Crypto-Tatouage et Mojette

Sécurité & Mojette

Florent Autrusseau

IRCCyN-IVC
Polytech'Nantes, University of Nantes

Mojette Day, 4 Fev. 2015

Outline

Outline

Co-auteurs.

- *Jeanpierre Guédon (IRCCyN)*
- *Andrew Kingston (IRCCyN-Univ. Canberra)*
- *Benoit Parrein (IRCCyN)*
- *Myriam Servières (IRCCyN-Cerma)*
- *Junyu Dong (Ocean Univ. China)*
- *Thierry Hamon(IRCCyN-)*
- *Vincent Ricordel (IRCCyN)*
- *Pierre Verbert (IRCCyN)*
- *Pierre Evenou (IRCCyN-Fizians)*
- *Yves Bizais (CHU-Brest-)*
- *Nicolas Normand (IRCCyN)*
- *Patrizio Campisi (Uni Roma 3)*
- *Simone Colosimo (Uni Roma 3-)*
- *Eric Grall (Thales-)*
- ...

Outline

Publications (Sécurité).

- C. Zhang, J. Dong, J. Li, F. Autrusseau, "A New Information Hiding Method for Image Watermarking Based on Mojette Transform", ISNNS, 2010
- A. Kingston, F. Autrusseau, E. Grall, T. Hamon, B. Parrein, "Mojette based security" (chap 10) The Mojette transform: Theory and Applications,wiley, 2009
- A. Kingston, S. Colosimo, P. Campisi, F. Autrusseau, "Lossless Image Compression and Selective Encryption Using a Discrete Radon Transform", IEEE-ICIP 2007
- F. Autrusseau, P. Evenou, T. Hamon, "Secure Distributed Storage based on the Mojette transform", Notere 2006
- F. Autrusseau, JP. Guédon, "Chiffrement Mojette d'images médicales", ISI, Lavoisier, 2003
- F. Autrusseau, JP. Guédon, Y. Bizais, "Watermarking and cryptographic schemes for medical imaging", SPIE Medical Imaging, 2003
- F. Autrusseau, JP. Guédon, "A joint multiple description-encryption image algorithm", ICIP 2003
- F. Autrusseau, JP. Guédon, "Perceptual image watermarking using a secure Mojette transmission scheme", COST 276, 2003
- F. Autrusseau, JP. Guédon, "Image Watermarking in the Fourier Domain Using the Mojette Transform", IEEE-DSP, 2002
- F. Autrusseau, JP. Guédon, "Image watermarking for copyright protection and data hiding via the Mojette transform", SPIE 2002
- F. Autrusseau, "Modélisation Psychovisuelle pour le tatouage des images", Signal and Image processing. Ph. D. Thesis, Université de Nantes, 2002. in French
- JP. Guédon, N. Normand, P. Verbert, B. Parrein, F. Autrusseau, "Load-balancing and scalable multimedia distribution using the Mojette transform", ITCOM, 2001

Outline

Projets financés.

Projets de recherche

- ANR-ARA/SSIA - “Transfert Sécurisé d’images d’art Haute Résolution” (TSAR) - (2005-2008)
- Financement de la Région, bourse post-doctorale (Andrew Kingston) (2007-2008)
- Projet OSEO/Région Miles (2006-2009)

Partenaires

- IRCCyN, IETR, LIRMM, GIPSA-Lab, C2RMF, LINA, IREENA, LERIA, LUIM, LISA, IMN-PCM, LGMPA, LAUM, LSO, UCO2M.

Outline

Thématiques.

La sécurité Mojette

- Le Tatouage
- La Cryptographie
- Le Secret partagé

La crypto

- Crypto-Tatouage
- Crypto-compression

Le Tatouage - Objectifs.

Protection de copyright

- Insertion d'un copyright invisible dans des images
- Robustesse face aux attaques

La Stéganographie

- Transmission de données secrètes
- Invisible et statistiquement non détectable

Le Fingerprinting

- Insertion d'une marque fragile
- Vérification de l'authenticité
- (*Traitor tracing*)

Le Tatouage - Objectifs.

