Le tatouage robuste aux désynchronisations

Marc Chaumont

10 mars 2009

Plan

1 Préambule

2 Les attaques désynchronisantes

3 Synchronisation par détection non aveugle

4 Recherche exhaustive

5 Tatouage invariant (espace invariant)

6 Pattern de synchronisation

7 Synchronisation implicite (tatouage basée contenu) ; Tatouage de seconde génération

8 Conlusion - Pistes

Références utilisées + remarques

- Livre **"Digital Watermarking and Steganography"**, I. Cox, M. Miller, J. Bloom, J. Fridrich, et T. Kalker, Nov. 2007, 2^{eme} édition,
- Transparents **"Resynchronisation techniques in watermarking"**, P. Bas, école ECRYPT, Septembre 2007, Grèce, + Livre "**Tatouage de documents audiovisuels numériques**", Traité IC2, 2003.
- Article (70 pages) **"A Survey of RST Invariant Image Watermarking Algorithms"**, D. Zheng, Y. Liu, J. Zhao, et A. el Saddik, ACM Computing Surveys, juin 2007.

- La plupart des *schémas* sont extraits de [Zheng et al. 2007]
- La plupart des techniques de tatouages sont non informées (simple étalement de spectre).

Rappel du problème

Image tatouée
(insertion d'un message)

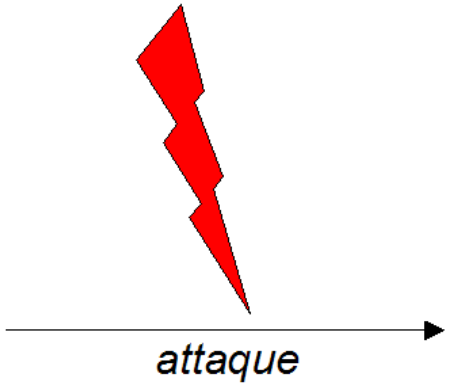
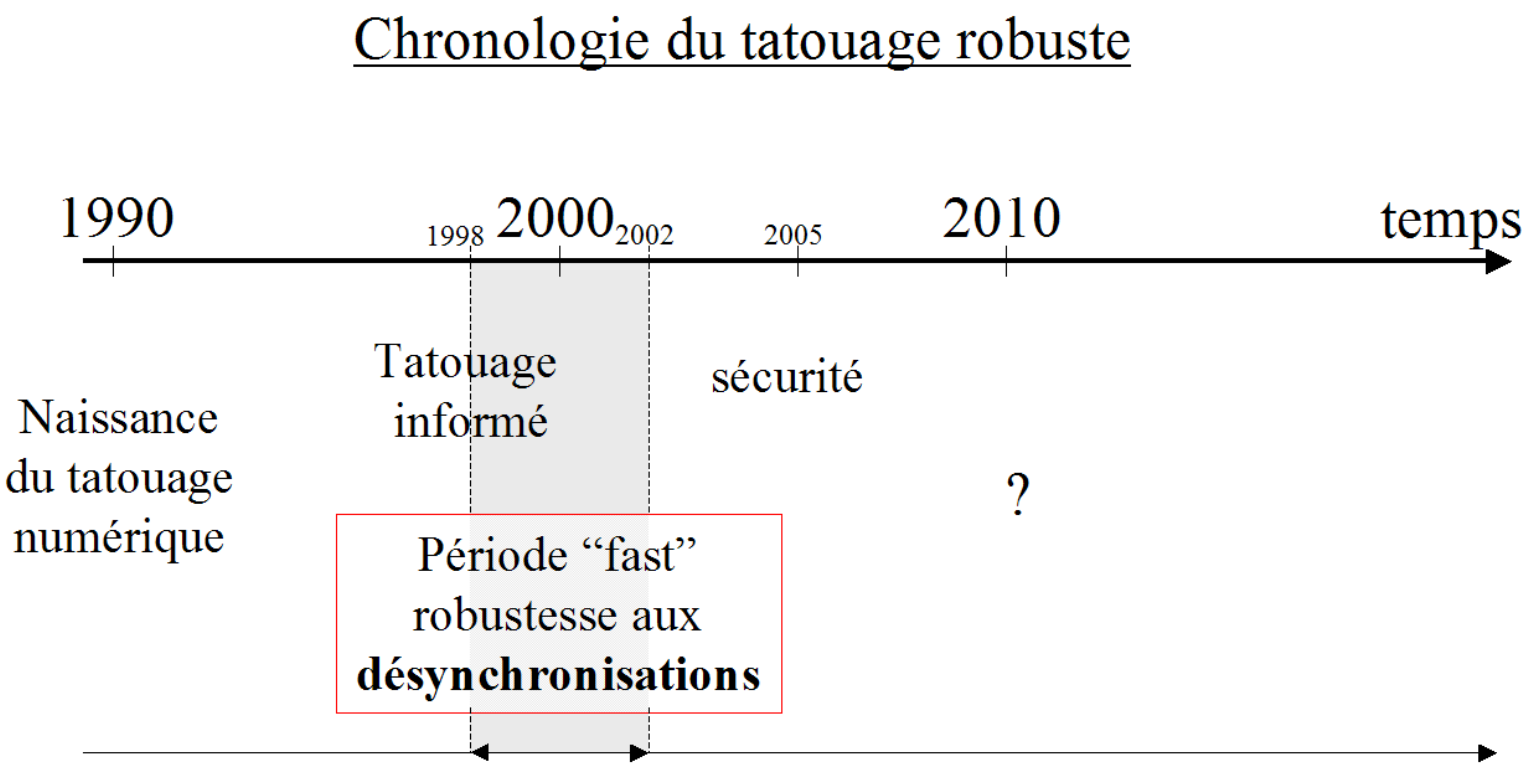


Image attaquée

… le message peut-il être extrait ?

