Le tatouage de documents numérique
Cours 4

Marc Chaumont

30 novembre 2007

Définition

- **faux positif :** Survient lorsque le détecteur indique qu'une marque est présente alors qu'il y en a pas.
- **faux négatif :** Survient lorsque le détecteur indique qu'une marque est abscente alors qu'il y en a une.

Dans une application de **surveillance de diffusion télévisuelle** où les publicités sont tatouées, un **faux négatif** mène à la conclusion que la publicité n'a pas été diffusée...
Dans une application où la présence de la marque autorise la **lecture d'un DVD**, un **faux négatif** empêche la lecture d'un DVD censé être autorisé.
Dans une application de preuve d'appartenance, la détection d'un faux positif mène à une accusation de vol de l'œuvre d'un ayant-droit (alors que la marque n'a pas été insérée).

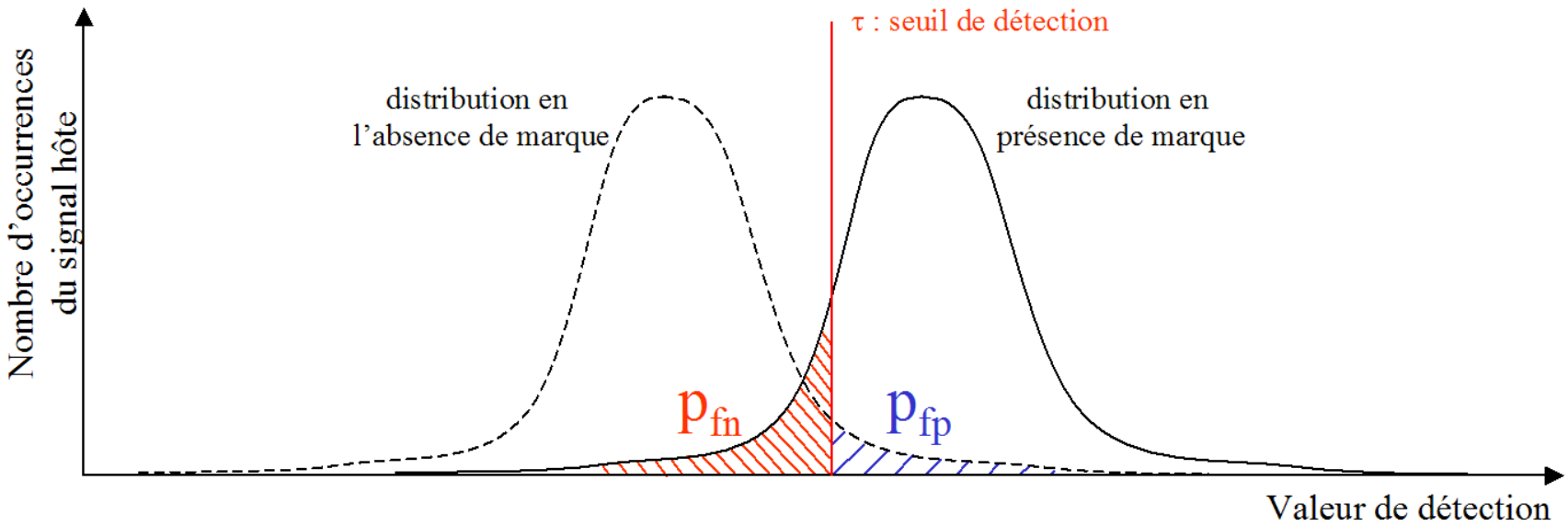
Quelques chiffres

- Dans le cas d'une application de preuvre d'appartenance, le détecteur étant rarement utilisé, une probabilité de **faux-positif** de 10^{-6} doit suffire.
- Dans le cas d'une application de contrôle de copies, des millions de détecteurs tournent constament sur des millions de documents. La probabilité de **faux-positif** doit être de 10^{-12} (1 erreur pour 1000 années de calcul continu).

Intérêt de l'analyse des performances

1. **A priori :** En fonction de la spécification du système (probabilité de faux négatif ou faux positif souhaitée) la technique choisie peut être différente, les seuils de détection sont différents ;
2. **A posteriori :** Les expérimentations permettent de valider les taux d'erreur.

Faux positif - Faux négatif



Caractérisation d'un schéma de tatouage

- **L'efficacité :** représente la capacité du système à détecter la marque sans qu'il y ait eu d'attaque. L'efficacité est mesurée par la valeur de $1 - p_{fn}$.
- **La robustesse :** représente la capacité du système à détecter la marque après avoir subi une distortion liée à un traitement du signal. La robustesse est mesurée par la valeur de $1 - p_{fn}$.
- **La sécurité :** définition non encore partagée :
  - "Attacks to robustness are those whose target is to increase the probability of error of the data hiding channel"
  - "Attacks to security are those aimed at gaining knowledge (measurable as information) about the secrets of the system (e.g. the embedding and/or detection keys)" F. Perez-Gonzalez et al., "First summary report on fundamentals", ECRYPT - European Network of Excellence in Cryptology,IST-2002-507932, deliverable D.WVL.1, 2005.

Plan

Analyse de la proba - Faux positif - cas corrélation linéaire

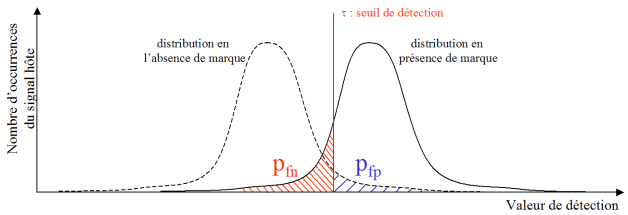
Avec une détection par corrélation linéaire

$$z_{lc} = \frac{1}{N}\sum_{i=1}^{N} w_r[i].c[i]$$

En supposant être dans le cas "random-watermark", Chaque $w_r[i]c[i]$ est une variable aléatoire distribuée selon $w_r[i]$ et multipliée par une valeur $c[i]$. En assumant que le théorème de la limite centrale est valide, z_{lc} tend vers une loi normale de moyenne $\mu_{lc} = \mu_w\mu_c$ et d'écart-type $\sigma_{lc} = \sigma_w|c|$. Si l'on choisit les vecteurs marque de moyenne nulle alors $\mu_{lc} = 0$. La probabilité que le détecteur retourne une valeur x est donnée par :

$$P_{z_{lc}}(x) = \frac{1}{\sigma_{lc}\sqrt{2\pi}} exp(\frac{-x^2}{2\sigma_{lc}^2})$$

Analyse de la proba - Faux positif - cas corrélation linéaire



La probabilité de faux positif (cas "random work") est alors :

$$P_{fp} = \int_{\tau}^{\infty} P(x)dx = \int_{\tau}^{\infty} \frac{1}{\sigma_{lc}\sqrt{2\pi}} exp(\frac{-x^2}{2\sigma_{lc}^2})$$

Les expériences (Livre Cox, Miller, Bloom) montrent que dans le cas "random-watermark" l'analyse est correcte par contre dans le cas "random-work" l'analyse ne l'est pas.

Analyse de la proba - Faux positif - RANDOM WATERMARK - cas corrélation linéaire

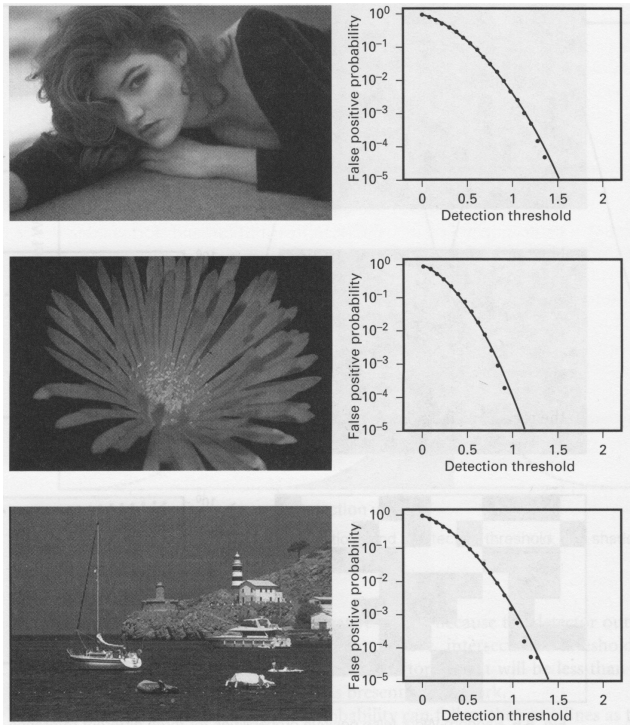


Fig. 6.4 Random-watermark false positive probabilities for three different images at varying detection thresholds applied to linear correlation. Each image was tested against 20,000 reference marks. The solid lines are the theoretical predictions. The points are the measured results.

Analyse de la proba - Faux positif - RANDOM WORK - cas corrélation linéaire

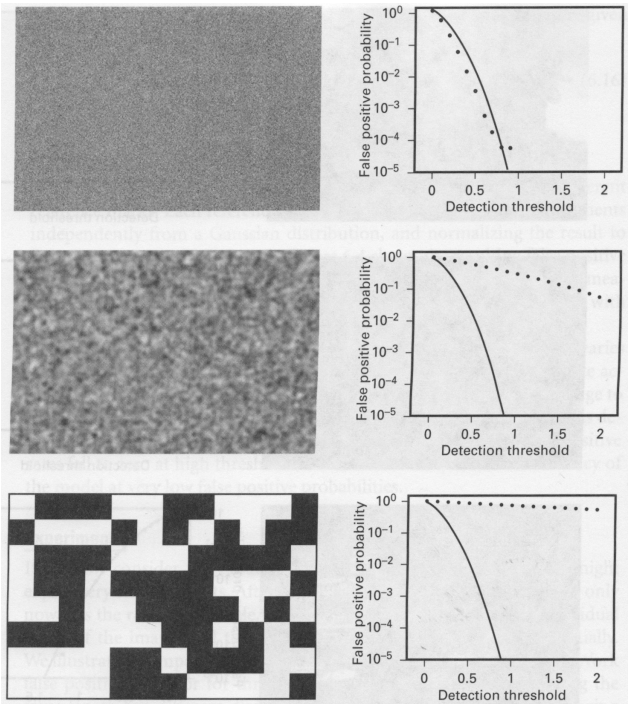


Fig. 6.5 Random-Work false positive probabilities for three different reference patterns at varying detection thresholds applied to linear correlation. The graphs were calculated using 20,000 images from the Corel database.