Protection de copyright

- Insertion d'un copyright invisible dans des images
- Robustesse face aux attaques

La Stéganographie

- Transmission de données secrètes
- Invisible et statistiquement non détectable

Le Fingerprinting

- Insertion d'une marque fragile
- Vérification de l'authenticité
- (*Traitor tracing*)

Le Tatouage - Objectifs.

Protection de copyright

- Insertion d'un copyright invisible dans des images
- Robustesse face aux attaques

La Stéganographie

- Transmission de données secrètes
- Invisible et statistiquement non détectable

Le Fingerprinting

- Insertion d'une marque fragile
- Vérification de l'authenticité
- (*Traitor tracing*)

Outline

Tatouage Mojette.

Insertion de fantomes

- Insertion d'un fantome Mojette dans les LSB d'une image.
- Transmission des projections dans lesquelles la marque (le fantome) est invisible
- Transmission des autres projections comme clef de détection

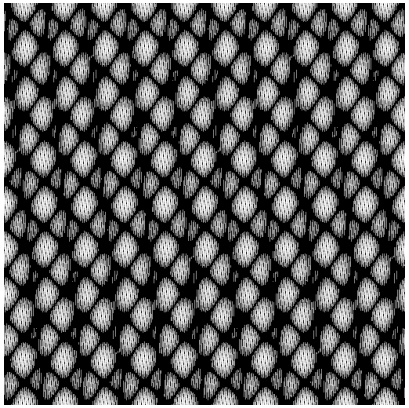
- F. Autrusseau, JP. Guedon, "Image watermarking for copyright protection and data hiding via the Mojette transform", SPIE Electronic Imaging, Security and Watermarking of Multimedia Contents IV, vol. 4675, pp. 378-386, San Jose, CA, January 2002.
- F. Autrusseau, JP. Guedon, "Image Watermarking in the Fourier Domain Using the Mojette Transform", 14th IEEE International Conference on Digital Signal Processing (DSP2002), vol. II, pp. 725-728, Santorini Greece, July 2002.

Tatouage Mojette.

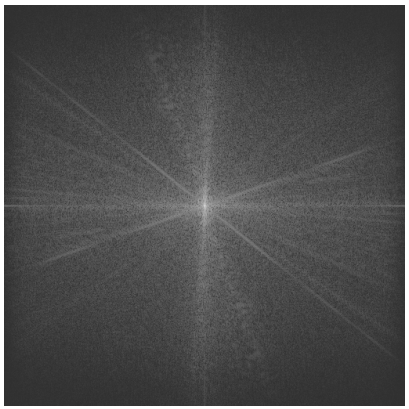
Insertion d'un fantome Mojette dans le spectre de Fourier d'une image