Un peu d'histoire



Constat

Bon système de tatouage = système robuste aux désynchronisations.

Les schémas de tatouage : Broken Arrows, QIM, SCS, DPTC ... ne sont pas robustes aux attaques désynchronisantes (de bonne qualité psychovisuelle).

Un schéma sûr et robuste aux désynchronisations et à détection aveugle : **le Saint Graal ?**

Plan

1 Préambule

2 Les attaques désynchronisantes

3 Synchronisation par détection non aveugle

4 Recherche exhaustive

5 Tatouage invariant (espace invariant)

6 Pattern de synchronisation

7 Synchronisation implicite (tatouage basée contenu) ; Tatouage de seconde génération

8 Conlusion - Pistes

Quelques distortions géométriques

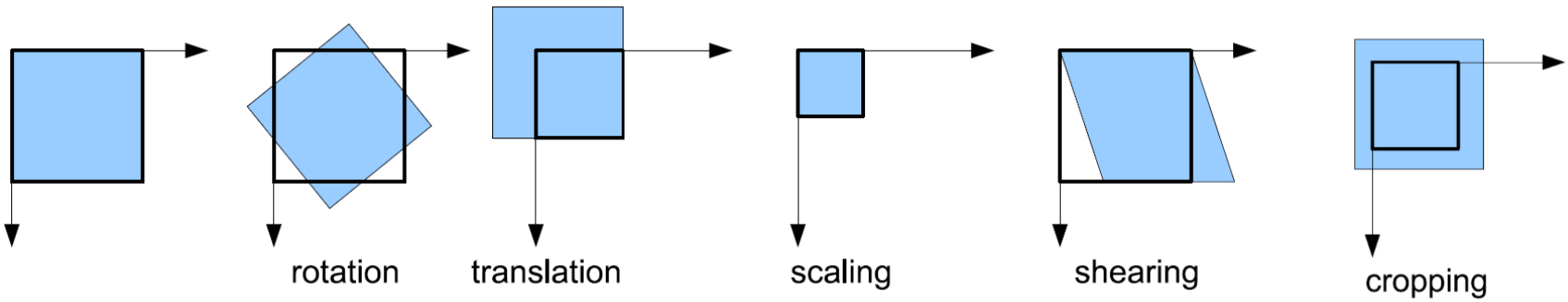


Fig.: Différentes déformations

Modèle de déformation affine

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_o \\ y_o \end{pmatrix} + \begin{pmatrix} t_x \\ t_y \end{pmatrix}$$

scaling	:	$\begin{pmatrix} s_x & 0 \\ 0 & s_y \end{pmatrix}$
rotation d'angle θ	:	$\begin{pmatrix} cos(\theta) & -sin(\theta) \\ sin(\theta) & cos(\theta) \end{pmatrix}$
étirement suivant x	:	$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$
étirement suivant y	:	$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$

Il existe également des modèles plus complexes (perspective, warping, ...).

Stirmark

Fig.: Illustration de l'attaque de type print & scan de stirmark

Les 5 grandes familles

Les différentes approches de tatouage robuste aux désynchronisations :

- tatouage à détection non aveugle (détecteur non aveugle),
- recherche exhaustive,
- tatouage invariant (espace invariant),
- synchronisation ou recalage (pattern de syncho),
- synchronisation implicite (tatouage basé contenu)