Analyse de la proba - Faux positif - cas corrélation normalisée

Avec une détection par corrélation normalisée

$$z_{nc} = \frac{\sum_{i=1}^{N} w_r[i].c[i]}{|w_r||c[i]|}$$

En supposant être dans le cas "random-watermark", chaque $w_r[i]c[i]$ est une variable aléatoire distribuée selon $w_r[i]$ et multipliée par une valeur $c[i]$. En assumant que le théorème de la limite centrale est valide, z_{lc} tend vers une loi normale de moyenne $\mu_{lc} = \mu_w \mu_c$ et d'écart-type :

$$\sigma_{lc} = \frac{\sigma_{w_r}|c|}{|w_r||c|}$$

Analyse de la proba - Faux positif - cas corrélation normalisée

Si l'on choisit les vecteurs marque de moyenne nulle on a alors $\mu_{Ic} = 0$ et :

$$|w_r| \approx \sqrt{N}\sigma_{w_r}$$

donc la variance :

$$\sigma_{nc}^2 = \frac{1}{N}$$

Analyse de la proba - Faux positif - cas corrélation normalisée

La probabilité que le détecteur retourne une valeur x est donnée par :

$$P_{z_{nc}}(x) = \frac{N}{\sqrt{2\pi}} exp(\frac{-x^2.N}{2})$$

La probabilité de faux positif (cas "random work") est alors :

$$P_{fp} = \int_{\tau}^{\infty} P(x)dx = \int_{\tau}^{\infty} \frac{N}{\sqrt{2\pi}} exp(\frac{-x^2.N}{2})$$

L'expérience du livre de Cox, Miller, Boom montre que dans le cas "random-watermark" l'analyse est correcte jusqu'à un seuil. Passé ce seuil, il y a surestimation de la probabilité d'erreur.

Analyse de la proba - Faux positif - RANDOM WATERMARK - cas corrélation normalisée

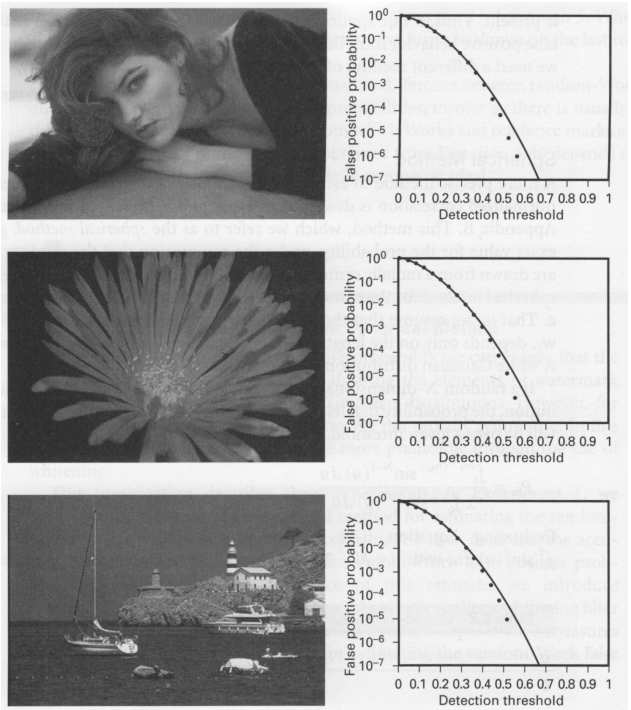
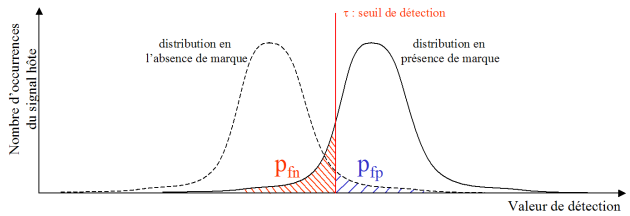


Fig. 6.13 Random-watermark false positive rates for the correlation-coefficient-based D_BLK_CC detection algorithm. Empirical results (points) are for 1,000,000 random reference marks compared against the three illustrated images, using the D_BLK_CC detector. Theoretical estimates (solid lines) are computed using the approximate Gaussian method.

Remarque sur l'analyse des Faux négatif

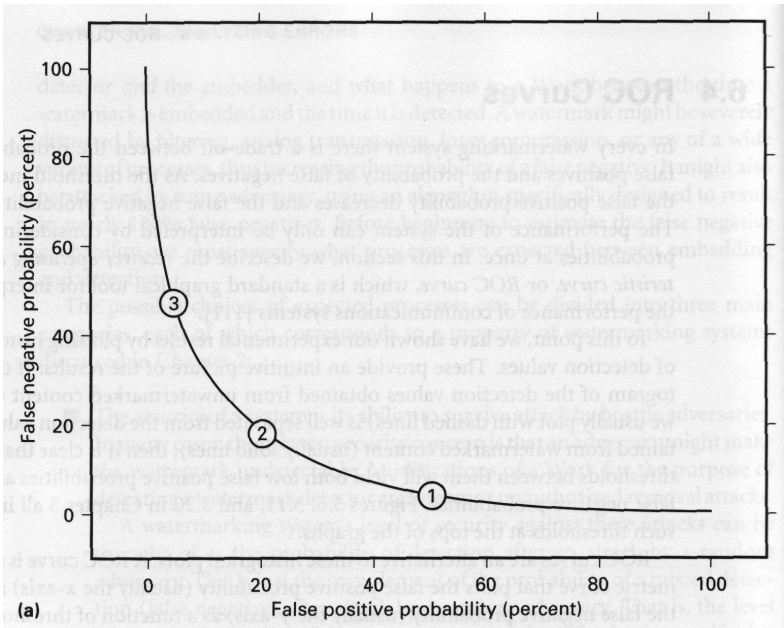


Pour l'expression analytique des faux négatifs il faut d'abord définir la technique de tatouage (par exemple $c_w = c_o + \alpha w_r$) puis on peut également traiter d'une attaque particulière (par exemple l'ajout d'un bruit $c_{wn} = c_w + n$) et ensuite on exprime la probabilité du détecteur de retourner une valeur x. Ensuite, on intègre entre entre $-\infty$ et τ pour obtenir la probabilité de faux négatif.

Plan

La courbe ROC

ROC : Receiver operating characteristic courbe.



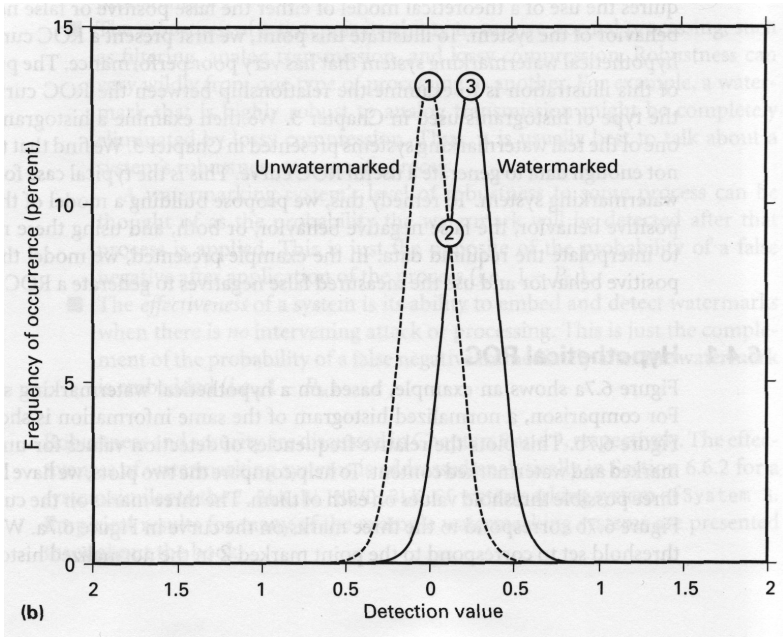


Fig.: Courbe ROC (a) et histogramme normalisé (b) pour un système de tatouage hypothétique

La courbe ROC dans la vrai vie ...

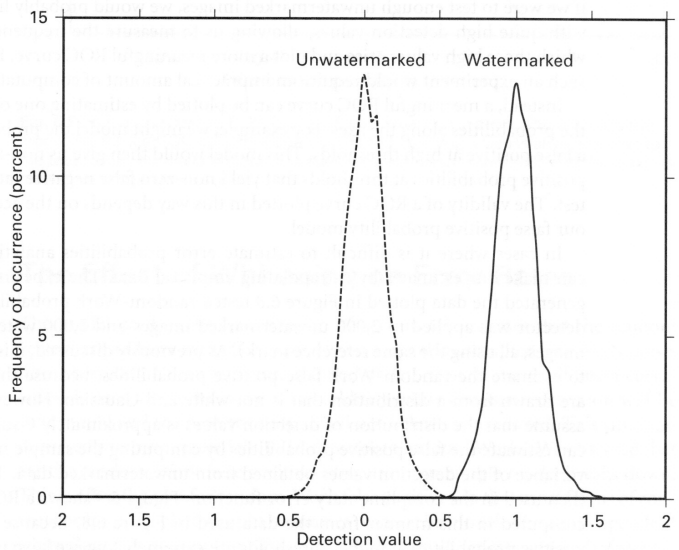


Fig. 6.8 Normalized histogram for the E_BLIND/D_LC watermarking system.

Fig.: 2000 images non marquées, les même 2000 images marquées (m=1)

- L'histogramme est peu précis et il n'y a pas assez de données,
- Il est nécessaire d'interpoler les courbes.

Définition

La robustesse d'un schéma désigne le fait qu'après tatouage, la marque **résiste à des "usages de tous les jours"**.

- compression avec perte
- conversion analogique-numérique
- enregistrement analogique (VHS...)
- print & scan
- changement de format (Jpeg $\longrightarrow$ Jpeg2000)
- rotation
- half-toning ...

Plan

Solution : Insertion redondante

L'insertion redondante permet de survivre à des dégradations locales (en fréquence ou spatiales).

- Solution 1 : découper le signal hôte en tuiles et insérer la marque dans chaque tuile
- Solution 2 : insertion avec différentes techniques de tatouage (cocktail).

Plan

L'étalement de spectre (Spread Spectrum)

La technique provient du monde des télécommunications. Un message m est composé d'un ensemble de symboles $m[i]$ ($m[i]$ vaut bien souvent 0 ou 1). Chaque symbole $m[i]$ est transmis à travers un signal appelé **porteuse** et noté u_i. Une porteuse est un signal pseudo-aléatoire (obtenu par un GNPA) pouvant être composé de 0 et de 1 ou bien distribué suivant une loi Gaussienne normale $\mathcal{N}(0,1)$. On peut également contraindre les porteuses à être orthogonales ($\forall i$, $\forall j,\ u_i.u_j = 0$).