(a) Image Originale

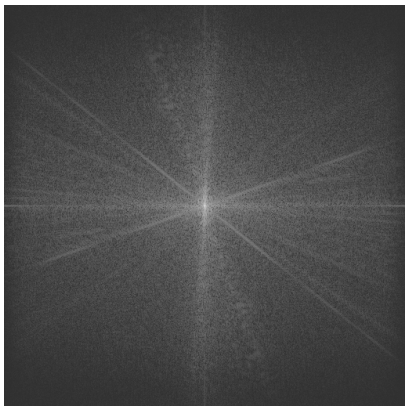
(b) Image tatouée



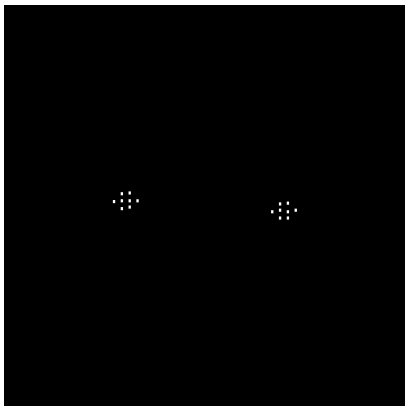
(c) Marque en spatial



(d) Spectre Original



(e) Spectre Tatoué

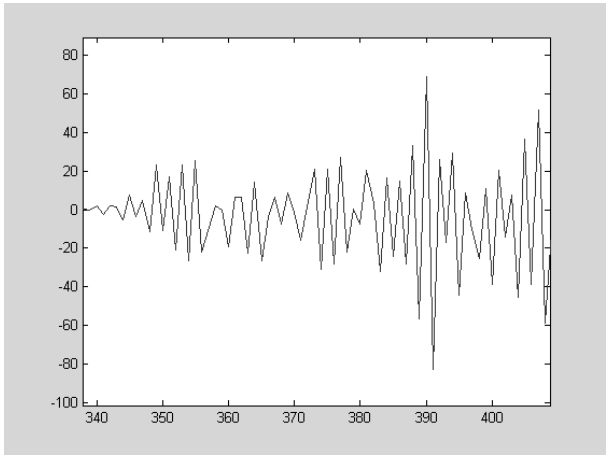


(f) Marque dans Fourier

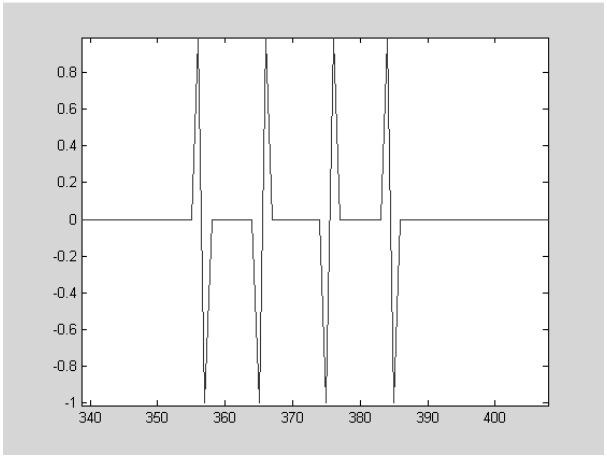
Figure : Tatouage

Tatouage Mojette.

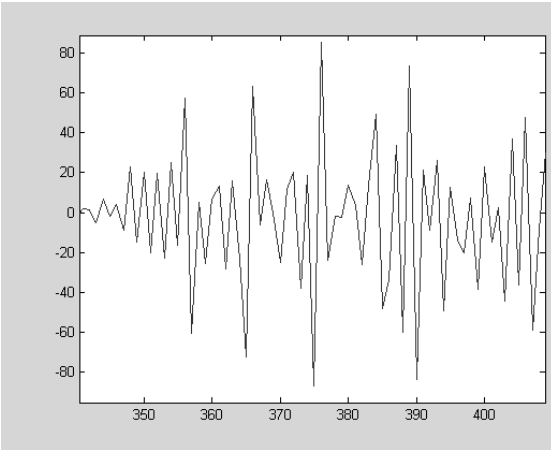
La Mojette est utilisée pour la détection...



