Encryption, Watermarking and Mojette

Security & Mojette

Florent Autrusseau

IRCCyN-IVC
Polytech'Nantes, University of Nantes

Mojette Day, 4 Feb. 2015

Outline

Outline

Co-authors.

- *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 (Security).

- 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

Funded Projects.

Research Projects

- ANR-ARA/SSIA - “Transfert Sécurisé d’images d’art Haute Résolution” (TSAR) - (2005-2008)
- Funding from Région Pays de la Loire, postdoctoral position (Andrew Kingston) (2007-2008)
- OSEO/Région Project - Miles (2006-2009)

Partners

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

Outline

Topics.

Mojette-based security

- Watermarking
- Encryption
- Shared secret

Encryption

- Encryption+watermarking
- Encryption+coding

Watermarking - goals.

Protection de copyright

- Embed an invisible copyright within images
- Robustness against attacks

Steganography

- Transmit secret data
- Invisible and statistically not detectable

Fingerprinting

- Embed a fragile watermark
- Check Authenticity
- *Traitor tracing*

Watermarking - goals.

Protection de copyright

- Embed an invisible copyright within images
- Robustness against attacks

Steganography

- Transmit secret data
- Invisible and statistically not detectable

Fingerprinting

- Embed a fragile watermark
- Check Authenticity
- *Traitor tracing*

Watermarking - goals.

Protection de copyright

- Embed an invisible copyright within images
- Robustness against attacks

Steganography

- Transmit secret data
- Invisible and statistically not detectable

Fingerprinting

- Embed a fragile watermark
- Check Authenticity
- *Traitor tracing*

Outline

Mojette-based watermarking.

Embed ghosts

- Embed Mojette ghosts onto the image's LSB planes.
- Transmit Mojette projections for which the ghost is invisible.
- Transmit other projections as a detection key.

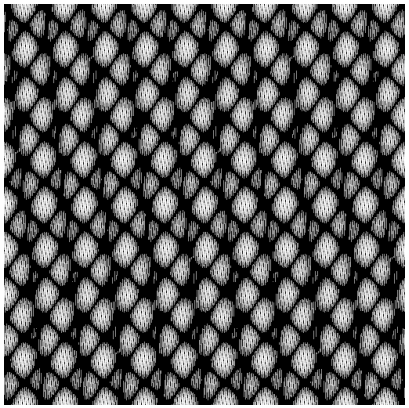
- F. Autrusseau, JP. Guedon, "Image watermarking for copyright protection and data hiding via the Mojette transform", SPIE Electronic Imaging, Security and Watermarking of Multimedia Contents IV, vol. 4675, pp. 378-386, San Jose, CA, January 2002.
- F. Autrusseau, JP. Guedon, "Image Watermarking in the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

Mojette-based watermarking.

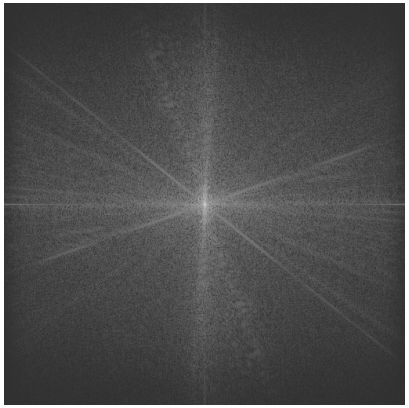
Embed a Mojette ghost within the Fourier spectrum.