L'étalement de spectre (Spread Spectrum), formalisation

Insertion :

- w_i : un vecteur (porteuse) de la taille du signal hôte N,
- m : un message composé de N_c bits.
- s : une fonction (appelée modulation) $0, 1 \rightarrow \mathbb{R}$. Par exemple $s(m[i]) = \gamma(-1)^{m[i]}$ avec γ un facteur réglant l'ampleur de la distortion.
- La marque est alors $w = \sum_{i=1}^{N_c} w_i.s(m(i))$
- l'insertion est alors $c_w = c_o + w$

Détection :

- Soit c_{wn} un signal tatoué attaqué. Le message extrait est $\hat{m}[i] = sign(c_{wn}.u_i)$ avec :

$$sign(x) = \begin{cases} 0 \ si \ x > 0 \\ 1 \ si \ x \leq 0 \end{cases} \quad (1)$$

L'étalement de spectre ; Remarques

- la solution par étalement de spectre a été vue dans le premier exemple du cours (insertion d'un seul bit 0 ou 1).
- ...
- ...
- ...

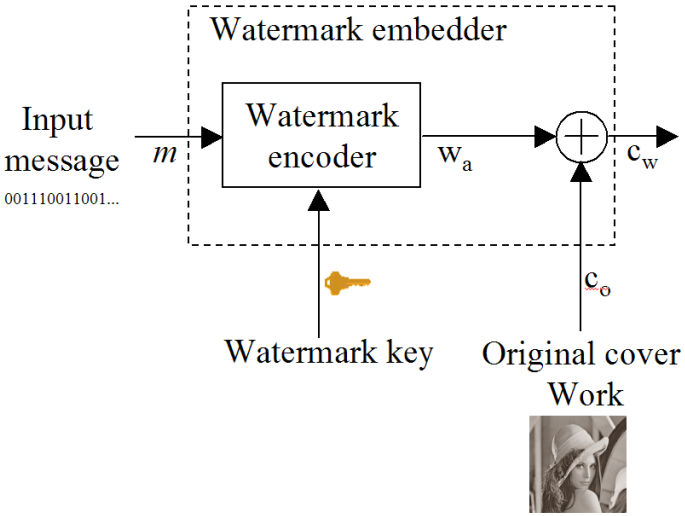
Rappel cours 1 ; Insertion aveugle

- Le message m est un unique bit (0 ou 1).
- Soit w_m généré à partir d'un unique pattern w_r de la même taille que l'image c_o. Ce pattern w_r est généré pseudo-aléatoirement via une clef secrête. On a :

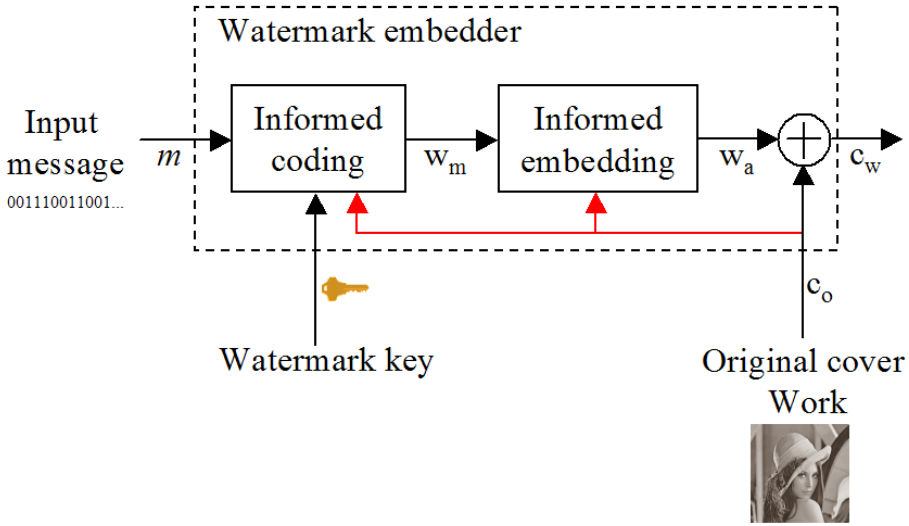
$$w_m = \begin{cases} w_r \ si \ m = 1 \\ -w_r \ si \ m = 0 \end{cases}$$

- La marque est alors définie par $w_a = \alpha w_m$. Le scalaire α permet de contrôler la force d'insertion de la marque.
- Finalement, le tatouage est réalisé comme ceci : $c_w = c_o + w_a$.

Rappel tatouage aveugle vs. informé



Tatouage aveugle



Tatouage informé

L'étalement de spectre ; Remarques

- la solution par étalement de spectre a été vue dans le premier exemple du cours (insertion d'un seul bit 0 ou 1).
- la solution par étalement de spectre n'est pas une solution informée. Il existe des solutions informées (Informed Spread Spectrum, ...)
- Dans le domaine fréquentiel, les porteuses vont modifier un grand nombre d'échantillons fréquentiels du signal hôte. Si le signal (tatoué) subit des dommages sur une fraction des fréquences (filtre passe-bande, ...), les porteuses restent identifiable et le message embarqué peut-être extrait correctement.
- caractérisation du spread spectrum : l'energie insérée dans 1 fréquence est très faible. Il y a donc peu de dégradations perceptuelles et il y a une bonne robustesse aux distortions grâce à la dispersion.

Plan

Solution : Insertion dans coefficients significatifs

- Certains coefficients sont peu fiables (haute fréquence) car facilement dégradés. Il vaut mieux éviter d'insérer dans ces coefficients.
- De manière générale, il faut essayer de tatouer dans les coefficients significatifs perceptuellement. En effet, ces coefficients ne changent pas sauf s'il y a modifications perceptuelles du contenu.
- Une marque n'a pas nécessairement besoin de résister à une dégradation perceptuelle. En effet si l'hôte est tellement dégradé qu'il n'est pas reconnaissable, l'information insérée n'est plus forcément utile.

Solution : Insertion dans coefficients significatifs

- Il y a donc un objectif contradictoire (imperceptibilité - robustesse) : insérer dans les coefficients significatifs perceptuellement implique une bonne robustesse mais une dégradation perceptuelle.
- Le compromis classique est d'insérer dans les fréquences moyennes (par exemple dans les 12 premiers coefficients DCT d'un bloc image 8×8). Ceci-dit, insérer spécifiquement dans certains coefficients entraîne une super-robustesse qui peut être une faille pour une attaque à la robustesse. "How we broke the BOWS watermark" S. Craver, I. Atakli and J. Yua, SPIE 2007.

Plan

Solution : Insertion dans des coefficients de robustesse connu

- On peut par exemple insérer dans un domaine de robustesse qui nous intéresse pour une application donnée (Par exemple le domaine de Fourier est insensible à la translation).
- Si l'on a déterminé les attaques auquel on souhaite survivre, on peu faire des tests intensif pour déterminer les coefficients interessants (solution à prendre avec des pincette car les coefficients robustes peuvent varier avec la nature des signaux hotes).

Plan

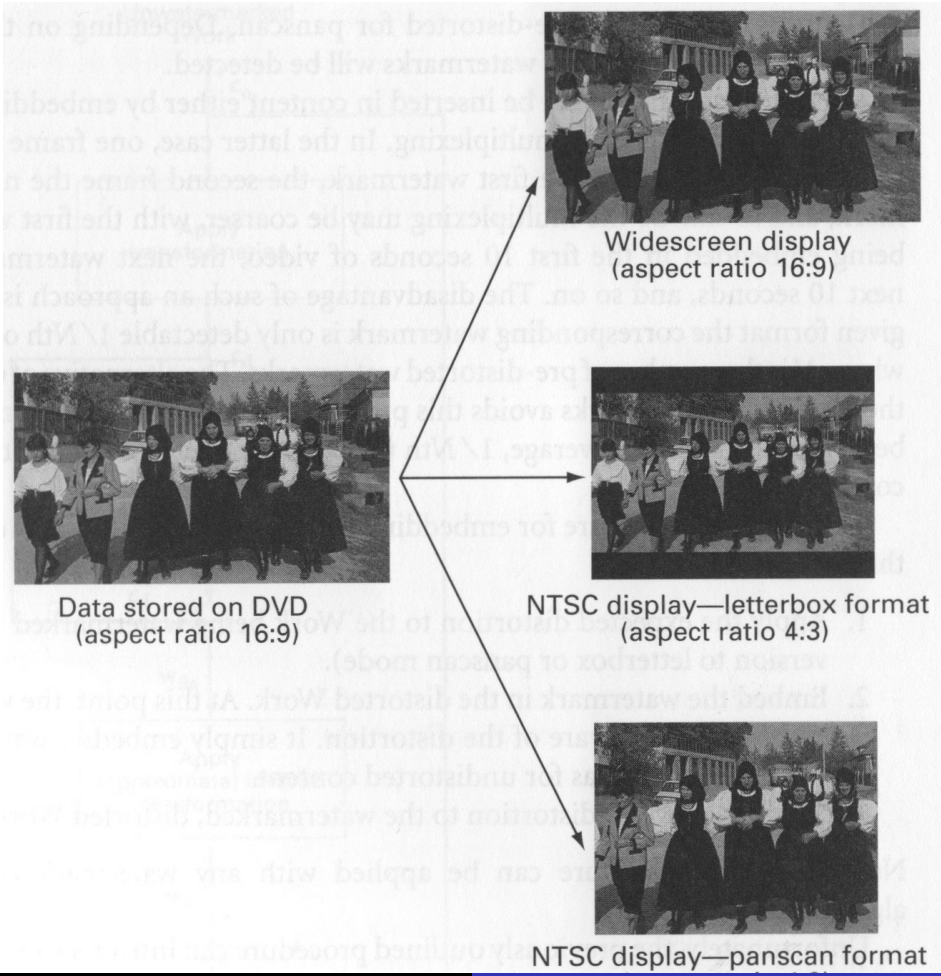
Solution : Inverser les distortions au détecteur

- Sol1 : Si le détecteur peut estimer la distortion (attaque), il inverse la distortion (exemple rotation) et il obtient une version approchée de la version tatouée non attaquée.
- Sol2 : Si le détecteur peut estimer la distortion (attaque), il applique la distortion (exemple passe-bas) au pattern de référence et ensuite il lance le détecteur.
- L'estimation de la distortion est plus aisée quand le détecteur est informée que lorsqu'il est aveugle.

Plan

Solution : Pré-inverser les distortions à l'insertion

Exemple : Les lecteurs DVD affichent le contenu d'un DVD en *16 :9*, *4 :3 letterbox* et *4 :3 panscan*.

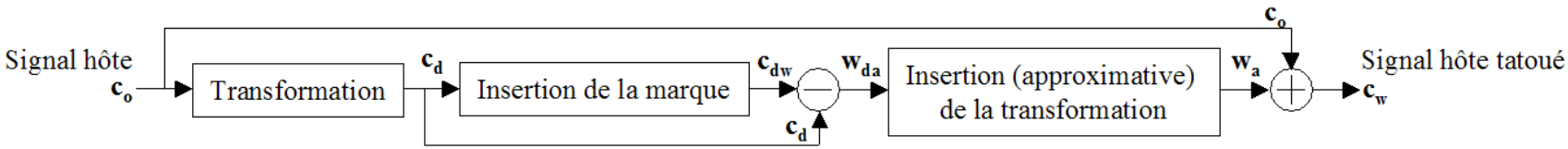


Solution : Pré-inverser les distortions à l'insertion

Exemple : Les lecteurs DVD affichent le contenu d'un DVD en *16 :9*, *4 :3 letterbox* et *4 :3 panscan*. La marque doit être insérée dans le format plein écran (16 :9) et donc lorsque le DVD est affiché dans les deux autres formats la marque est distordue.

