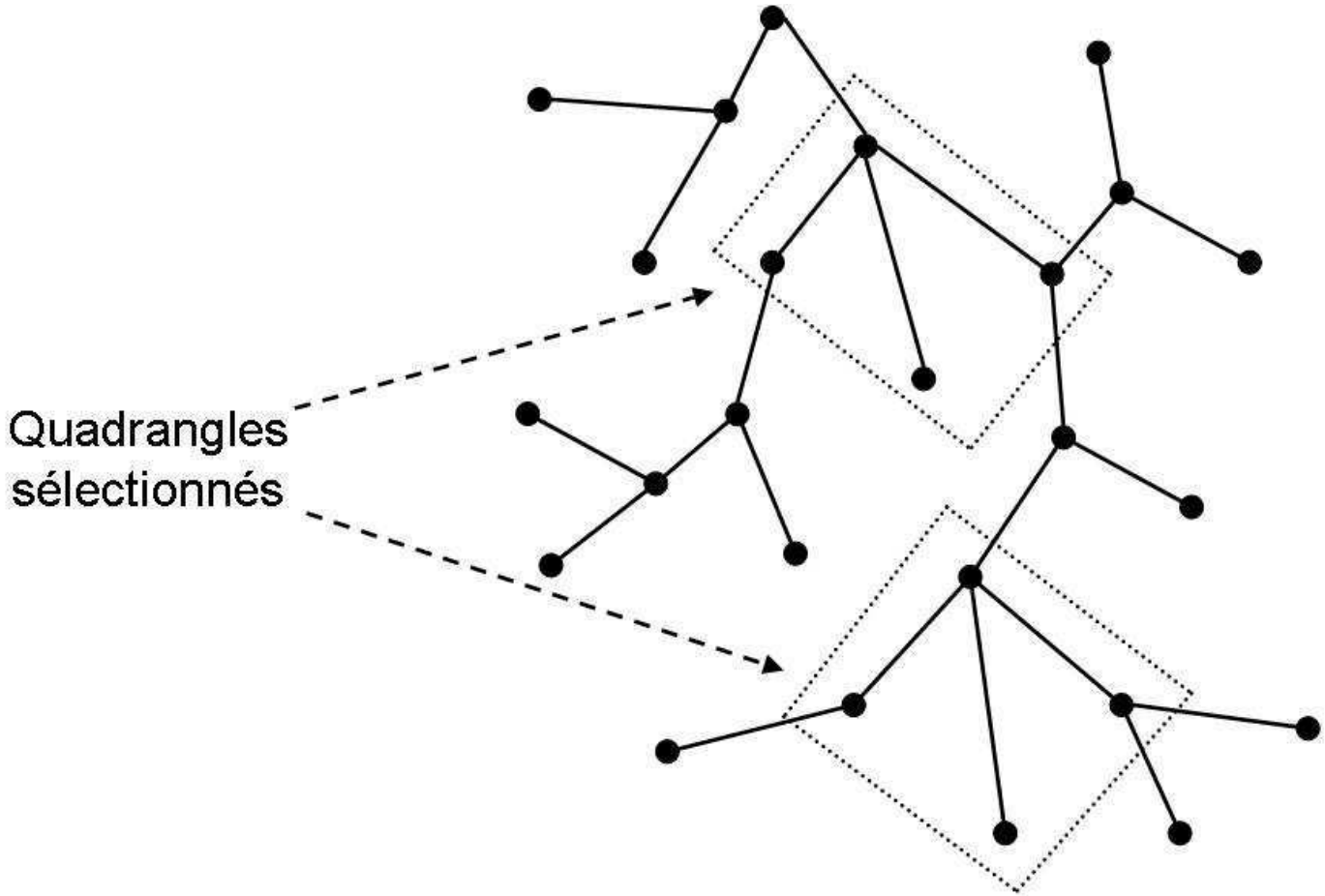


Figure: Selection of quadruples in the MST.