Plan

1 Préambule

2 Les attaques désynchronisantes

3 Synchronisation par détection non aveugle

4 Recherche exhaustive

5 Tatouage invariant (espace invariant)

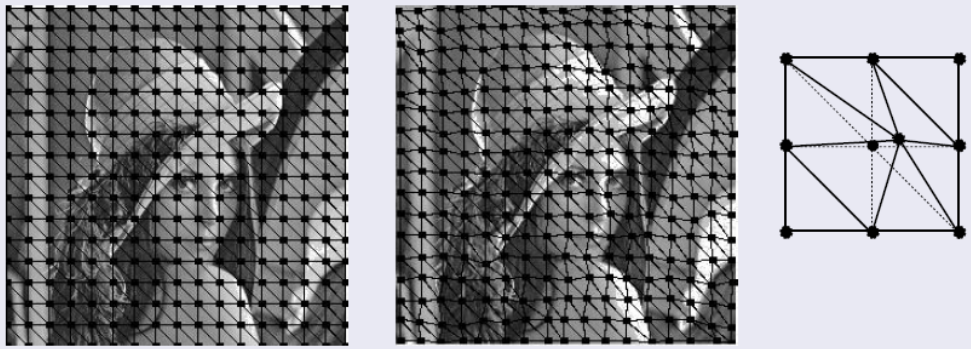
6 Pattern de synchronisation

7 Synchronisation implicite (tatouage basée contenu) ; Tatouage de seconde génération

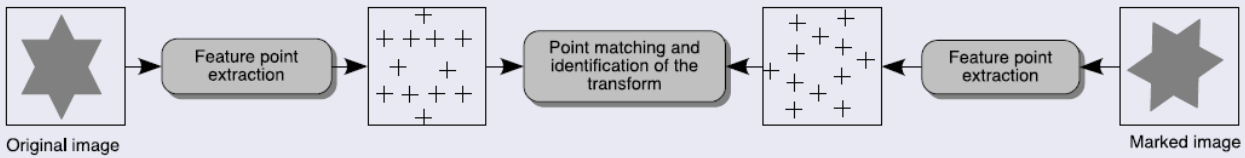
8 Conlusion - Pistes

Synchronisation par détection non aveugle

Geometrical compensation using a Tessellation



Geometrical compensation using a feature points



Plan

1 Préambule

2 Les attaques désynchronisantes

3 Synchronisation par détection non aveugle

4 Recherche exhaustive

5 Tatouage invariant (espace invariant)

6 Pattern de synchronisation

7 Synchronisation implicite (tatouage basée contenu) ; Tatouage de seconde génération

8 Conlusion - Pistes

Recherche exhaustive

- Solution 1 : appliquer un grand nombre de distortions inverses et lancer le détecteur,
- Solution 2 : appliquer un grand nombre de distortions inverses sur le pattern et lancer le détecteur,

On se limite ici à des distortions réalistes et également à des distortions qui maintiennent la marque présente.

Exemple de distortions acceptables

Main class of introduced distortions (for peceptual hash) to be robust to :

- analog-to-digital conversion,
- geometrical transformations (rotation (up to 10 degrees), translation, shearing (up to 10 %)),
- averaging filtering (up to 5×5 window),
- median filtering (up to 5×5 window),
- lossy compression (JPEG),
- additive noise (uniform on $[-0.5; 0.5]$, AWGN with variance below 3).

Oleksiy Koval, ECRYPT Summer School on Multimedia Security, Thessalonici, Greece, September 24-27 2007.

Problèmes

La solution par recherche exhaustive pose trois problèmes :

- Il y a un grand nombre d'applications du détecteur,
- Toutes les attaques ne sont pas forcément répertoriées (ou testées) par le détecteur,
- Si p_{fp} est la probabilité de faux positif. Après N détections par le détecteur, la probabilité d'avoir un faux positif parmi les N détections est bornée par $N \times p_{fp}$. Quand N est grand, cette probabilité devient inacceptable.

Plan

1 Préambule

2 Les attaques désynchronisantes

3 Synchronisation par détection non aveugle

4 Recherche exhaustive

5 Tatouage invariant (espace invariant)

6 Pattern de synchronisation

7 Synchronisation implicite (tatouage basée contenu) ; Tatouage de seconde génération

8 Conlusion - Pistes

Rappel sur Fourier

Soit la fonction $x_\tau(t) = x(t-\tau)$.
Sa transformée de Fourier est :

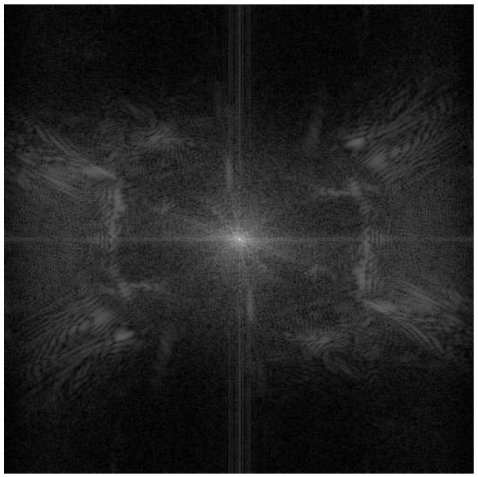
$$\begin{aligned} X_\tau(\omega) &= \int_{-\infty}^{\infty} x(t-\tau)\exp(-j\omega t)dt \\ &= exp(j\omega\tau)\int_{-\infty}^{\infty} x(t)\exp(-j\omega t)dt \\ &= \exp(-j\omega\tau)X(\omega) \end{aligned}$$

La **translation** dans le domaine temporel **ne modifie pas le module de la transformée de Fourier** ; Il y a juste un déphasage linéaire en fonction de la fréquence (terme $\exp(-j\omega t)$).

Illustration sur l'image Barbara

Barbara

Translation 100 pixels



Même module DFT

Rappel sur le Log-Polar Mapping

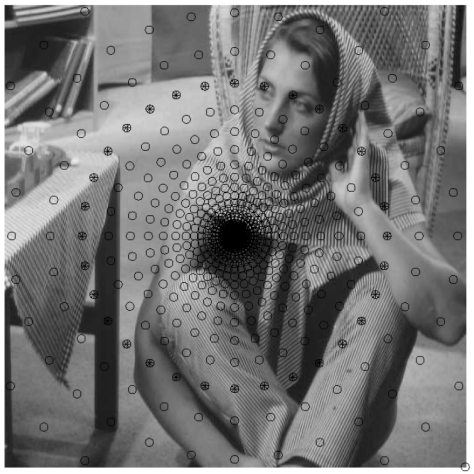
Le changement de repère d'un point (u,v) exprimé dans le repère Cartésien en un point (ρ, θ) exprimé dans le repère log-polaire est tel que :

$$\rho = ln(\sqrt{u^2 + v^2}), \quad (1)$$

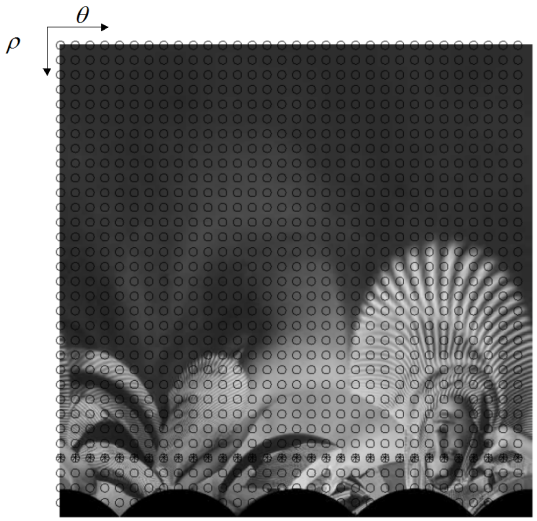
$$\theta = tan^{-1}\left(\frac{u}{v}\right), \quad (2)$$

avec $\rho \in \mathbb{R}$ et $\theta \in [0, 2\pi[$ On appelera ce changement de repère le Log-Polar Mapping : LPM.