(a) Original Image

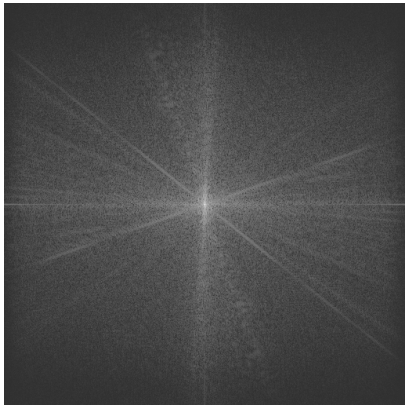
(b) Marked Image



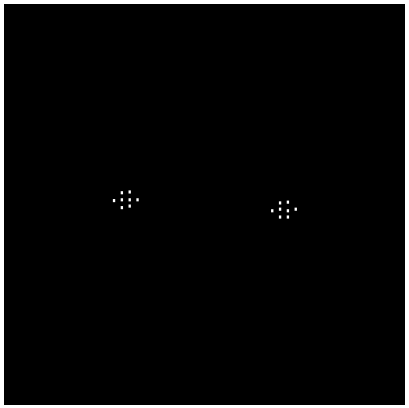
(c) Spatial watermark



(d) Original Spectrum



(e) Marked spectrum

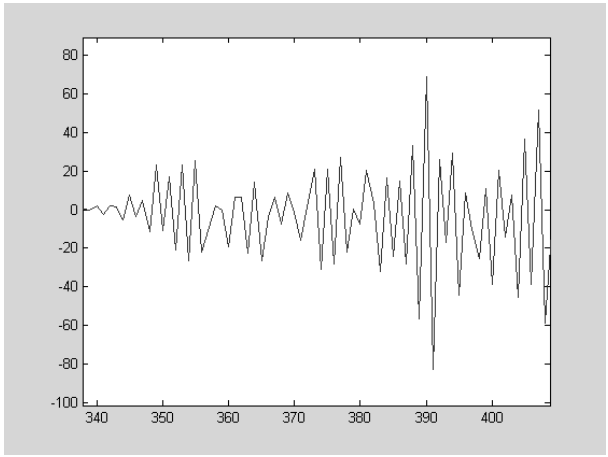


(f) Watermark in Fourier space

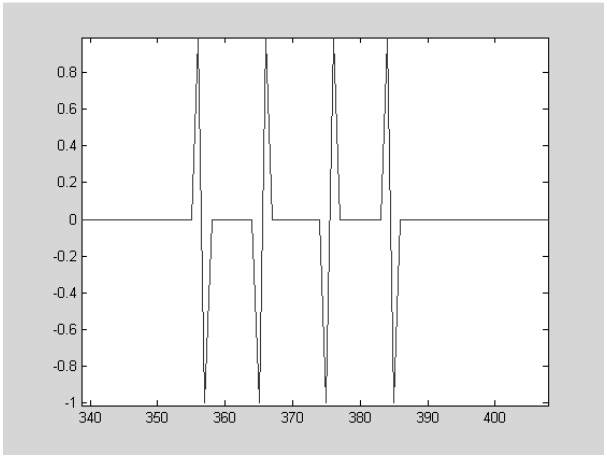
Figure : Watermarking

Mojette-based watermarking.

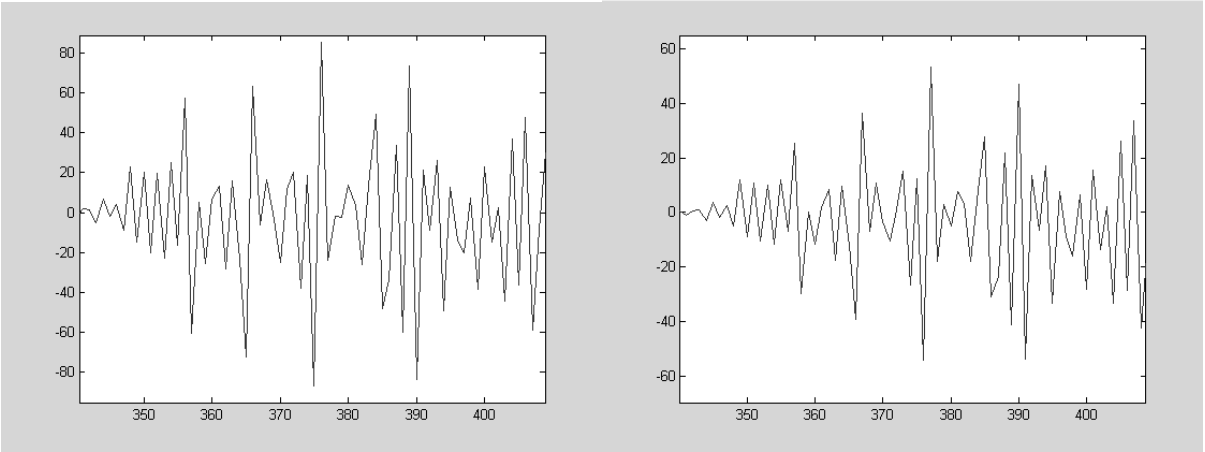
The Mojette transform is used for the detection...