3D watermarking based on MST

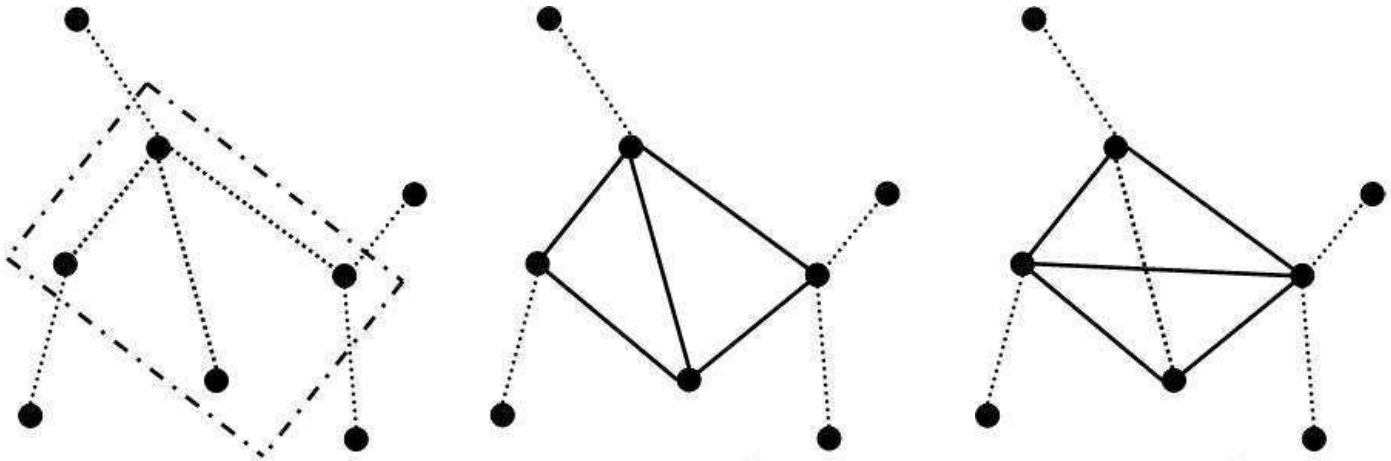


Figure: Data hiding of a 0-bit or a 1-bit.

3D watermarking based on MST

Advantages

- Global
- High payload
- Any modification of the vertex positions

Inconvenient

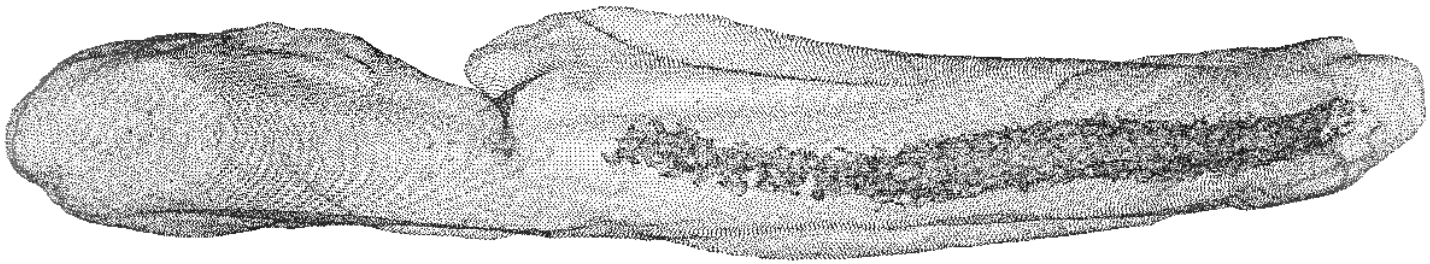
- No robust to noise

3D Watermarking

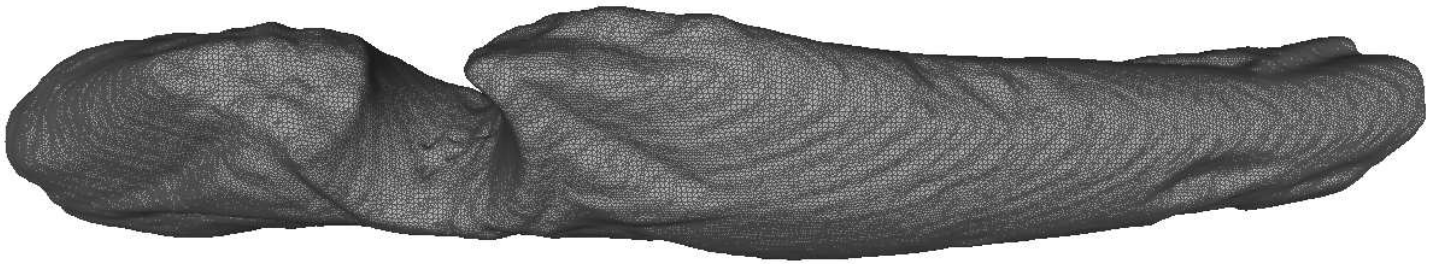
"Baton Percé": 102173 vertices.

