Méthode de tatouage fondée sur le contenu

Patrick Bas, Jean-Marc Chassery, Benoît Macq

Méthode de tatouage fondée sur le contenu

P. Bas, J-M. Chassery*et B. Macq

L.I.S. Laboratoire des Images et des Signaux, BP. 46, Saint Martin d'Heres, 38402, France

Laboratoire Tele, Bâtiment Stevin, Place du Levant, B-1348 Louvain-la-Neuve, Belgium

Abstract

Le tatouage d'images consiste à insérer une signature invisible et indélébile dans une image. Il permet de répondre à des problèmes de droit d'auteur ou d'intégrité. Les transformations géométriques peuvent cependant provoquer une perte de synchronisation et ainsi empêcher la détection de la signature. Nous proposons une méthode de tatouage fondée sur le contenu qui utilise un détecteur de points d'intérêts pour lier la signature au contenu de l'image. La détection de point d'intérêts permet de créer une partition triangulaire et la signature est ensuite insérée dans chacun des triangles. Nos résultats montrent que la méthode présentée est robuste aux déformations géométriques tels que Stirmark.

Mots clefs: Tatouage, Watermarking, contenu de l'image, transformations géométriques, points d'intérêts, partitionnement triangulaire, schéma additif

1 Introduction

Les documents numériques sont par essence très volatiles, cette propriété pose de nombreux problèmes car une image numérique peut être facilement copiée sans pour autant provoquer de perte. L'image peut également être représentée sous des formats multiples ce qui condamne toutes insertions d'informations autres que l'image comme par exemple des entêtes ou des fichiers attachés. Une image numérique peut

*Auteur de correspondance: E-mail: Jean-Marc.Chassery@inpg.fr; Tel: (33) 04 76 82 62 63, Fax: (33) 04 76 82 63 84

aussi être manipulée et modifiée sans que l'opération soit pour autant décelable. Le tatouage (appelé Watermarking en anglais) a pour objectif d'insérer dans l'image une information permettant de répondre à ces différents problèmes.

La marque peut contenir un numéro d'identification pour mettre en oeuvre un système de copyright, une description du contenu permettant son indexation ou bien encore une information "fragile" qui permettra son authentification.

La marque insérée ne doit pas surcharger l'image et doit donc être **invisible**: elle est contenue dans l'image mais n'est pas perceptible. La signature doit aussi être **indélébile**: une fois insérée dans l'image, il doit être impossible de l'enlever.

Cette deuxième condition implique de nombreuses contraintes. Dans le contexte de la protection des droit d'auteurs par exemple, la marque doit être robuste aux opérations classiques de sous/sur quantification, aux opérations de compression, de conversion N-A/A-N (impression et acquisition), aux opérations de filtrage (rehaussement de contours, lissage) et aux transformations géométriques.

2 Schéma de tatouage additif

Les méthodes de tatouage peuvent être décomposées en deux classes: la classe des schémas additif et la classe des schémas substitutifs [Bas00]. Nous détaillerons dans cet article le principe des schémas additifs qui servira de base pour le schéma qui sera présenté.

Les schémas additifs constituent une classe particulière de méthodes où la signature, qui représente le signal, est ajoutée à des composantes de l'image correspondant au bruit.

Dans un tel contexte, la difficulté consiste à mettre en forme le signal de telle manière qu'il puisse être détecté malgré la présence de l'image.

2.1 Insertion de la signature

Lorsque la méthode de tatouage appartient à la classe des schémas additifs, l'insertion de la signature peut se décomposer en plusieurs étapes (cf Fig 1):

1. Des composantes sont extraites de l'image originale I. Par "composantes" nous entendons l'image elle-même ou bien le produit d'une transformation fréquentielle (TCD, TFD) ou multirésolution (Ondelettes). Ces composantes peuvent être réordonnées en utilisant une clef secrète K, cette opération ayant pour effet de brouiller le domaine d'insertion. Les composantes extraites forment alors le vecteur $C_K(I)$.

2. Une signature de base que nous nommerons $W_b(K)$ est ensuite générée. Cette séquence est construite à l'aide d'un générateur aléatoire et dépend également de la clef secrète K.