(a) Proj. of the Original spectrum



(b) Proj. of the ghost



(c) Proj. of the marked spectrum (d) Proj. marked & attacked spectrum

Figure : Watermark Detection

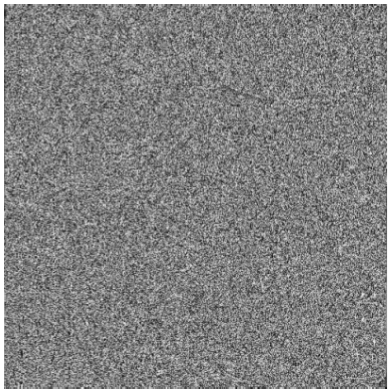
Outline

Mojette encryption.

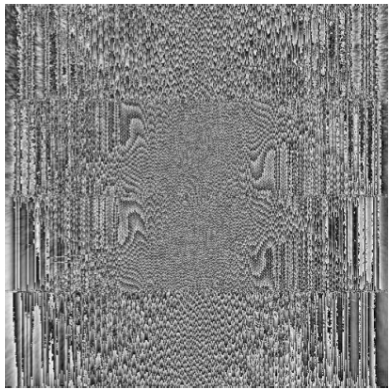
We can take benefit from the inverse Mojette instability... (erroneous projections backprojection)

(a) *One single modified bin.*

(b) *One single modified bin.*



(c) *Noise addition onto one proj.*



(d) *Noise addition onto one proj. (mod256).*

Mojette encryption.

Use a reconstruction path

- We keep track of the 1 to 1 (bin to pixel) correspondences during the direct MT.
- Store a unique path.
- Encrypt unused bins.
- $\rightarrow$ The original data is mixed with encrypted data

- 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.

Mojette encryption.

Backprojection path.