- With a threshold of 1 degree: message = 4466 bits (Hausdorff's error = 0.001637).
- With a threshold of 30 degree: message = 21698 bits (Hausdorff's error = 0.029063)

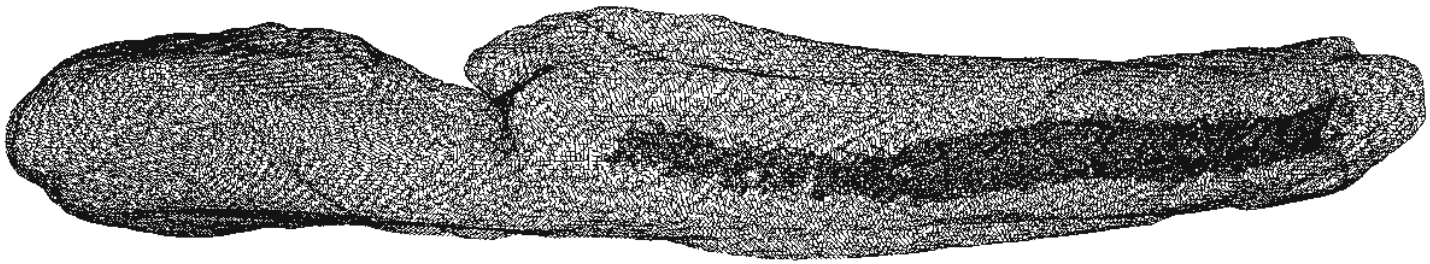
3D Watermarking



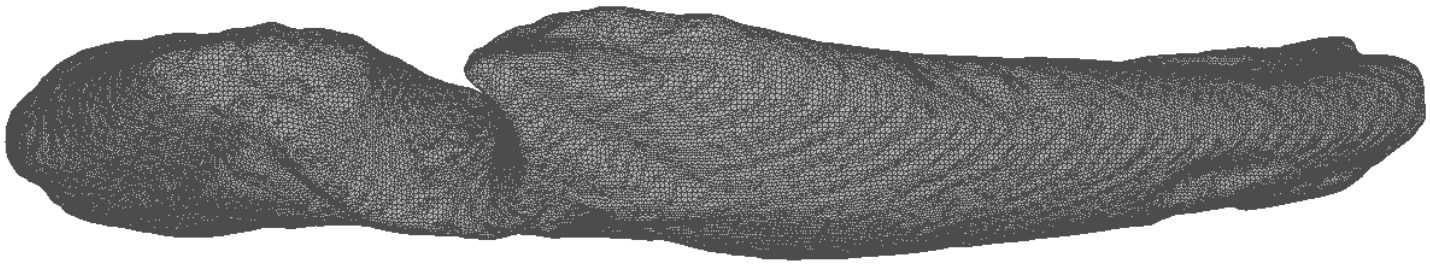
3D Watermarking



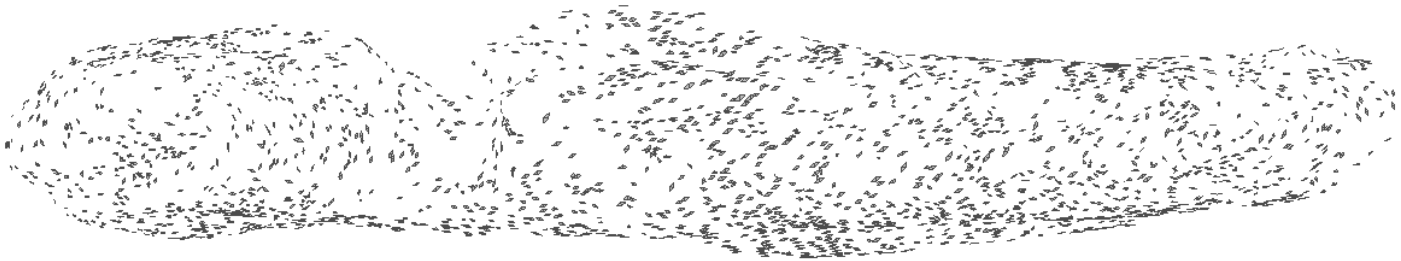