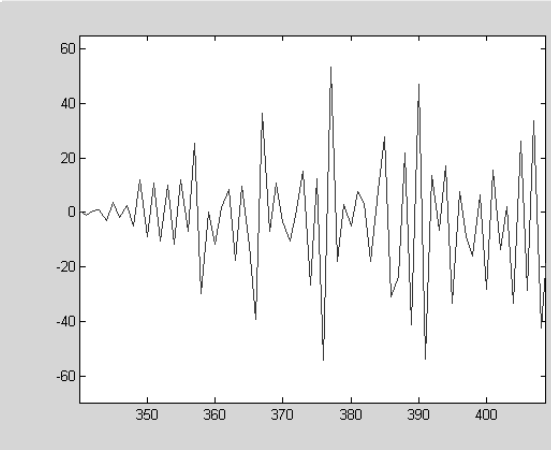
(a) Proj. du Spectre Original



(b) Proj. du fantôme



(c) Proj. du Spectre tatoué



(d) Proj. du Spectre tatoué & attaqué

Figure : Détection du Tatouage

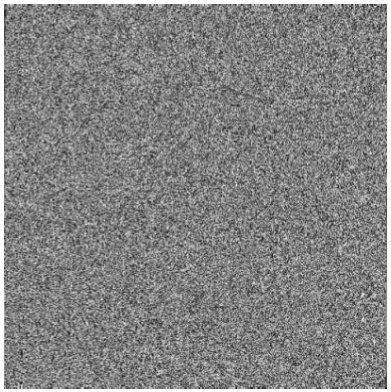
Outline

Crypto-Mojette.

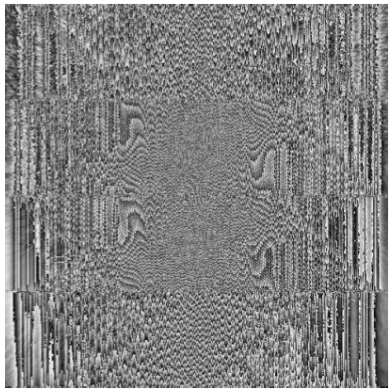
Nous pouvons tirer profit de l'instabilité de la Mojette inverse... (Rétroprojection erronée)

(a) *Modification d'un seul bin.*

(b) *Modification d'un seul bin.*



(c) *Ajout de bruit sur une projection.*



(d) *Ajout de bruit sur une projection (mod256).*

Crypto-Mojette.

Utilisation d'un chemin de reconstruction

- On mémorise la liste des correspondances univoques lors de la MT directe.
- On conserve un chemin unique dans cette liste.
- On brouille (crypte) les bins non utilisés.
- $\rightarrow$ Les données en clair sont noyées dans des données chiffrées

- F. Autrusseau, JP. Guedon, Y. Bizais, "Watermarking and cryptographic schemes for medical imaging", SPIE Medical Imaging, Image processing, vol. 5032-105, pp. 958-965, San Diego CA, USA, 15-20 February 2003.
- F. Autrusseau, JP. Guedon, "A joint multiple description-encryption image algorithm ", IEEE International Conference on Image Processing, ICIP'03, (3), pp. 269-272, Barcelona, Spain, 2003.

Crypto-Mojette.

Chemin de rétro-projection.