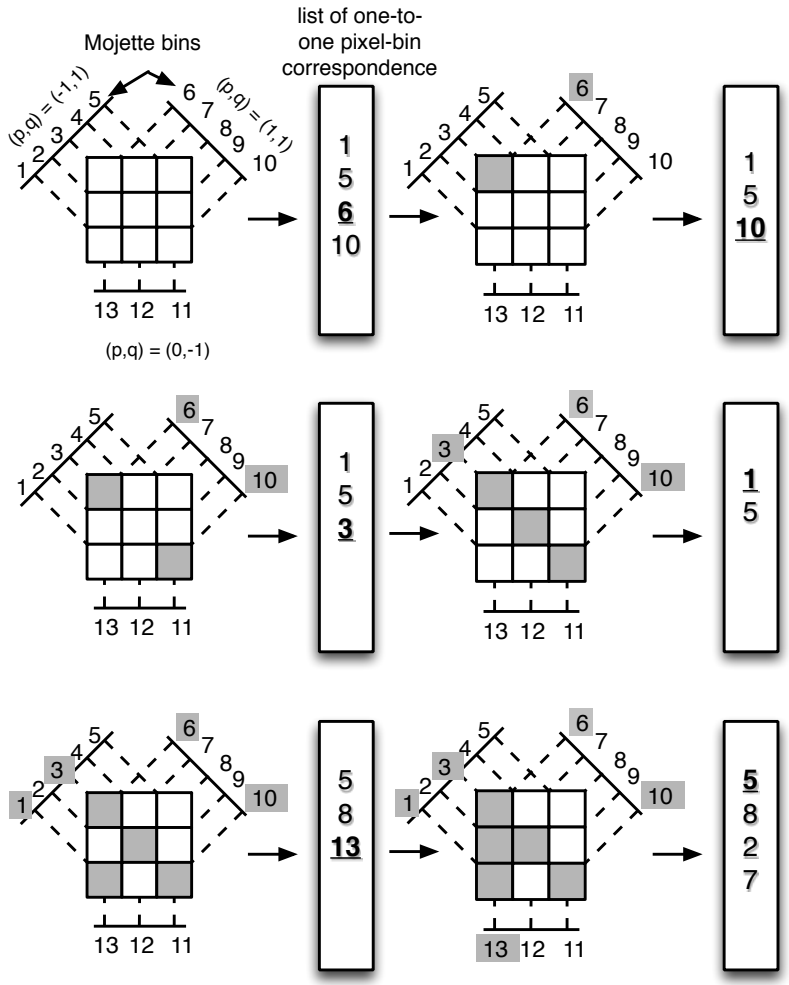


Figure : Encryption

Mojette encryption.

The number of possible paths significantly increases.

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

#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

For a 4×4 ! image

Outline

Encryption+Coding with the Mojette.