Illustration sur l'image Barbara



Point échantillonage



LPM

inverse LPM

Espace invariant : Fourier Mellin [O'Ruanaidh and Pun 1998]

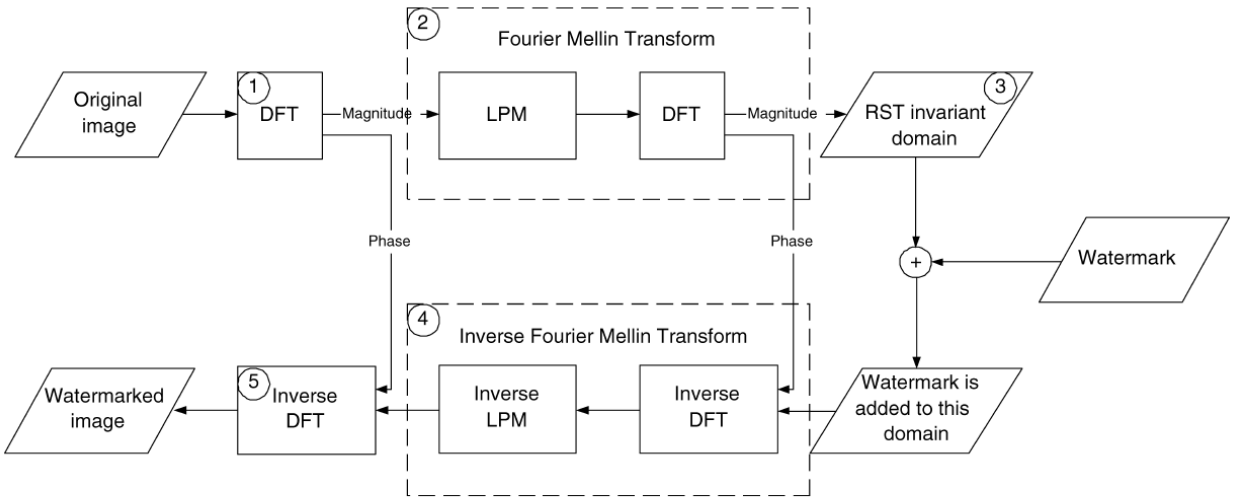


Fig. 9. Embedding watermark in Fourier–Mellin domain.

- DFT : invariance aux translations du module de Fourier
- LPM : rotation et scaling transformés en translation dans le repère log-polaire

Espace invariant : Fourier Mellin [O'Ruanaidh and Pun 1998]

Extraction dans le domaine de Fourier-Mellin.

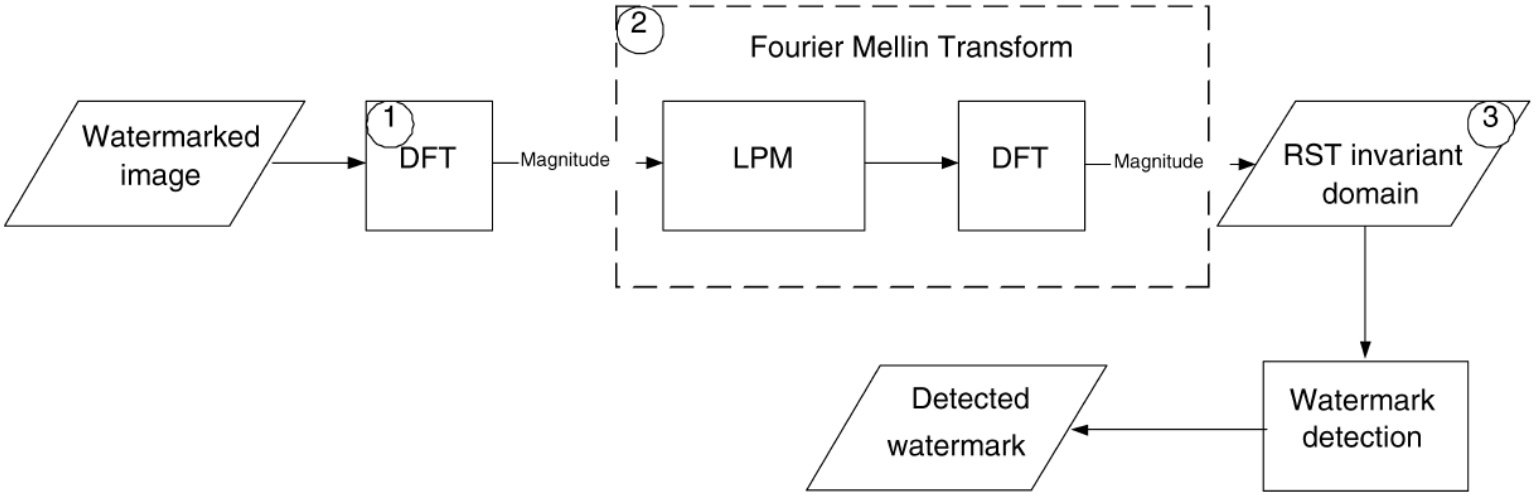


Fig. 10. Detecting watermark from Fourier–Mellin domain.