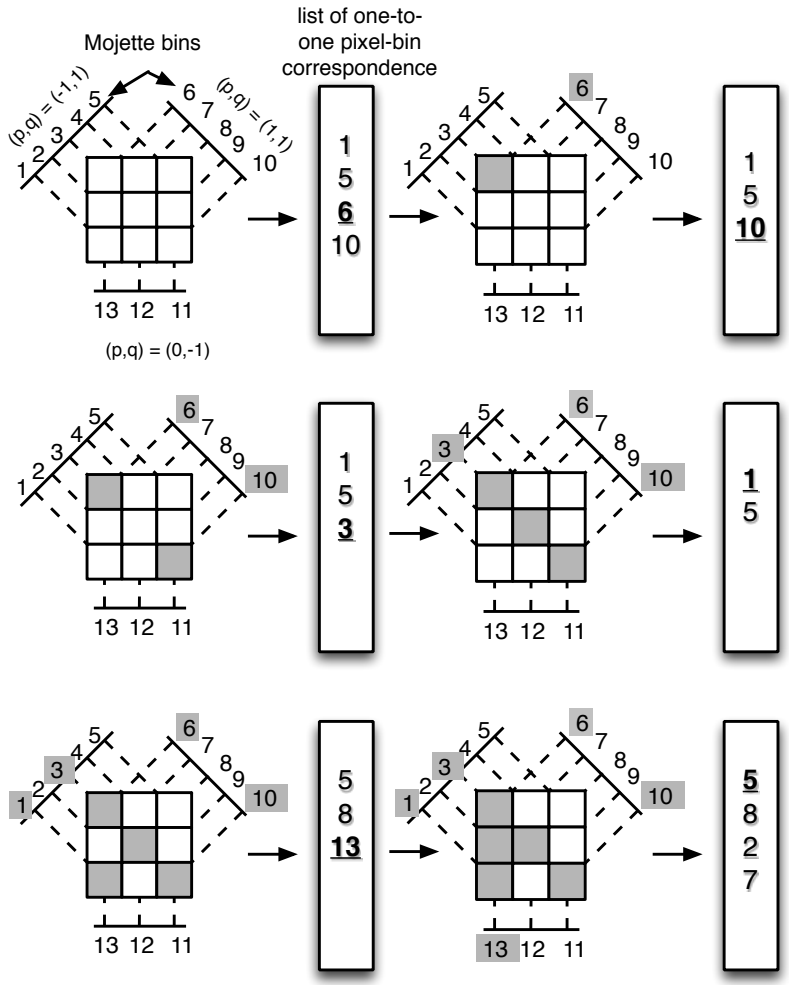


Figure : Crypto

Crypto-Mojette.

Explosion combinatoire, le nombre de chemins possibles augmente très vite.

$$C_n^k = \frac{n!}{k! \times (n-k)!}$$

#bins	19	20	22	23	24	25	30	34
C_n^k	969	4845	74613	2.4^5	7.3^5	2.0^6	1.4^8	2.2^9
Directions	(1,5)	(1,1) (1,3)	(1,6)	(1,2) (1,3)	(1,0) (1,1) (1,3)	(1,7)	(1,1) (1,2) (1,3)	(1,0) (1,1) (1,2) (1,3)
Redundancy	0.187	0.250	0.375	0.437	0.500	0.562	0.875	1.125

Pour une image 4×4 *!*

Outline

Crypto-Compression Mojette.