Solution : Pré-inverser les distortions à l'insertion

On peut donc envisager d'embarquer 3 marques (une par format) tel que le détecteur détecte la même marque quel que soit le format d'affichage. Tout est inséré dans le format 16 : 9 les distortions sont pré-inversées pour les 2 autres formats.



Solution : Pré-inverser les distortions à l'insertion

- La solution est générale et applicable si les distortions sont approximativement inversibles,
- La solution n'entraîne pas de coût supplémentaire au détecteur
- La solution peut être implémentée après le déploiement du détecteur.

Plan

Le bruit additif

$$c_{wn} = c_w + n$$

avec n un vecteur aléatoire choisi suivant une distribution donnée indépendante de c. Exemple de bruit : la neige qu'il peut y avoir sur un écran télé lorsque l'on capte mal une chaîne (ce bruit est un bruit blanc car il affecte uniformément et indépendamment tout le signal).

Le bruit additif - corrélation linéaire fixée

Expérimentation 1 : 2000 images tatouées avec insertion à corrélation linéaire fixée de valeur 1, message $m = 1$, et détection à $\tau_{lc} = 0.7$. Chaque image est distordue 10 fois par un bruit blanc à 16 puissances différentes.

lente décroissance due aux arrondis et clipping. 97% des marques sont détectées à forte disto (à ces fortes distos, l'image ne présente plus d'intéret).

Le bruit additif - insertion à corrélation linéaire fixée

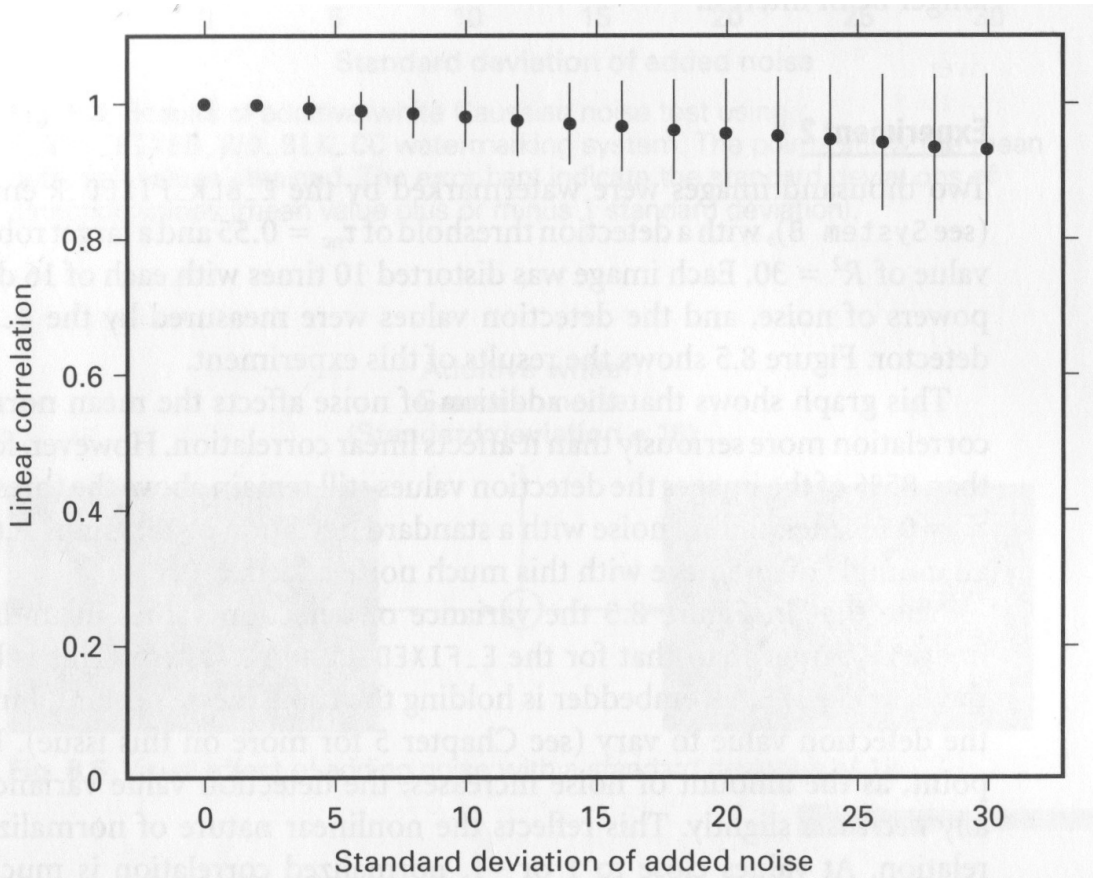


Fig. 8.4 Results of additive white Gaussian noise test using E_FIXED_LC/D_LC watermarking system. The points show the mean detection values obtained. The error bars indicate the standard deviations of detection values (mean value plus or minus 1 standard deviation).

Le bruit additif - insertion à robustesse (corrélation normalisée) fixée

Expérimentation 2 : 2000 images tatouées avec insertion à robustesse $R^2 = 30$ (détection à corrélation normalisée $\tau_{nc} = 0.55$) et message $m = 1$. Chaque image est distordue 10 fois par un bruit blanc à 16 puissances différentes. La marque pattern est de taille 8×8 et dupliquée sur toute l'image. À la détection on effectue la moyenne des blocs et on lance ensuite la détection par corrélation normalisée.

Le bruit additif - insertion à robustesse (corrélation normalisée) fixée

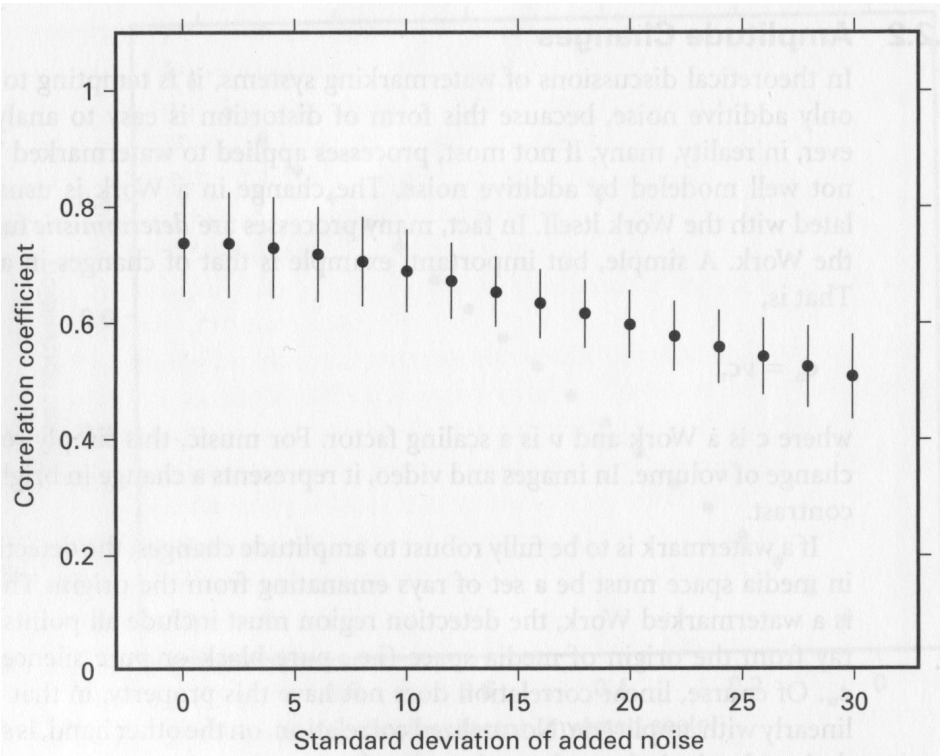


Fig. 8.5 Results of additive white Gaussian noise test using E_BLK_FIXED_R/D_BLK_CC watermarking system. The points show the mean detection values obtained. The error bars indicate the standard deviations of detection values (mean value plus or minus 1 standard deviation).

Plan

Le changement d'amplitude

$$c_{wn} = \mu c_w$$

avec μ un facteur de scaling. Cela se traduit sur l'image par un changement de contraste ou de luminosité. En musique cela se traduit par un changement de volume.

Expérimentation 1 : La corrélation linéaire change linéairement avec l'amplitude.

Expérimentation 2 : La corrélation normalisée est résistante à cette dégradation.

Le changement d'amplitude - insertion à corrélation linéaire fixée

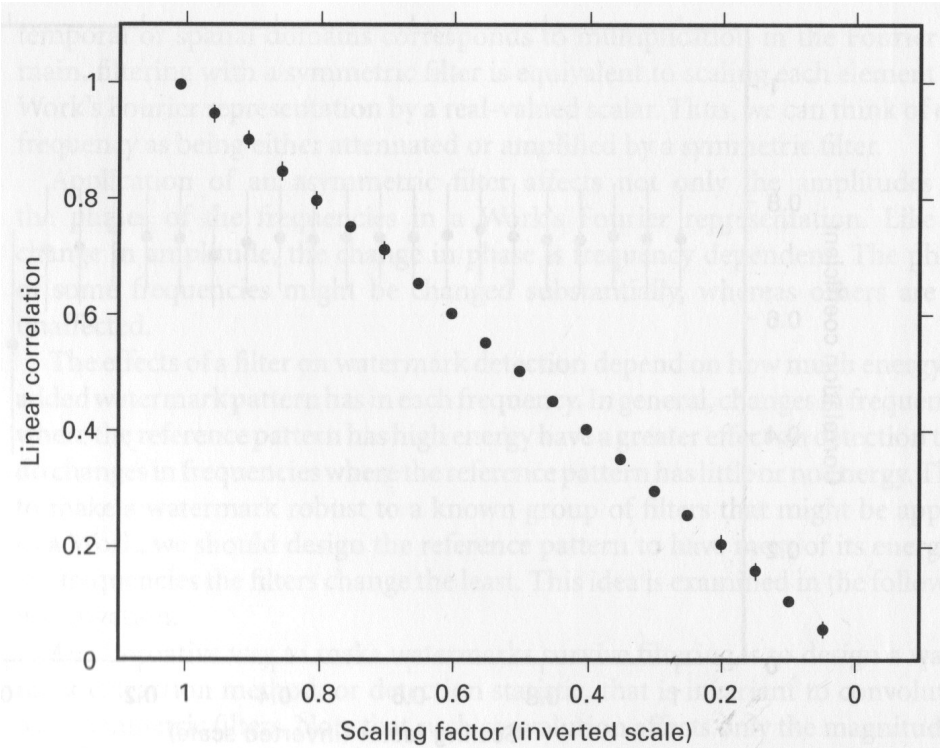


Fig. 8.7 Results of contrast scaling test using E_FIXED_LC/D_LC watermarking system. The points show the mean detection values obtained. The error bars indicate the standard deviations of detection values.