Espace invariant : Fourier Mellin [O'Ruanaidh et Pun 1998]

Problème : LPM et ILPM détériorent énormément l'image.
Solutions :

- [O'Ruanaidh et Pun 1998] dégradation du signal de tatouage uniquement,
- [Kim et al. 2004] dégradation uniquement au signal de tatouage + inversion des transformations + utilisation de points caractéristiques,
- [Zheng et al. 2003] dégradation uniquement du signal de tatouage + approximation de l'ILPM,
- [Liu et al. 2005] (rectification non aveugle + Fourier-Melin) : des blocs du domaine spatial et du domaine de Fourier Mellin sont extraits à l'insertion et utilisés à l'extraction pour rectifier l'image.
- [Lin et al. 2001] : Projection 1D (projection de Radon) du domaine Fourrier Mellin, puis tatouage de ce signal 1D.

Espace invariant : analyse des résultats de [Zheng et al. 2003]

- bon comportement face à la rotation, au scaling et à jpeg,
- L'espace d'insertion est limité,
- Dans le cas non aveugle, la recherche exhaustive augmente le nombre de faux positifs ainsi que le coût calculatoire.
- robustesse au print & scan ?, robustesse au croping ?

Espace invariant : Autres approches

- Calcul de CIT, RIT dans Fourier Mellin [Lin et al. 2001] (bonne résistance aux rotations + scaling + jpeg),
- Normalisation de l'image par calcul de moments [Alghoniemy and Tewfik 2004]. Pas très robuste aux rotations, au scaling et à jpeg. Ne résiste pas au cropping car nécessite toute l'information pour calculer la normalisation,
- Pseudo-Zenike Decomposition [Xin et al. 2004]. Utilisation de la normalisation de l'image en plus de la décomposition de Zernike.

Plan

1 Préambule

2 Les attaques désynchronisantes

3 Synchronisation par détection non aveugle

4 Recherche exhaustive

5 Tatouage invariant (espace invariant)

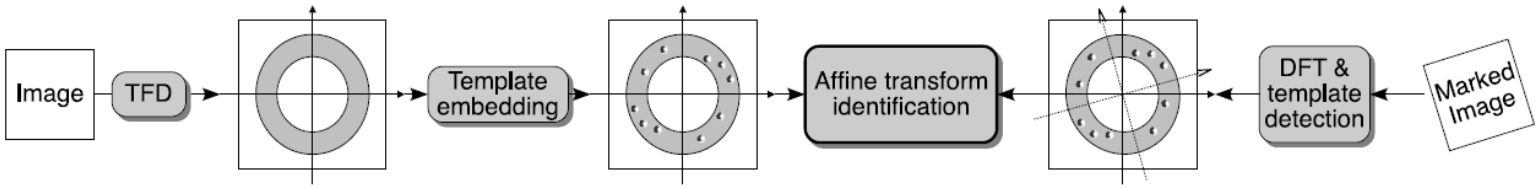
6 Pattern de synchronisation

7 Synchronisation implicite (tatouage basée contenu) ; Tatouage de seconde génération

8 Conlusion - Pistes

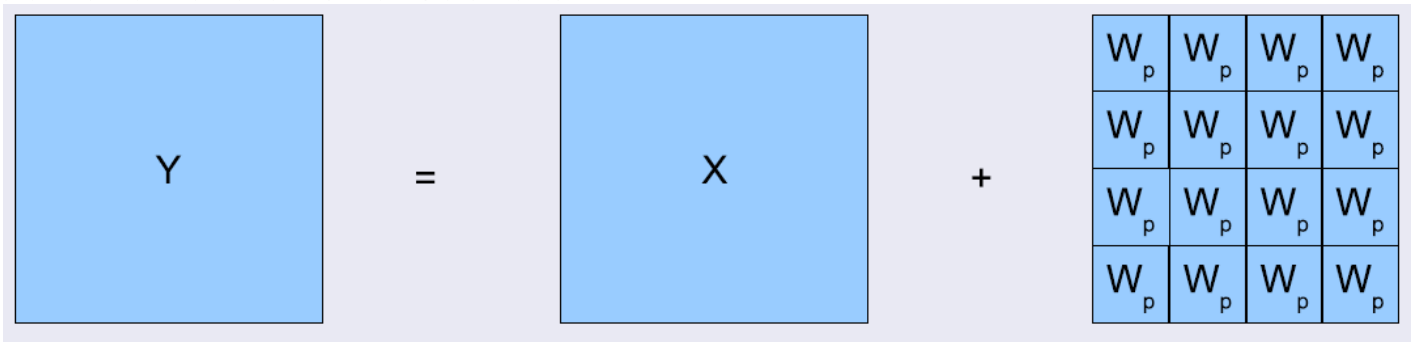
Synchronisation ou recalage - Insertion de template