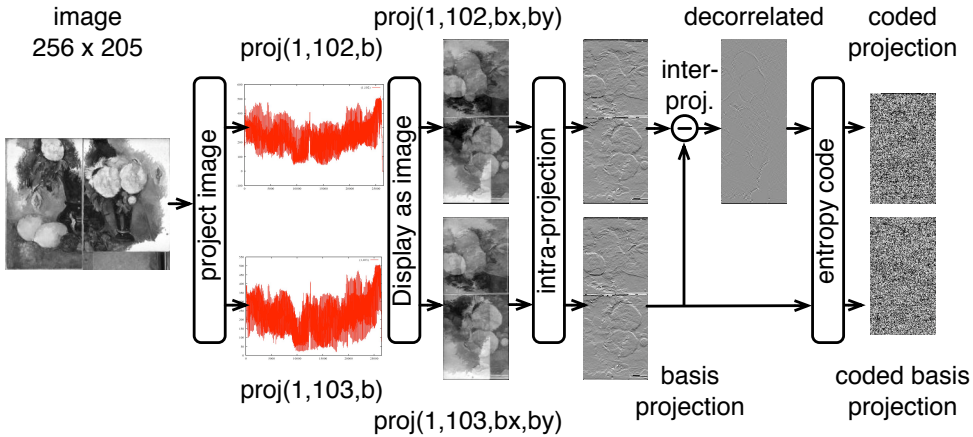
Compression Mojette

- Codage inter-projections
- Codage intra-projection

Codage Inter-projections

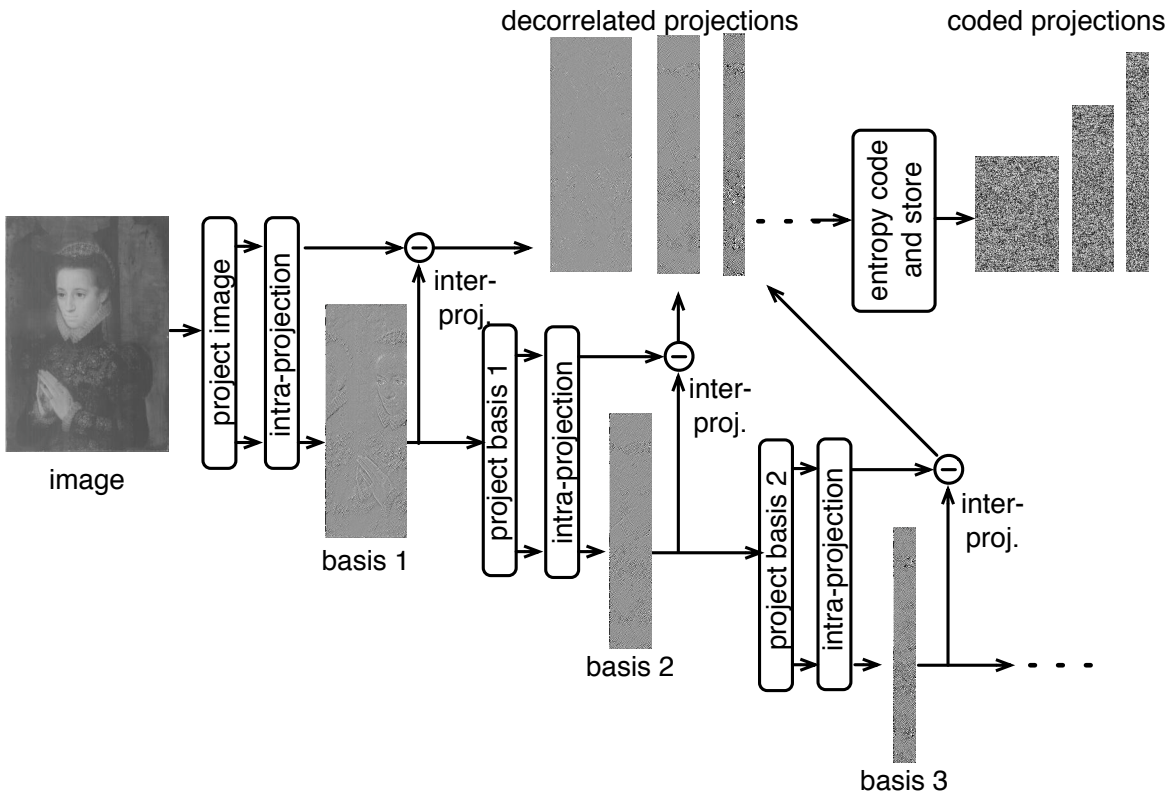
- Projection de base +
- Données décorrélées

Projection de base / projection de différences.



Crypto-Compression Mojette.

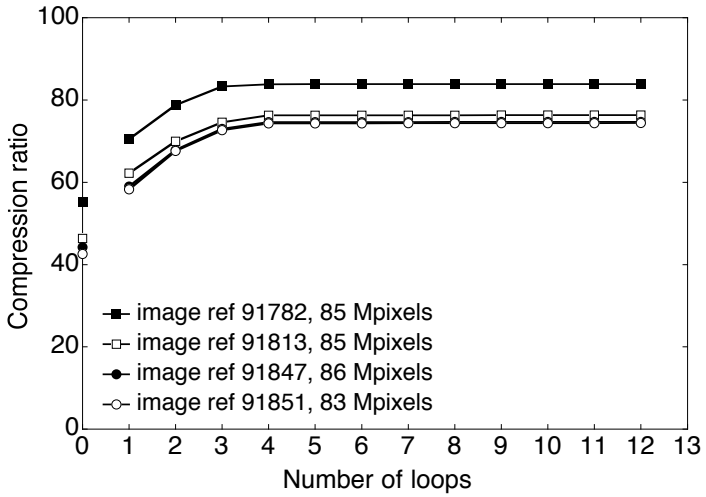
Cascade de projections.