Le changement d'amplitude - insertion à robustesse (corrélation normalisée) fixée

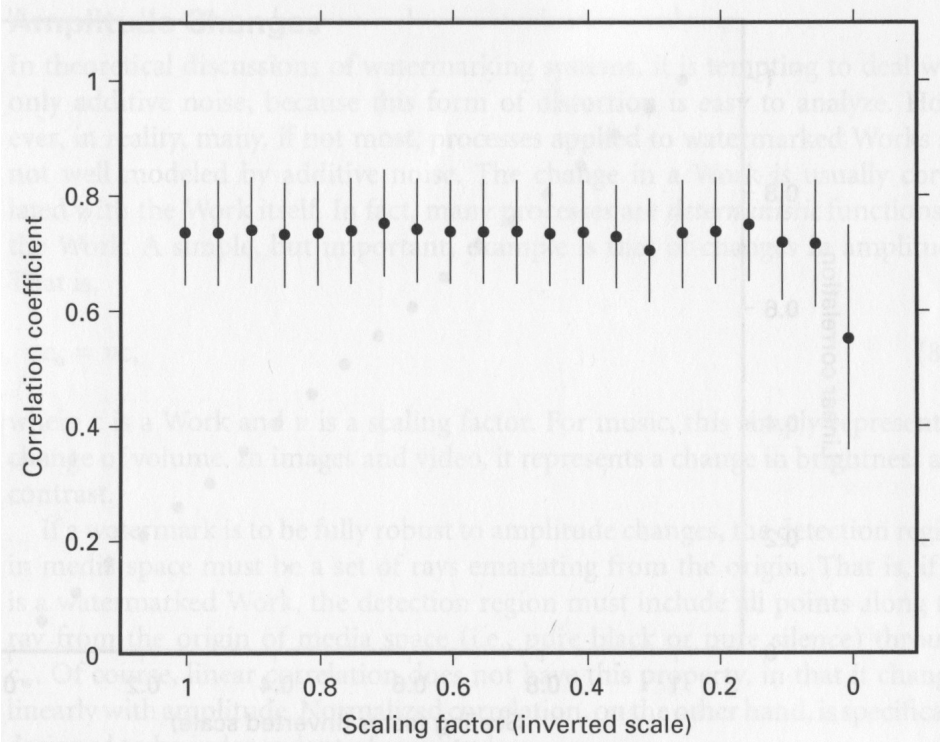


Fig. 8.8 Results of contrast scaling test using E_BLK_FIXED_R/D_BLK_CC watermarking system. The points show the mean detection values obtained. The error bars indicate the standard deviations of detection values.

Plan

Le filtrage linéaire

$$c_{wn} = c_w \star f$$

avec $\star$ l'opération de convolution :
$(f \star g)[k] = \sum_{i=-\infty}^{+\infty} f(i) \times g(k-i)$.

- Solution 1 : Pour être robuste, il faut insérer dans les fréquences que le filtre changera peu.
- Solution 2 : Pour être robuste, on peut insérer dans la phase de TF (il n'y a pas de modification de la phase lorsque le filtre est symétrique).

Le filtrage linéaire - corrélation linéaire fixée

Expérimentation 1 : 2000 images tatouées avec insertion à corrélation linéaire fixée de valeur 2, message $m = 1$, et détection à $\tau_{lc} = 0.7$. Chaque image est distordue par un filtre gaussien (valeur du noyau $G(u, v) = \frac{1}{2\pi\sigma^2} e^{-(u^2+v^2)/(2\sigma^2)}$)

Le filtrage linéaire - corrélation linéaire fixée

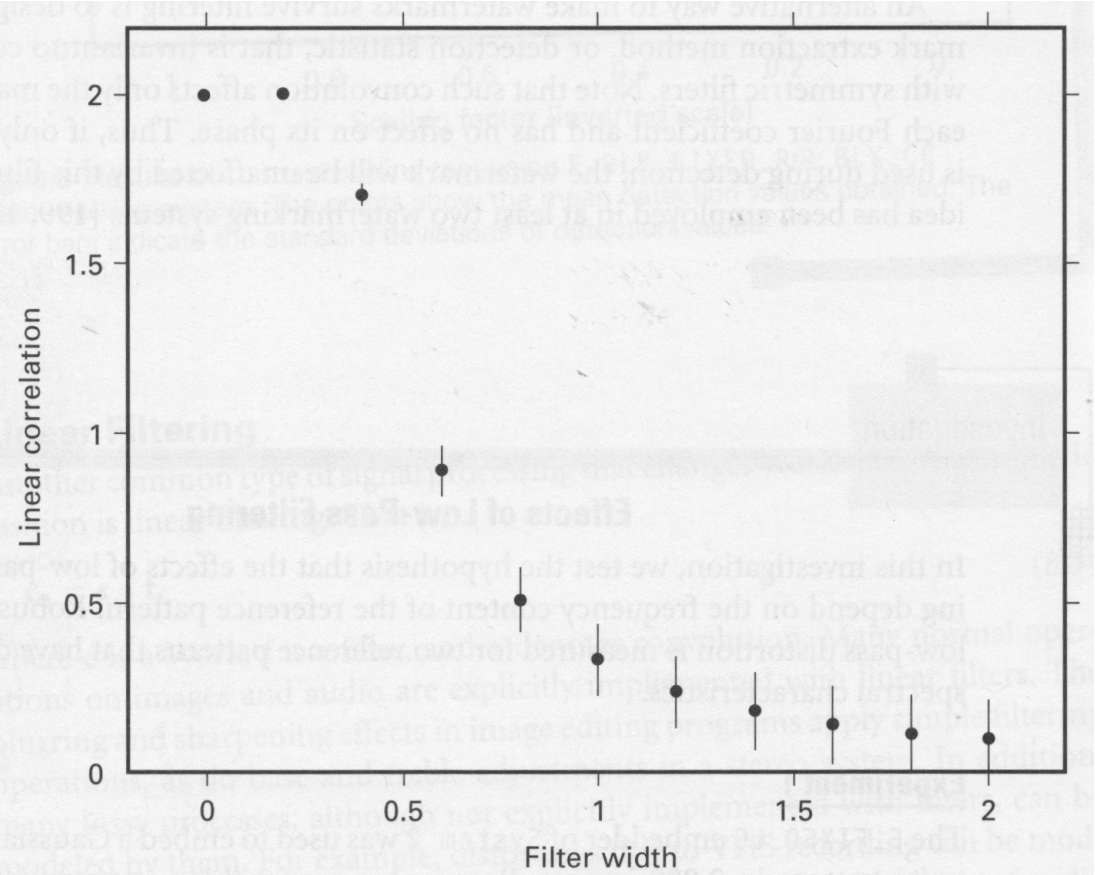
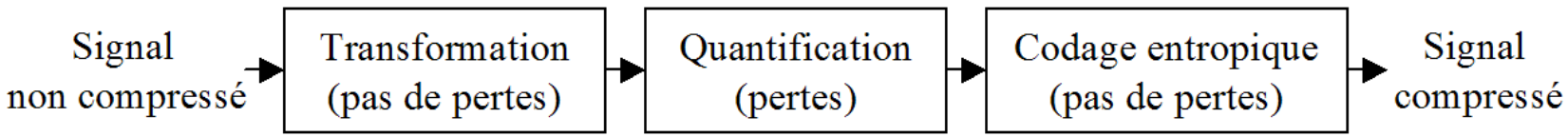


Fig. 8.9 Results of low-pass filtering test using E_FIXED_LC/D_LC watermarking system and a white-noise watermark reference pattern. The points show the mean detection values obtained. The error bars indicate the standard deviations of detection values.

Plan

La compression avec perte - la quantification

La plupart des schémas de compression avec perte suivent le schéma suivant :



Pour un pas de quantification q constant, un signal tatoué quantifié devient :

$$c_{wn} = q \left\lfloor \frac{c_w[i]}{q} + 0.5 \right\rfloor$$

La compression avec perte - effet de la simulation JPEG

Expérimentation 1 : 2000 images tatouées avec insertion à corrélation linéaire fixée de valeur 1, message $m = 1$, et détection à $\tau_{lc} = 0.7$. Dans chaque bloc DCT, chaque coefficient est quantifié par $q(i,j) \times Q$, avec Q le niveau de quantification global et $q(i,j)$ un terme de la matrice de quantification de luminance de JPEG.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

La compression avec perte - effet de la simulation JPEG

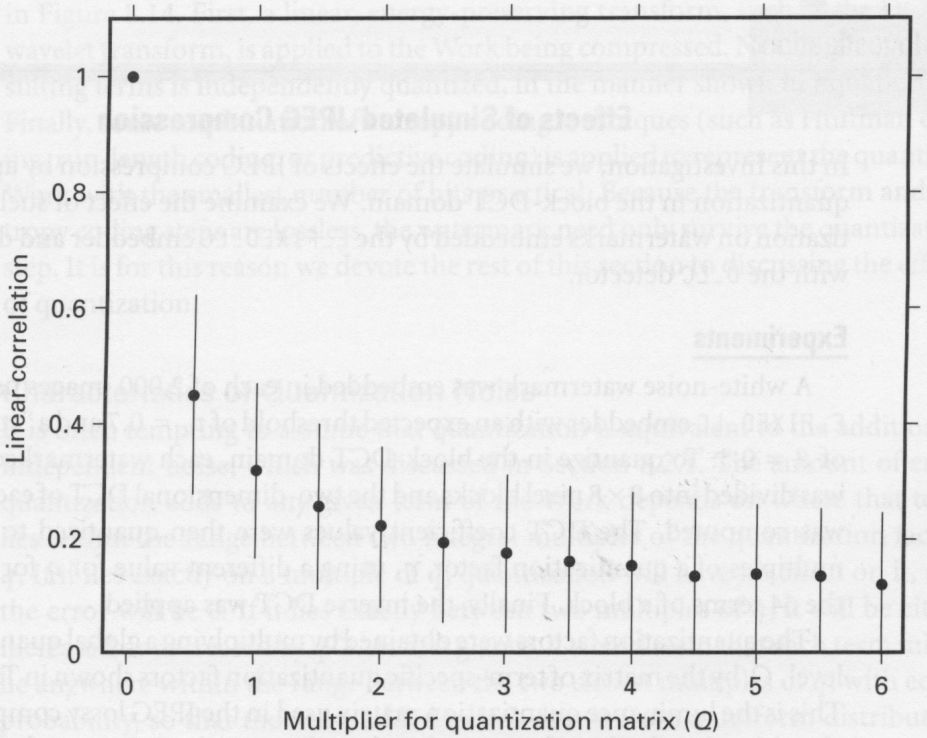


Fig. 8.15 Effect of quantization on linear correlation detection. Two thousand images were watermarked with white-noise reference marks, using the E_FIXED_LC embedding algorithm ($\tau_{lc} = 0.7$, $\beta = 0.3$). They were then converted to the block DCT domain, and the DCT coefficients were quantized by quantization factors computed as $Q \times q[i]$, where Q is a global multiplier (x-axis in this graph), and $q[i]$ is a frequency-dependent quantization value (see Table 8.1). Points show mean detection values. Bars show plus and minus one standard deviation.