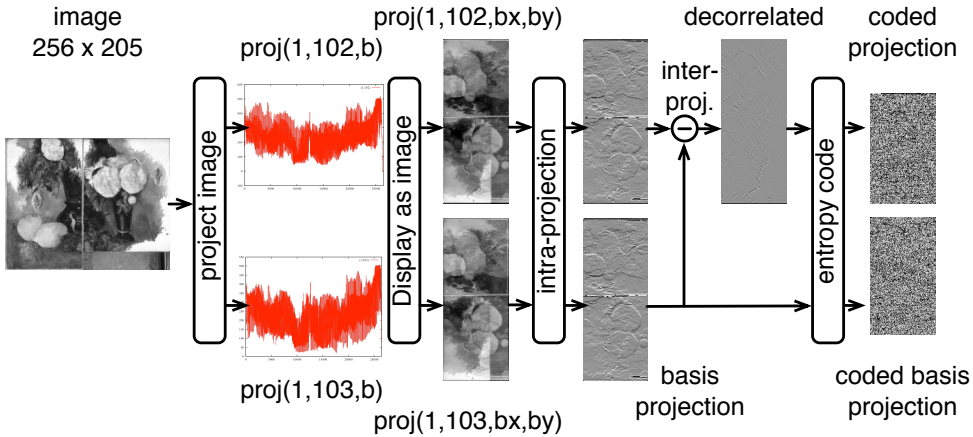
Encryption+Coding with the Mojette

- Inter-projections coding
- Intra-projections coding

Inter-projections coding

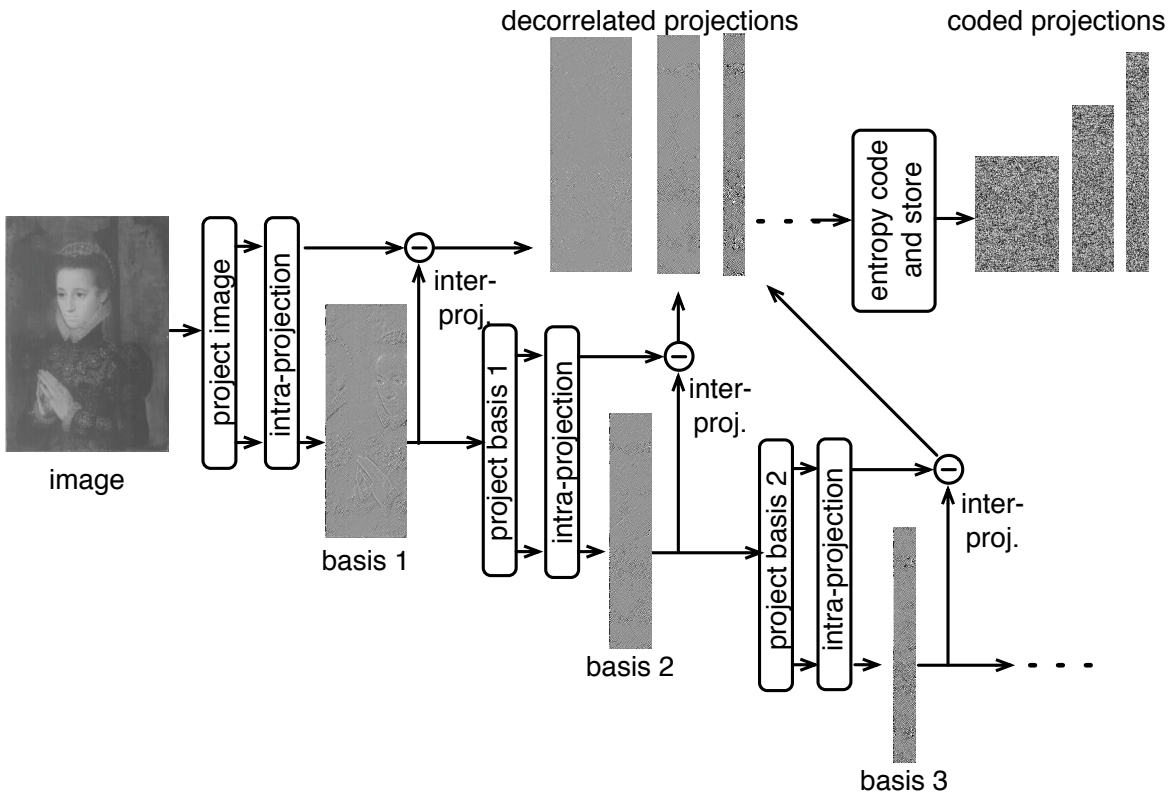
- Basis Projection +
- Uncorrelated data

Basis Projection / difference projection.



Encryption+Coding with the Mojette.

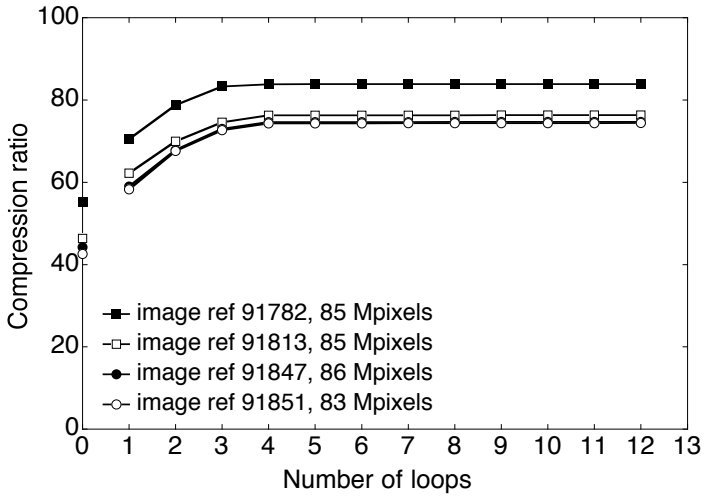
A cascade of projections.