3D Watermarking



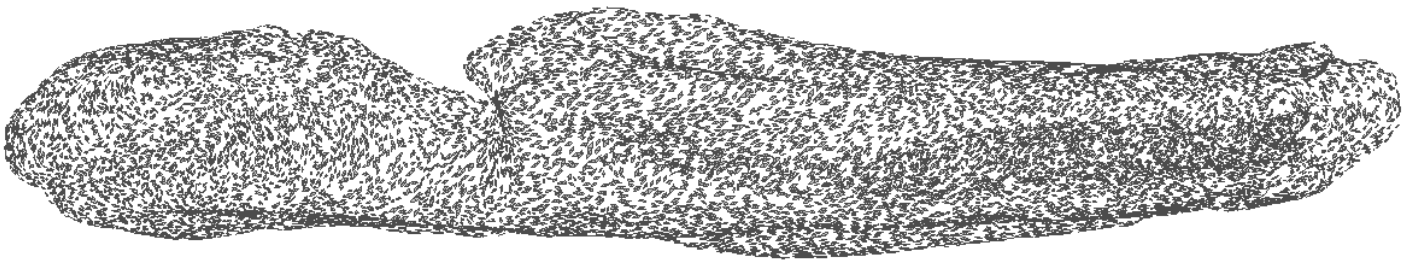
3D Watermarking



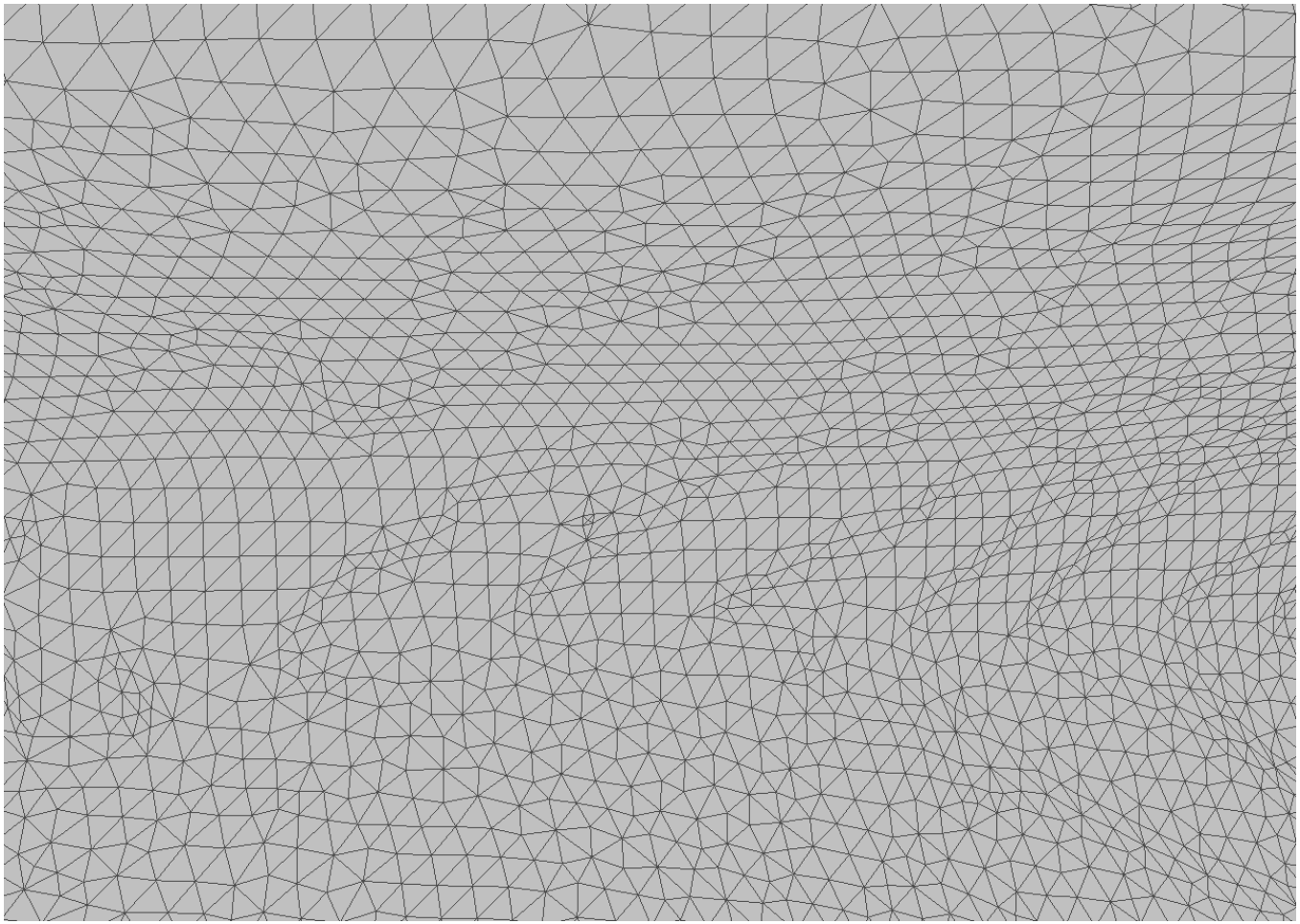
3D Watermarking



3D Watermarking

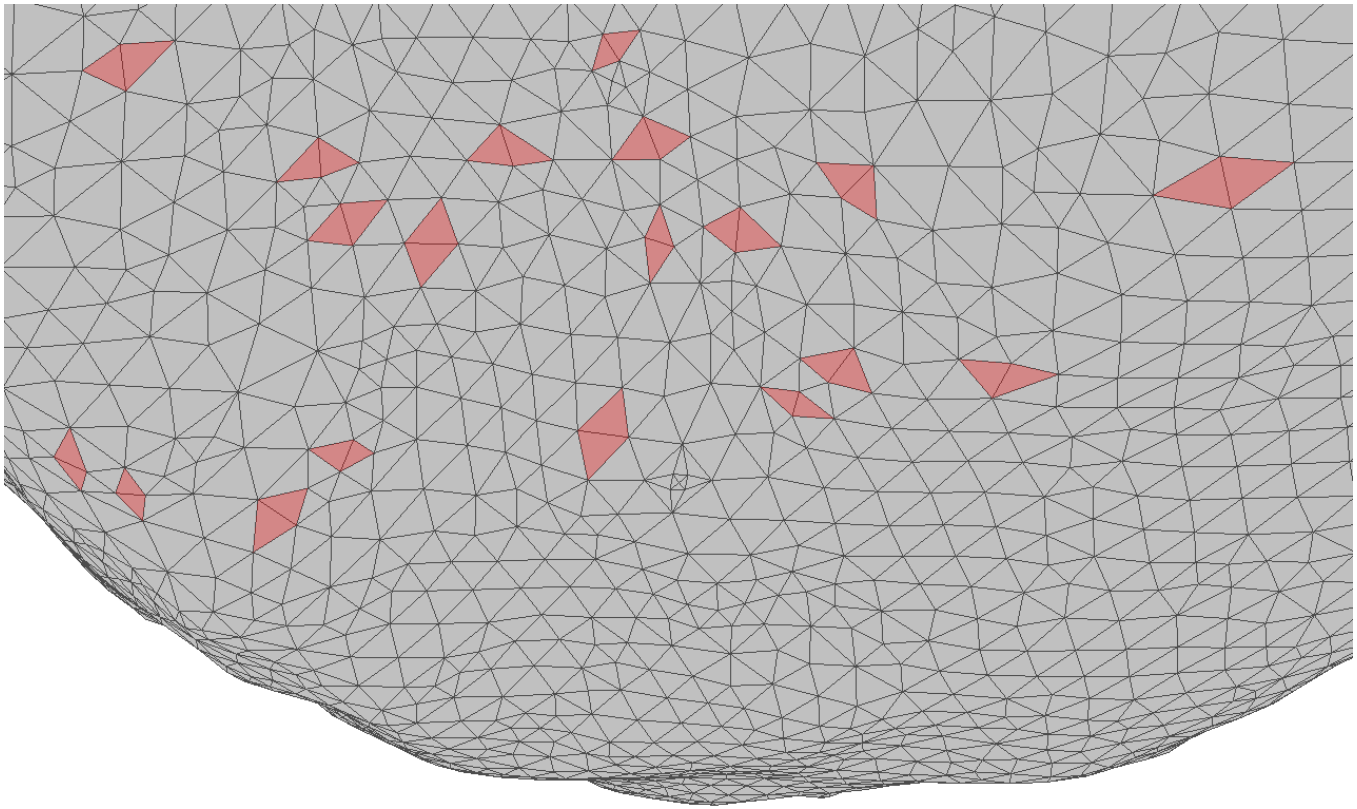


3D Watermarking



3D Watermarking

3D Watermarking



Robust 3D watermarking

References

F. Cayre and B. Macq
Data Hiding on 3D Triangle Meshes
IEEE Transactions on Signal Processing, 2003

Robust 3D watermarking

Algorithm

- Choice of a first triangle ABC,
- Choice of a reference edge AB,
- Divide AB in several parts,
- Associate each part to a 0-bit or a 1-bit,
- Move the vertex C in order to have a projection of C on AB in a wished part.