La compression avec perte - effet de la simulation JPEG

On peut penser que le bruit de quantification est assimilable à un bruit additif de distribution uniforme sur $[-q/2, q/2]$. Vrai pour q très faible mais rapidement cela devient faux.

Quelques distortions géométrique

Quelques distortions géométriques :

translation	rotation
inclinaison	transformation perspective
scaling	changement de ratio
cropping	stirmark
print & scan	...

Quelques distortions géométriques : stirmark

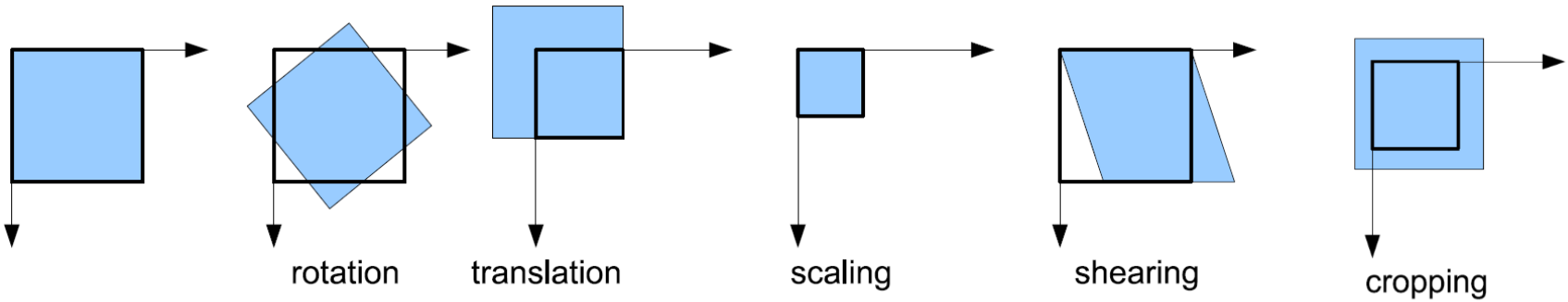


Fig.: Différentes déformations

Quelques distortions géométriques : stirmark

Fig.: Illustration de l'attaque stirmark

Quelques distortions géométrique

Les différentes approches de contre-attaque :

- 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)

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	:	$\begin{pmatrix} 1 & 0 \\ b & 1 \end{pmatrix}$

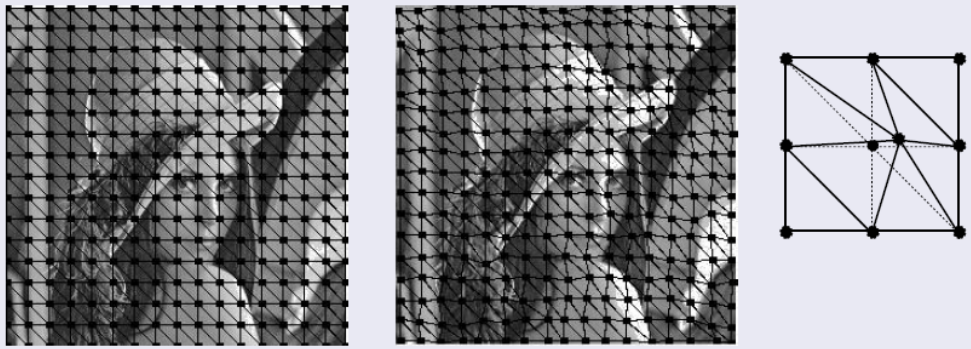
Il existe également des modèles plus complexes (perspective, warping, ...).

Remarque : Les schémas basés corrélation ont généralement une certaine robustesse aux faibles déformations.

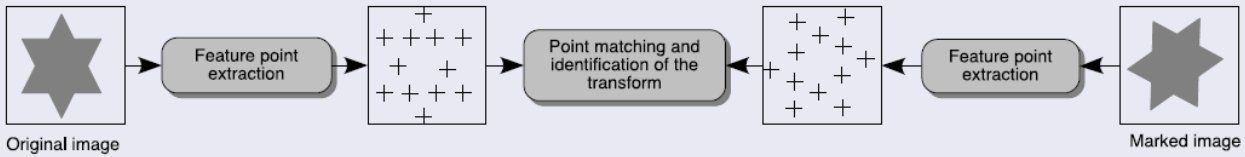
Plan

synchronisation par détection non aveugle

Geometrical compensation using a Tessellation



Geometrical compensation using a feature points



Plan

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.

Exemple de distortions acceptables

La solution par recherche exhaustive pose deux problèmes :

- Il y a un grand nombre d'applications du détecteur,
- Si p_{fp} est la probabilité de faux positif d'un "random-work". Après N détection 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

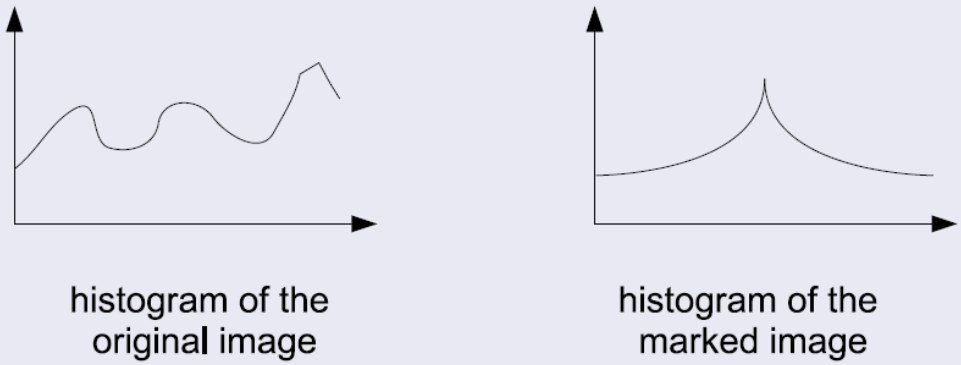
Espace invariant : Luminance

Average luminance embedding (video)

- sequence $[I_1, I_2, I_3, ..., I_n]$
- to be watermarked vector :
  $\mathbf{X} = [DC(I_1), DC(I_2), DC(I_3), ..., DC(I_n)]$
- Watermarking using SS techniques : $\mathbf{Y} = \mathbf{X} + \mathbf{W}$
- Effect of a crop : $\mathbf{Z} = \mathbf{Y} + \mathbf{N}$ (additive noise)

Espace invariant : Histogramme

Embedding by histogram modification (Images)



histogram of the original image

histogram of the marked image

- Detection using model matching
- Robust ot Stirmark
- Problem regarding security : every-body can compute an histogram and modify it...

Espace invariant : Fourier Mellin

La translation d'un signal ne produit pas de modification du module de la transformée de Fourier. Soit un signal 1D $c(t)$, le "scaling" sur l'axe temporel est également un "scaling" sur l'axe des fréquences dans le domaine de Fourier :

$$|\mathcal{F}\{c(st-\delta)\}| = \frac{1}{s}|C(f/s)|$$

avec $c(t)$ le signal variant suivant l'axe t, δ une translation, s le "scaling", $\mathcal{F}$ la transformée de Fourier, C le signal résultant de la transformée de Fourier variant suivant l'axe f.

Espace invariant : Fourier Mellin

$$|\mathcal{F}\{c(st-\delta)\}| = \frac{1}{s}|C(f/s)|$$

Si l'on passe en représentation logarithmique l'axe des fréquences dans le domaine de Fourier, le scaling s sur l'axe des fréquences devient une simple translation :

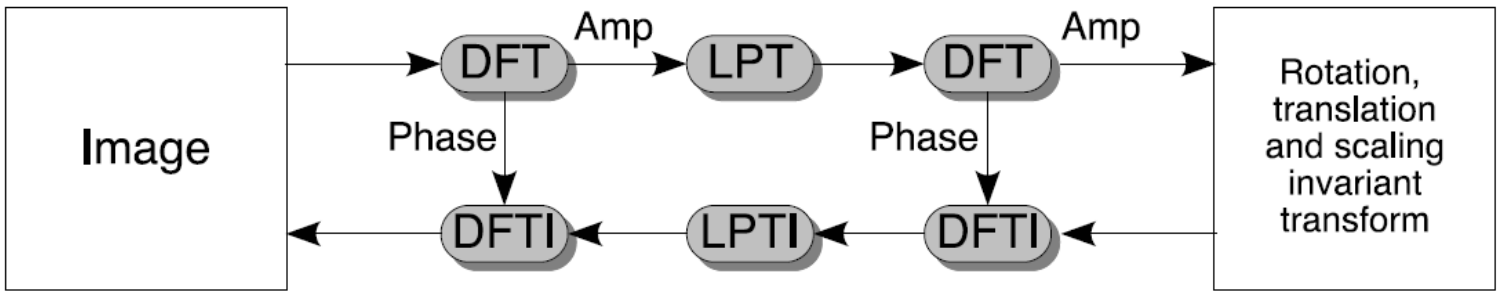
$$\frac{1}{s}|C(log(f/s))| = \frac{1}{s}|C(log(f)-log(s))|$$

Avec cette représentation, la translation temporelle n'a aucun effet (plus de terme δ) et le scaling temporel est juste une translation (terme $log(s)$). En appliquant une seconde fois la transformée de Fourier, le seul effet encore visible sera une simple variation d'amplitude.