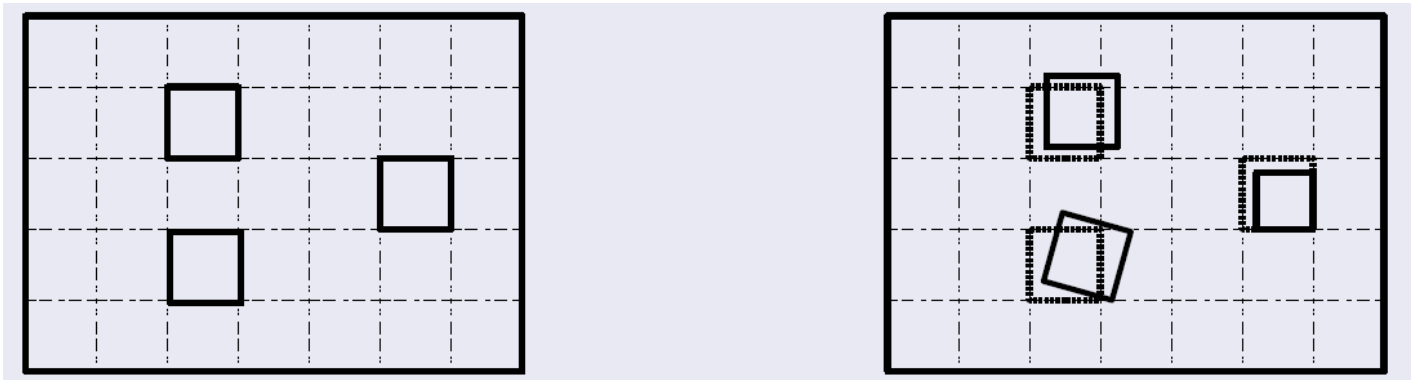
Insertion dans le domaine de Fourier de pics (template).



synchronisation ou recalage - Insertion de séquences périodiques

L'insertion de séquences périodiques permet de réduire l'espace de recherche de la distortion.





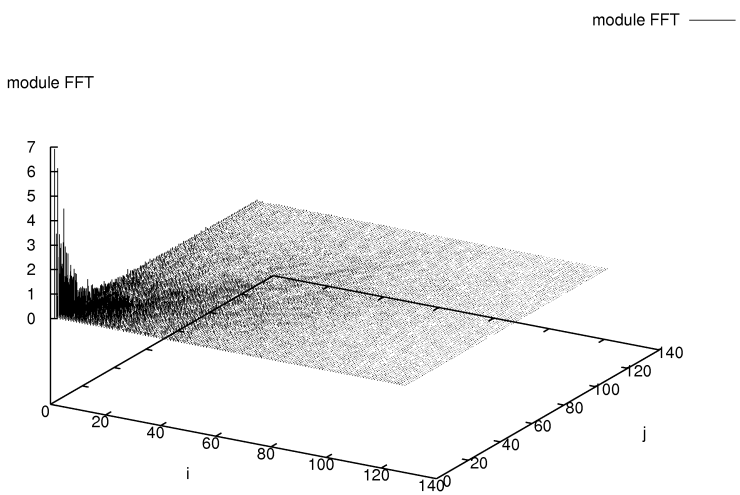
synchronisation ou recalage - Insertion de séquences périodiques

La recherche peut s'effectuer directement dans le domaine de fourier par convolution dans le domaine de Fourier (domaine insensible aux translations).

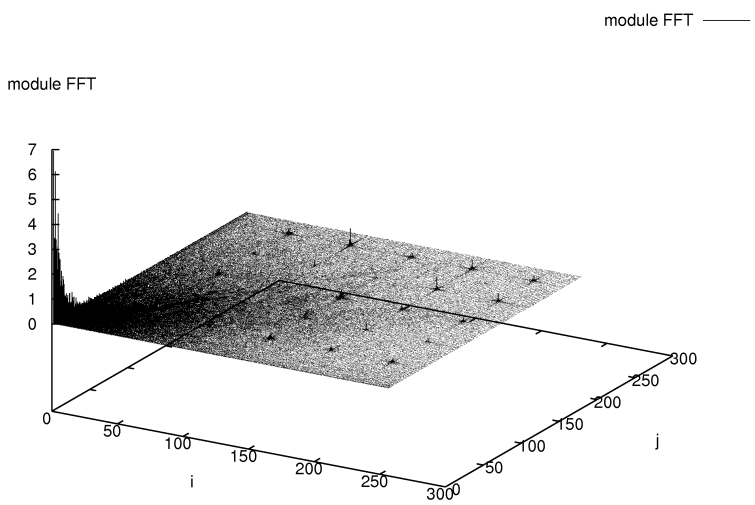
original

pattern ajouté

synchronisation ou recalage - Insertion de séquences périodiques



module FFT image originale



module FFT image avec pattern

synchronisation ou recalage - Insertion de séquences périodiques

Problèmes :

- L'insertion périodique n'est pas sûre ; la supression des pics par un attaquant dans le domaine DFT supprime la possibilité de re-syncrhoniser [Herrigel et al. 2001].
- L'insertion de maximum locaux dans la DFT peut dégrader l'image,
- L'imprécision de la détection peut provoquer l'échec de la détection.

synchronisation ou recalage - Insertion de séquences périodiques [Voloshynovskiy et al. 2001]

Le signal de tatouage est répété sur des petits blocs.

- rotation et scaling : bon
- jpeg, bruit additif, filtrage : moyen
- débruitage, copy attack : faible (contre attaque existe selon [Liu et al. 2002])
- Les paramètres détectés peuvent être trop imprécis (nécessite une recherche exhaustive locale)
- de petites distortions locales dégradent sérieusement la performance [Alvarez-Rodriguez and Perez-Gonzales 2002],

synchronisation ou recalage - Insertion de séquences périodiques

Solution : pseudo-periodicity (local search but no more peaks)

Random sequence

W[0]	W[1]	....	W[N-2]	W[N-1]

Random periodic sequence generated around i

...	...	...
W[(i-k1-k2) mod N]	W[(i-k2) mod N]	W[(i+k1-k2) mod N]
W[(i-k1) mod N]	W[i]	W[(i+k1) mod N]
W[(i-k1+k2) mod N]	W[(i+k2) mod N]	W[(i+k1+k2) mod N]

Damien Delannay UCL Louvain

- la détection est assez délicate si l'on considère des attaques scaling, rotation (perturbation du signal hôte + mapping) .
- un attaquant peut réussir à observer la périodicité.