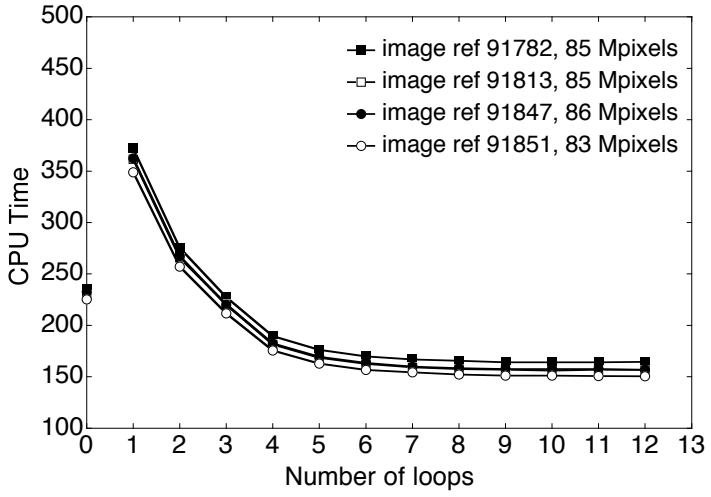


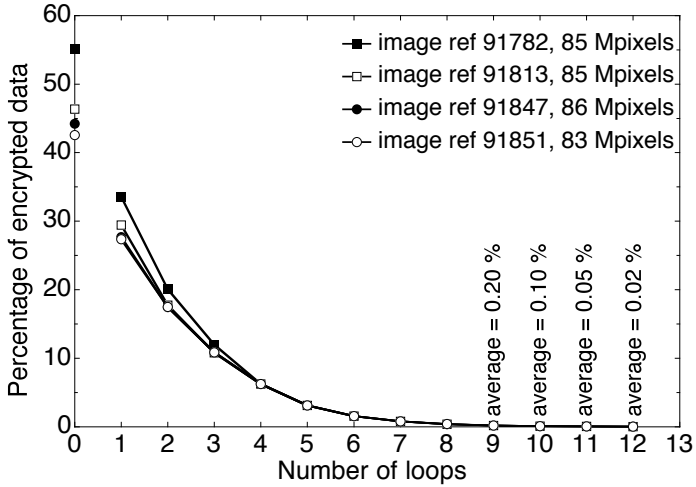
A. Kingston, S. Colosimo, P. Campisi, F. Autrusseau, "Lossless Image Compression and Selective Encryption Using a Discrete Radon Transform", IEEE International Conference on Image Processing, ICIP'07, vol. 4, pp. 465-468, San Antonio, TX, USA, 2007.

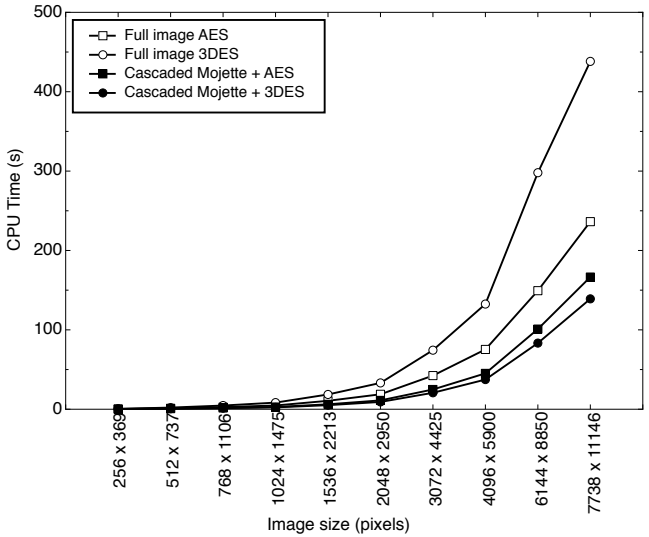
Encryption+Coding with the Mojette.

Results









Conclusion

Conclusion

- Initially: image watermarking...
- Encountered some issues to watermark the bins, obtain a stable reconstruction and offer sufficient robustness.
- $\rightarrow$ Let's do some encryption.
- Efficient selective encryption methods..
- Encryption+coding.
- + Some other works on Mojette encryption (E. Grall & B. Parrein)

TODOs

- Use Mojette encryption in a distributed storage framework (Fizians)
- ...

Conclusion

Conclusion

- Initially: image watermarking...
- Encountered some issues to watermark the bins, obtain a stable reconstruction and offer sufficient robustness.
- $\rightarrow$ Let's do some encryption.
- Efficient selective encryption methods..
- Encryption+coding.
- + Some other works on Mojette encryption (E. Grall & B. Parrein)

TODOs

- Use Mojette encryption in a distributed storage framework (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