Espace invariant : Fourier Mellin

$$|\mathcal{F}\{\frac{1}{s}|C(log(f) - log(s))|\}| = \frac{1}{s}\mathcal{F}\{|C(log(f))|\}|$$

Pour les images, le domaine de Fourier-Mellin est invariant aux translations, scalings et rotations. Au lieu de passer dans un domaine logarithmique on passe dans le domaine log-polaire ($x = e^{\mu}cos(\theta), y = e^{\mu}sin(\theta)$) :



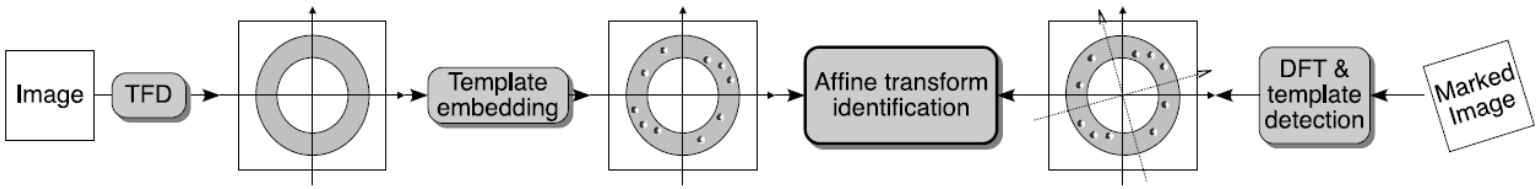
Plan

synchronisation ou recalage

Le recalage (synchronisation pour l'audio) consiste à ré-aligner l'hôte et la marque avant détection de la marque. Pour ceci, lors du tatouage on ajoute un pattern de synchronisation. À la détection, on recherche le pattern de synchronisation, on inverse la distortion et on lance la détection de la marque.

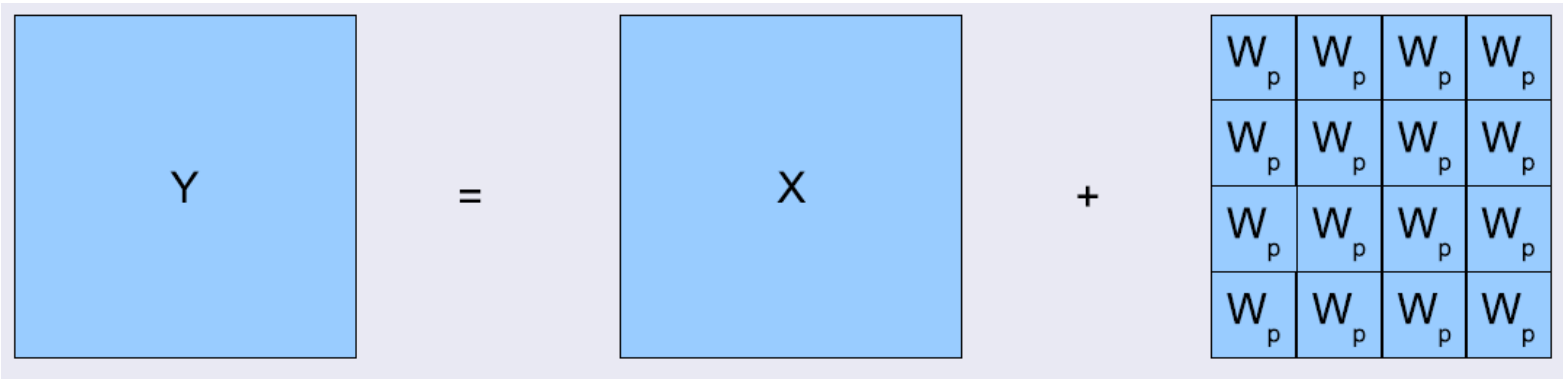
synchronisation ou recalage - Insertion de template

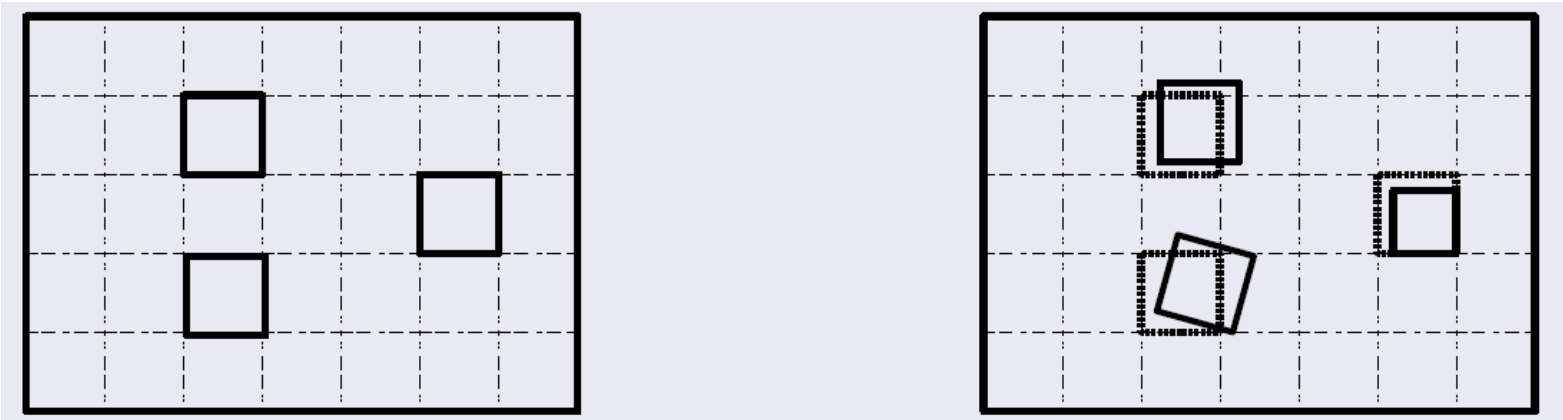
Insertion dans le domaine de Fourier de pics (template).



synchronisation ou recalage - Insertion de séquences périodiques

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





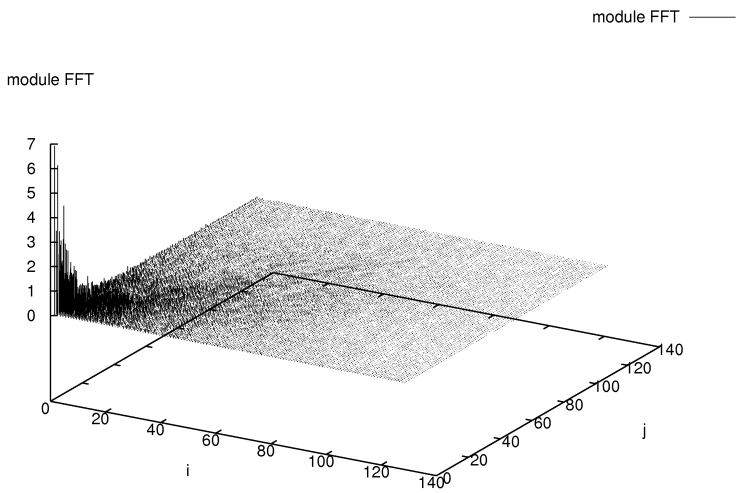
synchronisation ou recalage - Insertion de séquences périodiques

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

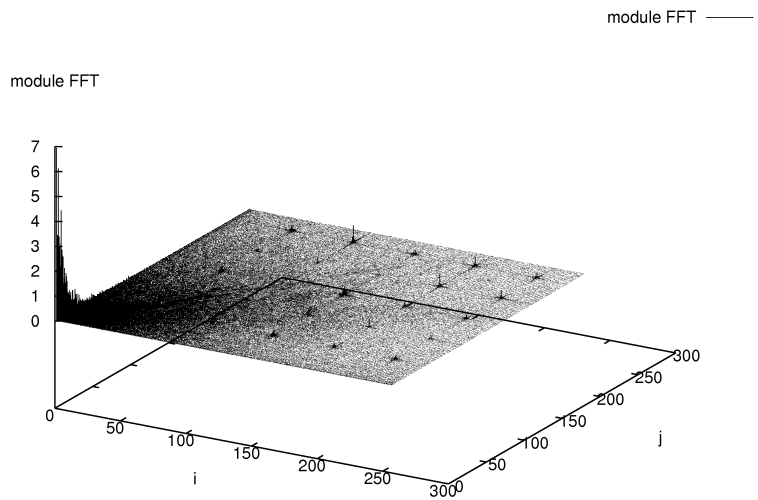
original

pattern ajouté

synchronisation ou recalage - Insertion de séquences périodiques



module FFT image originale



module FFT image avec pattern

Problème : L'insertion périodique n'est pas sûre ; la supression des pics par un attaquant dans le domaine DFT supprime la possibilité de re-syncrhoniser.

synchronisation ou recalage - Insertion de séquences périodique

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

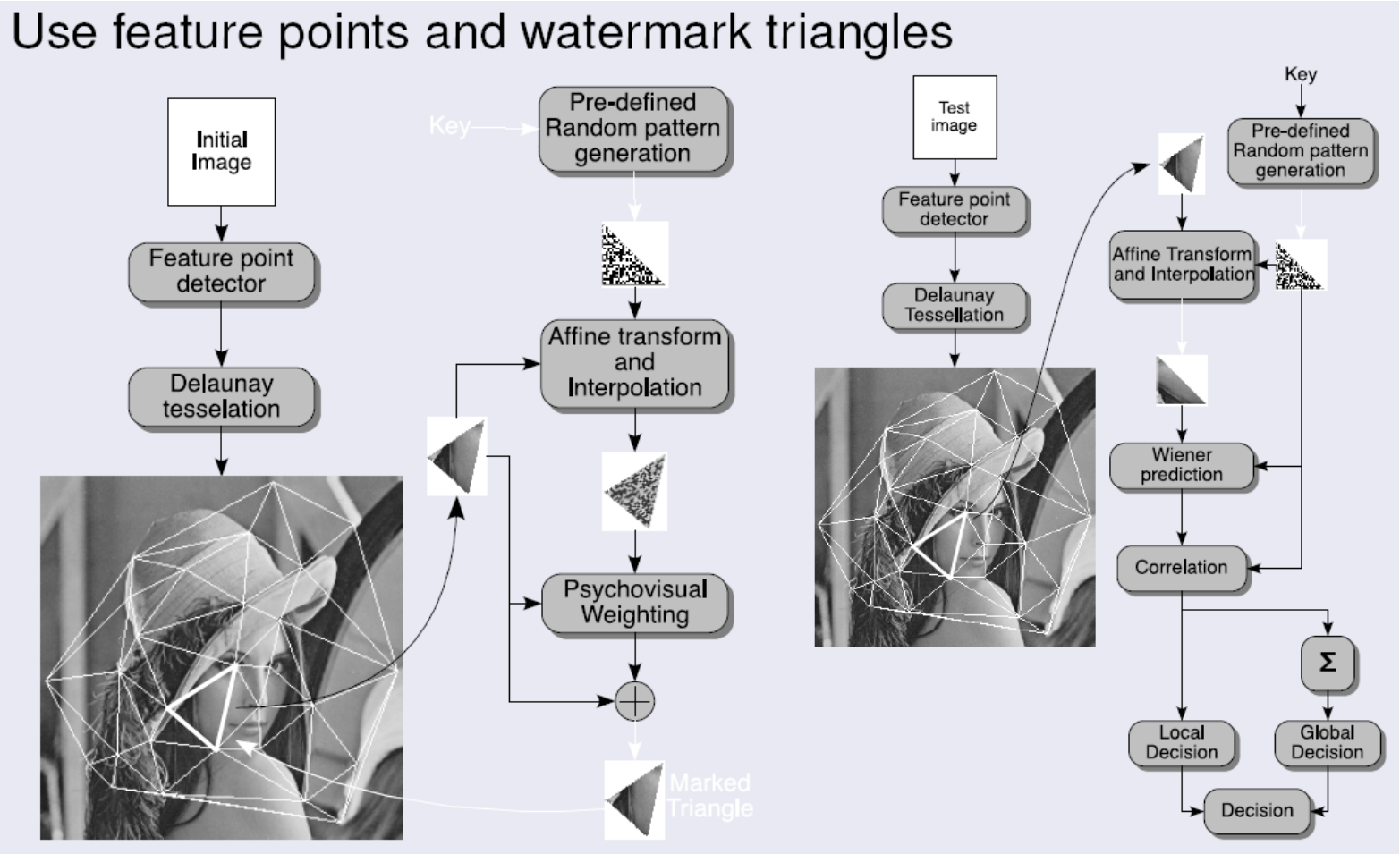
...	...	...
W[(i-k1-k2) mod N]	W[(i-k2) mod N]	W[(i+k1-k2) mod N]
W[(i-k1) mod N]	W[i]	W[(i+k1) mod N]
W[(i-k1+k2) mod N]	W[(i+k2) mod N]	W[(i+k1+k2) mod N]