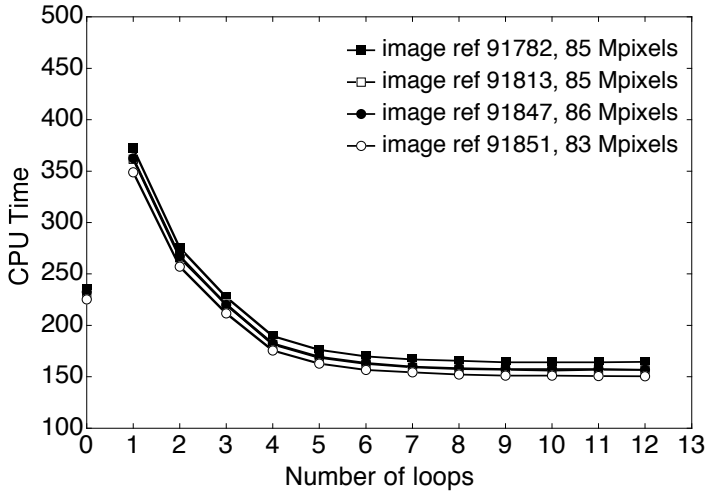


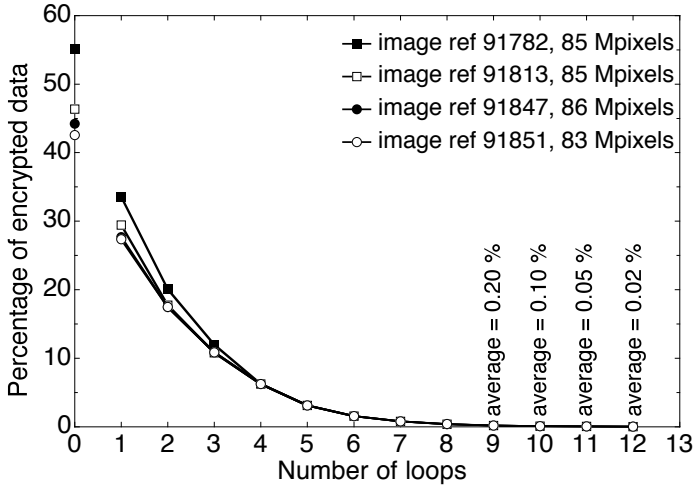
A. Kingston, S. Colosimo, P. Campisi, F. Autrusseau, "Lossless Image Compression and Selective Encryption Using a Discrete Radon Transform", IEEE International Conference on Image Processing, ICIP'07, vol. 4, pp. 465-468, San Antonio, TX, USA, 2007.

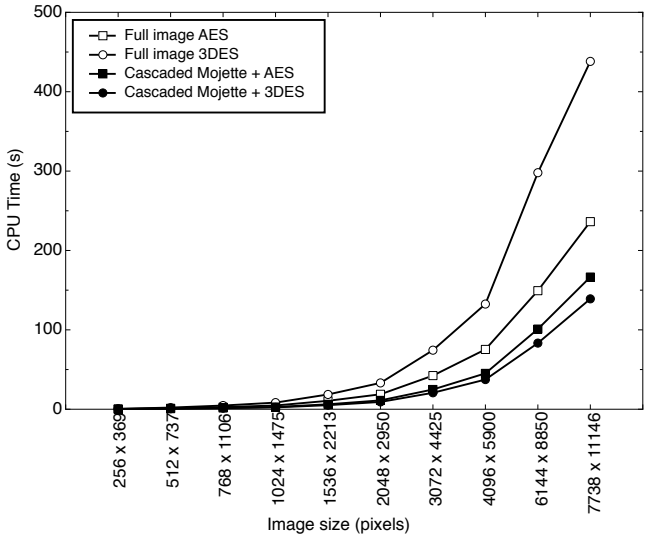
Crypto-Compression Mojette.

Résultats









Conclusion

Conclusion

- Initialement: Travaux sur du tatouage d'images...
- Difficultés pour modifier des projections Mojette et obtenir une reconstruction stable.
- $\rightarrow$ Orientation des travaux vers de la cryptographie.
- Méthodes de chiffrement sélectif efficaces.
- Crypto-compression.
- + Autres travaux sur la crypto (E. Grall & B. Parrein)

TODOs

- Intégration de la crypto dans du stockage distribué (Fizians)
- ...