Plan

1 Préambule

2 Les attaques désynchronisantes

3 Synchronisation par détection non aveugle

4 Recherche exhaustive

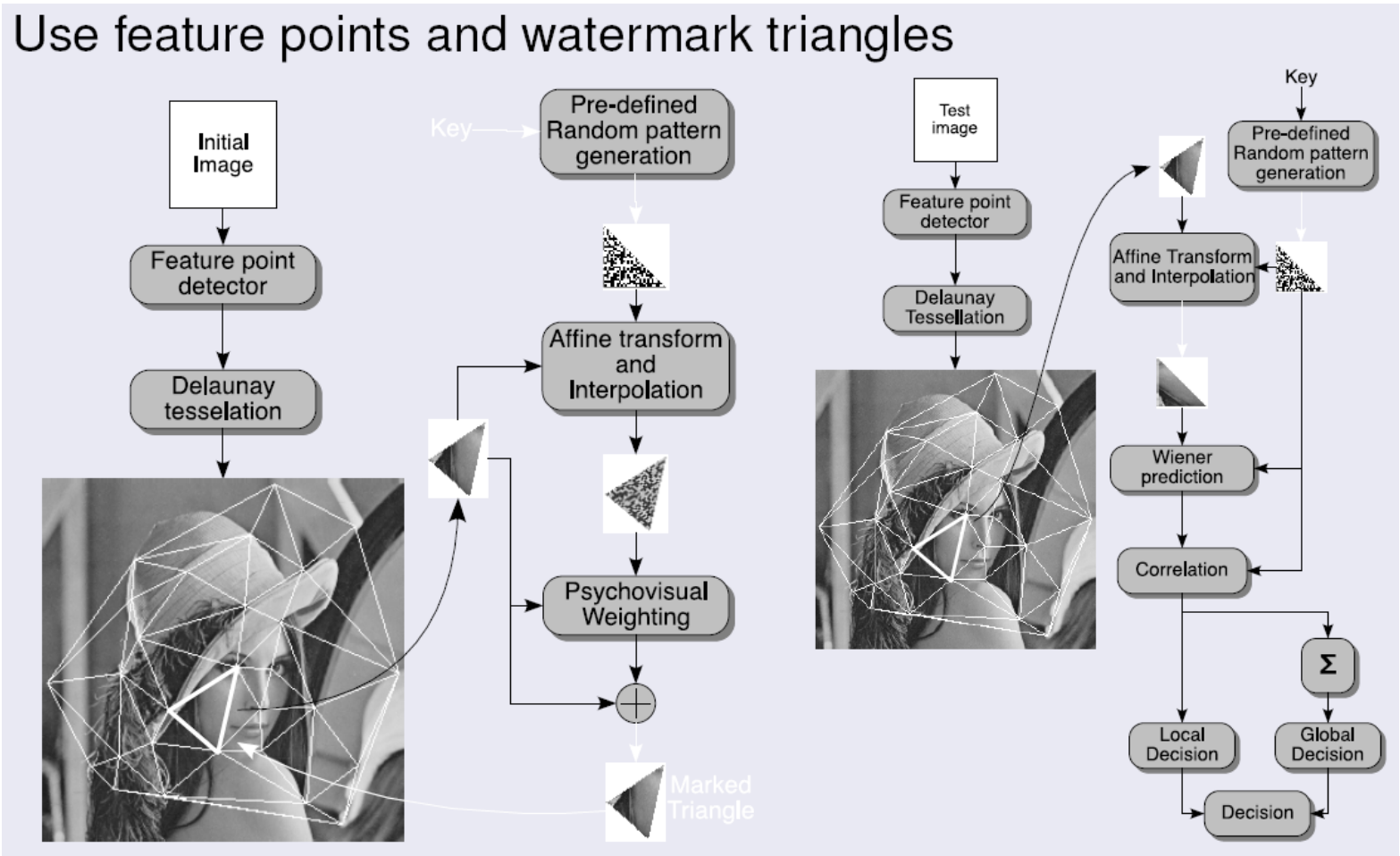
5 Tatouage invariant (espace invariant)

6 Pattern de synchronisation

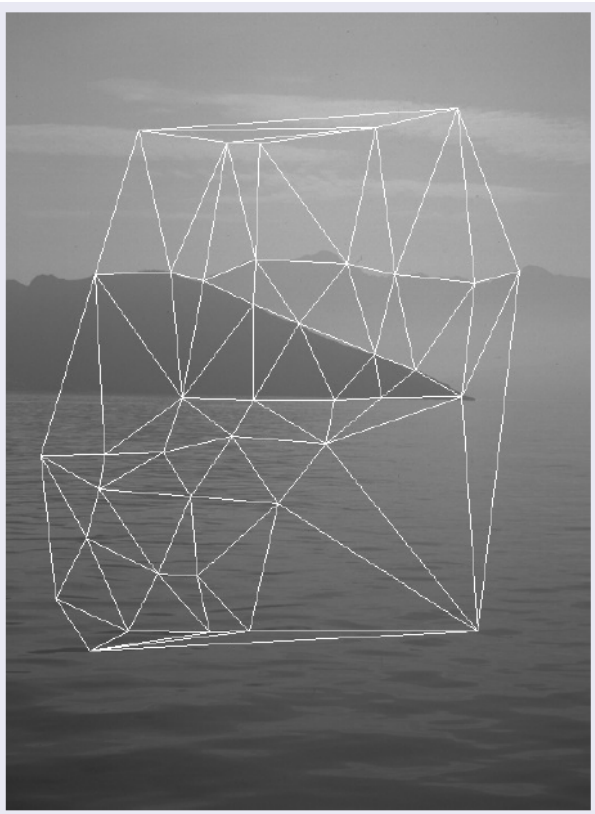
7 Synchronisation implicite (tatouage basée contenu) ; Tatouage de seconde génération