synchronisation ou recalage - Signal autocorellant

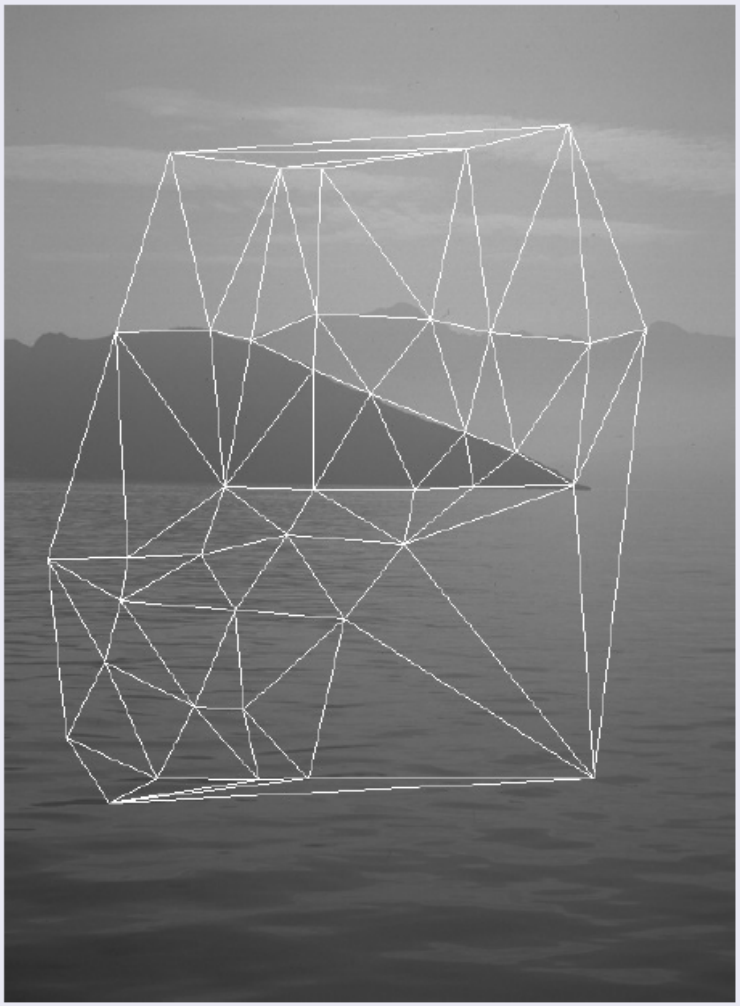
Remarque : Le pattern de synchronisation inséré peut à la fois servir de synchronisation et de pattern contenant de l'information. La détection peut être réalisée par autocorélation. Les pics de corrélation permettent d'identifier la périodicité du pattern et donc de corriger (en plus de la rotation et de la translation) un changement d'échelle. Le problème de la présence de pics reste une faille de sécurité.

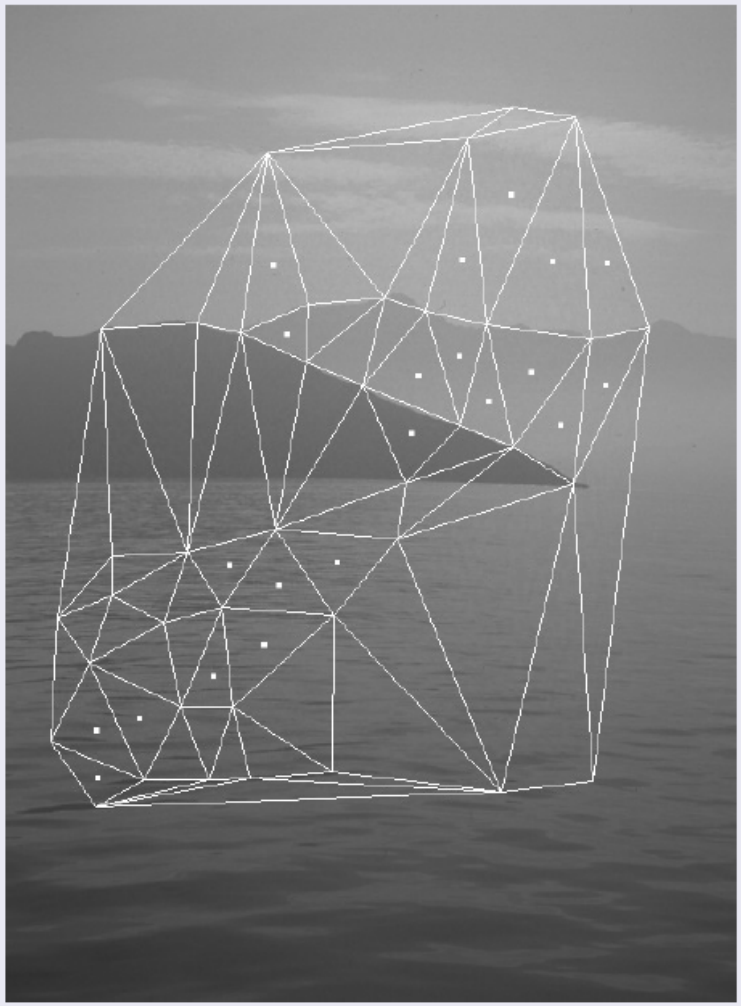
Plan

synchronisation implicite

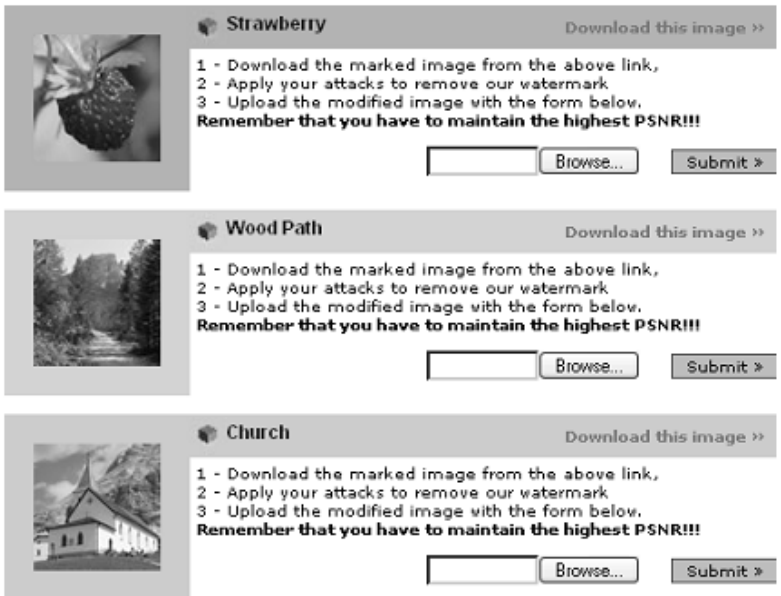


synchronisation implicite (tatouage basé contenu)





Quelques mots sur BOWS-1 : Break Our Watermarking System - 1



(a)

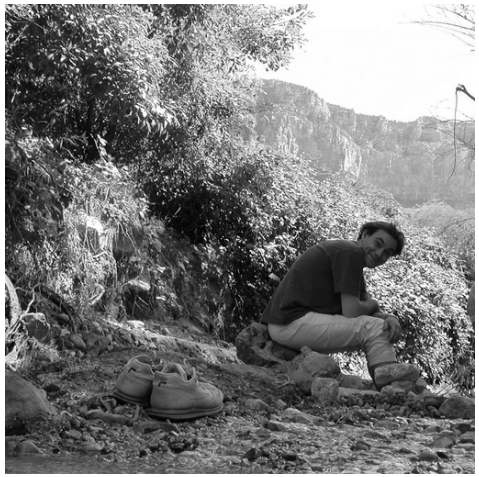
(b)

Quelques mots sur BOWS-1 : Break Our Watermarking System - 1

- **Première phase 15 December 2005 au 16 Mars 2006 :**
  Equipe gagnante de Scott Craver de l'université de Binghamton : PSNR(Strawberry)=39.69dB, PSNR(WoodPath)=39.67dB, PSNR(Church)=38.47dB.
- **Deuxième phase 17 mars au 15 juin :**
  L'algo est M.L.Miller, G.J.Doerr, and I.J.Cox, "Applying informed coding and embedding to design a robust, high capacity watermark," IEEE Trans.on Image Processing 13, pp.792-807, June 2004.
  Andreas Westfeld de TU Dresden : PSNR(Strawberry) = 60.74dB, PSNR(WoodPath) = 57.05dB, PSNR(Church) = 57.29dB,

Quelques mots sur BOWS-2 http ://bows2.gipsa-lab.inpg.fr/





- Episode 1 : Robustness against image processing Jul 17, 2007 - Oct 17, 2007
- Episode 2 : Sensitivity against oracle attacks Oct 17, 2007 - Jan 17, 2008
- Episode 3 : Security against information leakages Jan 17, 2008 - Apr 17, 2007

Ce qu'on n'a pas vu

- les modèles perceptuels utilisables pour le tatouage (exemple Watson),
- l'analyse de la sécurité des schémas par théorie de l'information,
- les attaques à la sécurité,
- les schéma de tatouage fragiles et semi-fragiles,
- les schéma de tatouage révérsibles,
- le tatouage asymétrique,
- les schémas de tatouage pour la 3D, le son, la vidéo, le texte, les programmes ...
- la stéganographie,
- les fonctions de hash perceptuel, ...