Conclusion

Conclusion

- Initialement: Travaux sur du tatouage d'images...
- Difficultés pour modifier des projections Mojette et obtenir une reconstruction stable.
- $\rightarrow$ Orientation des travaux vers de la cryptographie.
- Méthodes de chiffrement sélectif efficaces.
- Crypto-compression.
- + Autres travaux sur la crypto (E. Grall & B. Parrein)

TODOs

- Intégration de la crypto dans du stockage distribué (Fizians)
- ...

Références I


J. Dong, L. Su, Y. Zhang, F. Autrusseau, Y. Zhanbin, "Estimating Illumination Direction of 3D Surface Texture Based on Active Basis and Mojette Transform", SPIE-JEI 2013


C. Zhang, J. Dong, J. Li, F. Autrusseau, "A New Information Hiding Method for Image Watermarking Based on Mojette Transform", ISNNS, 2010


A. Kingston, F. Autrusseau, E. Grall, T. Hamon, B. Parrein, "Mojette based security" (chap 10) The Mojette transform: Theory and Applications,wiley, 2009


A. Kingston, F. Autrusseau, "Lossless compression" (chap 9) The Mojette transform: Theory and Applications, wiley, 2009


A. Kingston, F. Autrusseau, B. Parrein, "Multiresolution Mojette transform" (chap 6), The Mojette transform: Theory and Applications, wiley, 2009


A. Kingston, F. Autrusseau, "Lossless Image Compression via Predictive Coding of Discrete Radon Projections", Elsevier SigPro Image, 2008


A. Kingston, B. Parrein, F. Autrusseau, "Redundant Image Representation via Multi-Scale Digital Radon Projection", IEEE-ICIP 2008


P. Jia, J. Dong, L. Qi, F. Autrusseau, "Directionality Measurement and Illumination Estimation of 3D Surface Textures by Using Mojette Transform", IEEE-ICPR 2008


A. Kingston, S. Colosimo, P. Campisi, F. Autrusseau, "Lossless Image Compression and Selective Encryption Using a Discrete Radon Transform", IEEE-ICIP 2007

Références II


F. Autrusseau, P. Evenou, T. Hamon, "Secure Distributed Storage based on the Mojette transform", Notere 2006


F. Autrusseau, B. Parrein, M. Servieres, "Lossless Compression Based on a Discrete and Exact Radon Transform: A Preliminary Study",IEEE-ICASSP 2006


V. Ricordel, F. Autrusseau, W. Dupuy, D. Barba, "1D-mosaics grouping using lattice vector quantization for a video browsing application", CBMI 2005


F. Autrusseau, JP. Guédon, "Chiffrement Mojette d'images médicales", ISI, Lavoisier, 2003


F. Autrusseau, JP. Guédon, Y. Bizais, "Watermarking and cryptographic schemes for medical imaging", SPIE Medical Imaging, 2003


F. Autrusseau, JP. Guédon, "A joint multiple description-encryption image algorithm", ICIP 2003


F. Autrusseau, JP. Guédon, "Perceptual image watermarking using a secure Mojette transmission scheme", COST 276, 2003


F. Autrusseau, JP. Guédon, "Image Watermarking in the Fourier Domain Using the Mojette Transform", IEEE-DSP, 2002


F. Autrusseau, JP. Guédon, "Image watermarking for copyright protection and data hiding via the Mojette transform", SPIE 2002

Références III

F. Autrusseau, "Modélisation Psychovisuelle pour le tatouage des images", Ph. D. Thesis, U. Nantes, 2002.

JP. Guédon, N. Normand, P. Verbert, B. Parrein, F. Autrusseau, "Load-balancing and scalable multimedia distribution using the Mojette transform", ITCOM, 2001