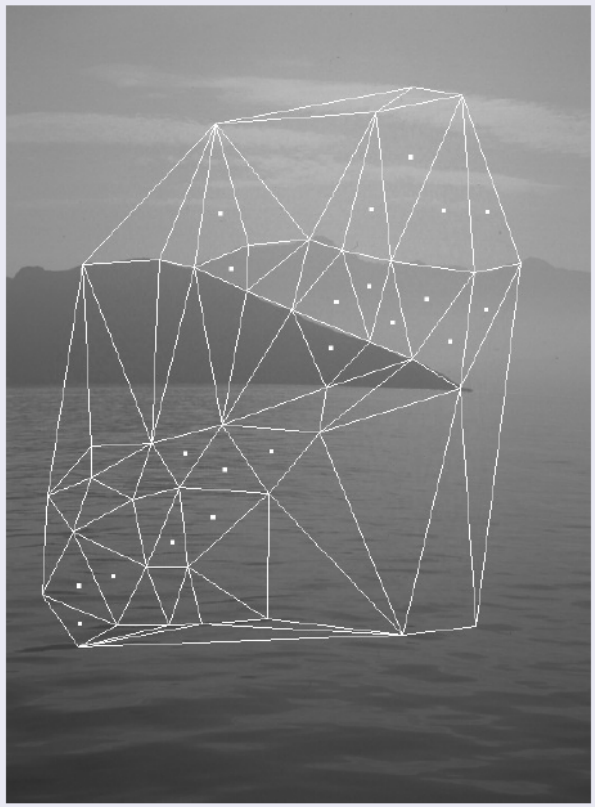
8 Conlusion - Pistes

synchronisation basée contenu [Bas et al. 2002]



synchronisation basée contenu [Bas et al. 2002]





synchronisation basée contenu [Bas et al. 2002]

Problèmes :

- rotation et scaling : moyen,
- jpeg, bruit additif et filtrage : bon
- capacité limité,
- points caractéristique sensibles aux déformations géométriques (Harris améliorés)

synchronisation implicite (tatouage basé contenu)

- [Kutter et al. 1999], [Duric el al. 1999] restorent l'image à partir des points caractéristiques de l'image,
- [Dittman et al 2000] détection aveugle avec utilisation d'un pattern dépendant du contenu,
- [Tang et Hang 2003] points caractéristiques obtenus par filtrage par chapeau mexicain + normalisation des régions circulaires puis FFT de la région et tatouage.

Plan

1 Préambule

2 Les attaques désynchronisantes

3 Synchronisation par détection non aveugle

4 Recherche exhaustive

5 Tatouage invariant (espace invariant)

6 Pattern de synchronisation

7 Synchronisation implicite (tatouage basée contenu) ; Tatouage de seconde génération

8 Conlusion - Pistes

Conclusion - Techniques les plus perfomantes par famille

	point(s) positif(s)	point(s) négatif(s)
espace invariant	robuste RST	détection souvent non-aveugle échantillonage, interpolation taille espace d'insertion résistance au print & scan et cropping
pattern de synchro	robuste au RST possible gestion print & scan et cropping	augmente localement l'énergie sensible aux attaques par débruitage
basé contenu	points caractéristiques indissociables de l'image possible gestion print & scan et cropping	repose sur la robustesse du détecteur de points caractéristiques

Cas particuliers :

- espace invariant spéciaux : histogramme ou luminance moyenne,
- détection non aveugle,
- recherche exhaustive.

Conclusion - Perspectives

- Aucune solution n'est encore complétement satisfaisante,
- Beaucoup de traitement du signal et peu de formalisation,
- Les solutions futures devraient :
  - gérer l'attaque de déformation géométrique locale,
  - gérer le cropping,
  - utiliser des approches informées pour le multi-bits et des approches "à la Broken Arrows" pour le 0-bit,
  - prendre en compte le compromis débit - distortion - robustesse - sécurité,
  - Utiliser les codes correcteurs (gérant l'effacement) pour les approches multi-bits,

Conclusion - Quelques pointeurs pour poursuivre la réflexion

- **"'Print and Scan' Resilient Data Hiding in Images"**,

  Kaushal **Solanki**, Member, Upamanyu Madhow, B. S. Manjunath, Shiv Chandrasekaran, and Ibrahim El-Khalil, IEEE Transactions on Information Frensics and Security, Vol. 1, N° 4, Décembre 2006,

- **"Stochastic Image Warping for Improved Watermark Desynchronization"**,

  Angela **D'Angelo**, Mauro **Barni**, and Neri Merhav, EURASIP Journal on Information Security, Vol. 2008, 14 pages.

- **"Universal Decoding of Watermarks Under Geometric Attacks"** Pierre **Moulin**, IEEE International Symposium on Information Theory, Volume 2006, 9-14 Juillet 2006, pp 2353 - 2357.