Robust 3D watermarking

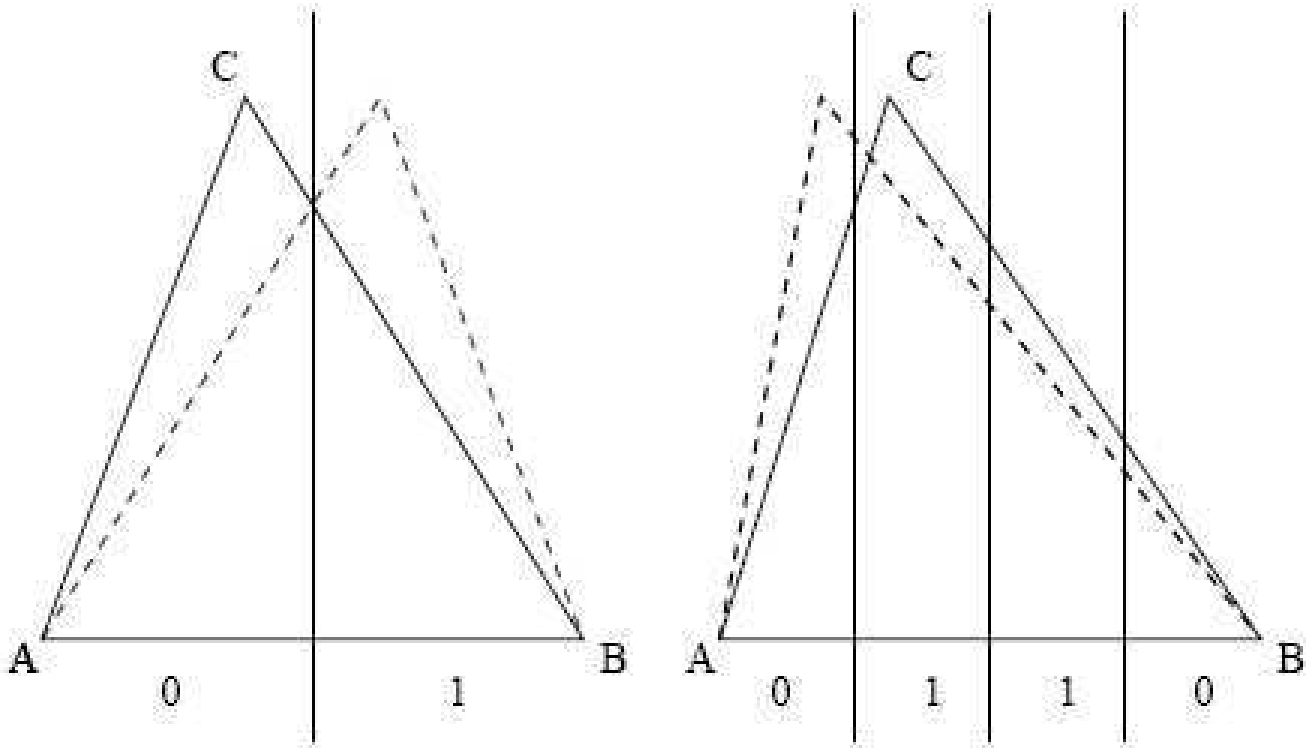


Figure: Overview of the method.

Robust 3D watermarking

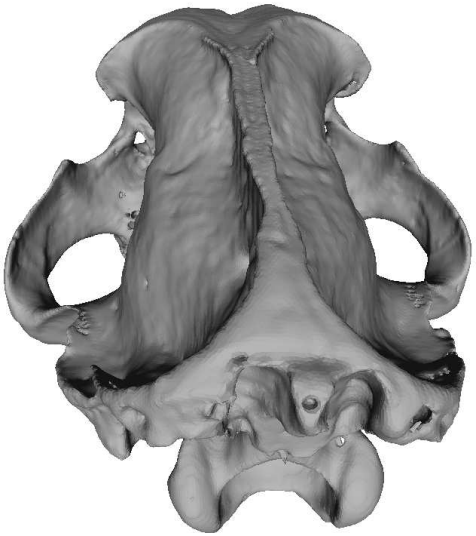
Advantage

- Invisible
- Robust to noise

Inconvenient

- Local

3D Watermarking



(a)

(b)

Figure: a) Original 3D object “Smilodon” 508796 vertices, b) Watermarked 3D object with 314071 bits (= 38.3 kBytes)

Conclusion

- Visual data protection is necessary,
- First proposed methods: *high payload but not robust to noise* or *robust to noise with a small payload*,
- But not robust to cropping for example.

Outline

Conclusions

- Possibility to encrypt a part of the data
- Decreasing of the computation time.
- Scalable protection.
- Variable Length Coding (VLC: stream cipher.
- During the JPEG algorithm:
  - Preservation of the compression rate.
  - Preservation of the JPEG format.
- Visible in Low Resolution (LR) without key or in High Resolution (HR) with the key.

Conclusions

- Possibility to encrypt a part of the data
- Decreasing of the computation time.
- Scalable protection.
- Variable Length Coding (VLC: stream cipher.
- During the JPEG algorithm:
  - Preservation of the compression rate.
  - Preservation of the JPEG format.
- Visible in Low Resolution (LR) without key or in High Resolution (HR) with the key.

Conclusions

- Possibility to encrypt a part of the data
- Decreasing of the computation time.
- Scalable protection.
- Variable Length Coding (VLC: stream cipher.
- During the JPEG algorithm:
  - Preservation of the compression rate.
  - Preservation of the JPEG format.
- Visible in Low Resolution (LR) without key or in High Resolution (HR) with the key.

Conclusions

- Possibility to encrypt a part of the data
- Decreasing of the computation time.
- Scalable protection.
- Variable Length Coding (VLC: stream cipher.
- During the JPEG algorithm:
  - Preservation of the compression rate.
  - Preservation of the JPEG format.
- Visible in Low Resolution (LR) without key or in High Resolution (HR) with the key.

Conclusions

- Possibility to encrypt a part of the data
- Decreasing of the computation time.
- Scalable protection.
- Variable Length Coding (VLC: stream cipher.
- During the JPEG algorithm:
  - Preservation of the compression rate.
  - Preservation of the JPEG format.
- Visible in Low Resolution (LR) without key or in High Resolution (HR) with the key.

- Methods of Image Safe Transfer
  - With stream ciphers
  - Robust to noise
  - Can ensure the integrity
- Cryptanalysis
- Analysis of the noise
- Comparison with modes of AES: synchronous (OFB) and asynchronous (CFB).
- Asymmetric encryption faster than RSA: elliptic curves ?
- Selective Encryption in the wavelet domain


A. Uhl and A. Pommer.
Image and Video Encryption. From Digital Rights Management to Secured Personal Communication
Springer, New York, USA, 2005.

Thank you

Conclusions

- Methods of Image Safe Transfer
  - With stream ciphers
  - Robust to noise
  - Can ensure the integrity
- Cryptanalysis
- Analysis of the noise
- Comparison with modes of AES: synchronous (OFB) and asynchronous (CFB).
- Asymmetric encryption faster than RSA: elliptic curves ?
- Selective Encryption in the wavelet domain

Conclusions

- Possibility to encrypt a part of the data
- Decreasing of the computation time.
- Scalable protection.
- Variable Length Coding (VLC: stream cipher.
- During the JPEG algorithm:
  - Preservation of the compression rate.
  - Preservation of the JPEG format.
- Visible in Low Resolution (LR) without key or in High Resolution (HR) with the key.


A. Uhl and A. Pommer.
Image and Video Encryption. From Digital Rights Management to Secured Personal Communication
Springer, New York, USA, 2005.

Conclusions

- Possibility to encrypt a part of the data
- Decreasing of the computation time.
- Scalable protection.
- Variable Length Coding (VLC: stream cipher.
- During the JPEG algorithm:
  - Preservation of the compression rate.
  - Preservation of the JPEG format.
- Visible in Low Resolution (LR) without key or in High Resolution (HR) with the key.


A. Uhl and A. Pommer.
Image and Video Encryption. From Digital Rights Management to Secured Personal Communication
Springer, New York, USA, 2005.

Conclusions

- Possibility to encrypt a part of the data
- Decreasing of the computation time.
- Scalable protection.
- Variable Length Coding (VLC: stream cipher.
- During the JPEG algorithm:
  - Preservation of the compression rate.
  - Preservation of the JPEG format.
- Visible in Low Resolution (LR) without key or in High Resolution (HR) with the key.


A. Uhl and A. Pommer.
Image and Video Encryption. From Digital Rights Management to Secured Personal Communication
Springer, New York, USA, 2005.

Conclusions

- Possibility to encrypt a part of the data
- Decreasing of the computation time.
- Scalable protection.
- Variable Length Coding (VLC: stream cipher.
- During the JPEG algorithm:
  - Preservation of the compression rate.
  - Preservation of the JPEG format.
- Visible in Low Resolution (LR) without key or in High Resolution (HR) with the key.


A. Uhl and A. Pommer.
Image and Video Encryption. From Digital Rights Management to Secured Personal Communication
Springer, New York, USA, 2005.

Conclusions

- Possibility to encrypt a part of the data
- Decreasing of the computation time.
- Scalable protection.
- Variable Length Coding (VLC: stream cipher.
- During the JPEG algorithm:
  - Preservation of the compression rate.
  - Preservation of the JPEG format.
- Visible in Low Resolution (LR) without key or in High Resolution (HR) with the key.


A. Uhl and A. Pommer.
Image and Video Encryption. From Digital Rights Management to Secured Personal Communication
Springer, New York, USA, 2005.


W. Puech and J.M. Rodrigues.
A New Crypto-Watermarking Method for Medical Images Safe Transfer.
In *Proc. 12th European Signal Processing Conference (EUSIPCO'04)*, pages 1481–1484, Vienna, Austria, 2004.

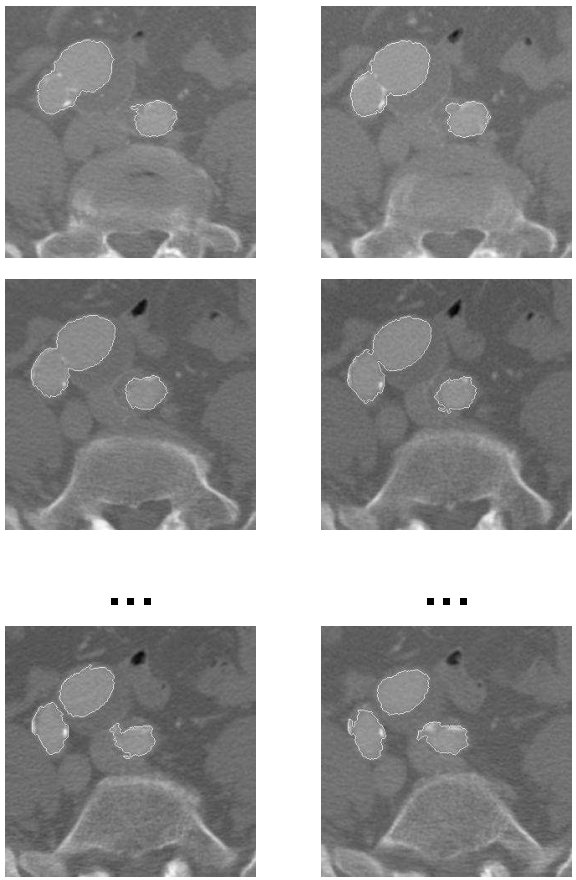

W. Puech, J.M. Rodrigues, and J.E. Develay-Morice.
A New Fast Reversible Method for Image Safe Transfer. Journal of Real-Time Image Processing.
Journal of Real-Time Image Processing (JRTIP), 2(1):55–65, Oct. 2007.

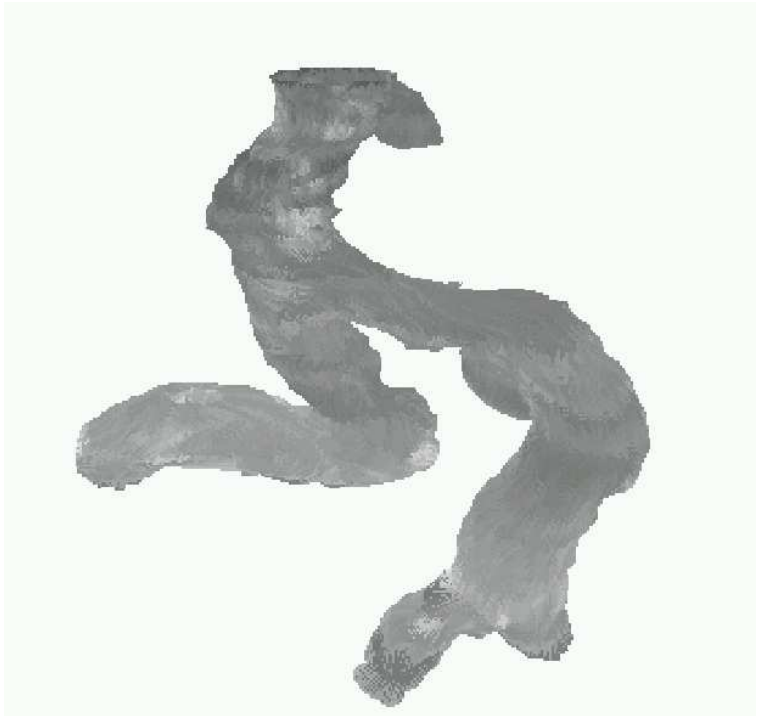
Thank you


W. Puech, M. Chaumont, and O. Strauss.
A Reversible Data Hiding Method for Encrypted Images.
In *Proc. SPIE, Electronic Imaging, Security, Forensics, Steganography, and Watermarking of Multimedia Contents X*, San Jose, CA, USA, January 2008.


W. Puech and G. Coatrieux.
Chapter 10: Coding: Encryption-Watermarking-Compression for Medical Information Security.
Compression of Biomedical Images and Signals, A. Naït-Ali and Christine Cavaro-Menard, Digital Signal Processing, ISTE-Wiley, May 2008.

3D object visualization





Retour

visualisation 3D

K. Djemal, W. Puech and B. Rossetto.
Automatic Active Contours Propagation in a Sequence of Medical Images.
International Journal of Image and Graphics (IJIG), vol. 5(4), 2005.