3. Un message binaire $M = \{m_1, ..., m_n\}, m_i \in \{0; 1\}$ peut éventuellement être modulé par la séquence aléatoire W_b. On obtient alors le vecteur $W(K)$.

4. La signature $W(K)$ est ajoutée sur les composantes de l'image $C_K(I)$ pour obtenir les composantes $C_K(I_w)$ de l'image marquée:

$$C_K(I_w) = C_K(I) + W(K)$$

5. L'image marquée est reconstruite à partir des composantes $C_K(I_w)$.

La détection de la signature est réalisée à partir d'un vecteur d'observation r. En effet, si l'on considère que la signature est transmise à travers un canal perturbé par un bruit blanc gaussien additif, la corrélation entre Y et W permet d'obtenir une information révélatrice de la présence du signal. Cette corrélation peut s'écrire sous la forme:

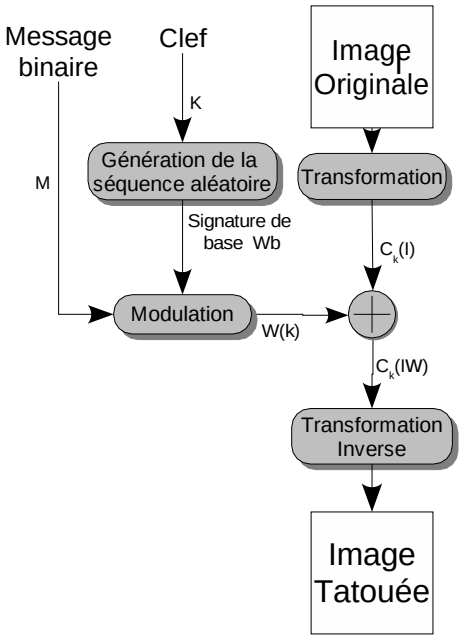

Figure 1: Insertion de la signature pour des schémas additifs.

$$r =< W; Y >= \sum_{i,j} w_{i,j} y_{i,j} \tag{1}$$

Si la signature est présente (H_1):

$$r(H_1) =< W; I + W >=< W; I > + < W; W > \# < W; W > \tag{2}$$

Si la signature n'est pas présente (H_0):

$$r(H_0) =< W; I >\ll r(H_1) \tag{3}$$

La procédure permettant de détecter la signature peut alors être représentée par les étapes suivantes (cf Fig 2):

1. Après une éventuelle transformation de l'image, les composantes tatouées sont extraites.

2. La séquence aléatoire de base W_b est générée à partir de la clef secrète.

3. Les composantes tatouées sont ensuite corrélées avec la séquence de base.

4. Le message peut enfin être décodé.

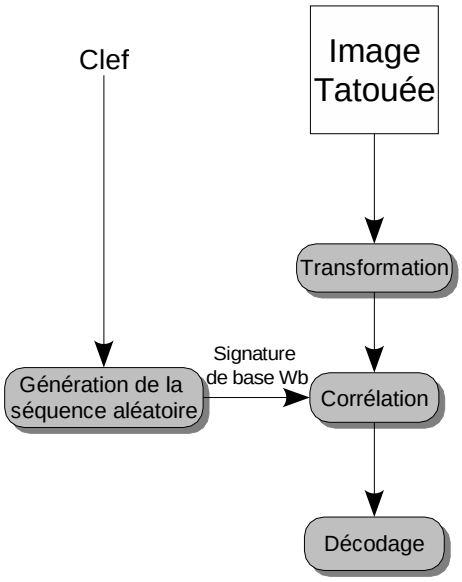

Figure 2: Détection et lecture la signature par addition.

3 Transformations géométriques et désynchronisation

Dans le cas des méthodes de tatouage additives comme substitutives, la détection de la signature est conditionnée par l'utilisation implicite du repère d'échantillonnage de l'image. Ainsi lorsque l'image subit une transformation géométrique, un algorithme classique ne pourra pas détecter la signature sans avoir au préalable identifié la transformation géométrique. Cette faiblesse a été exploitée pour générer des logiciels d'attaque permettant de rendre la détection de la signature impossible.

Le logiciel Stirmark a été proposé par Petitcolas et Kuhn [RJA98]. La principale "attaque" de ce logiciel consiste à simuler le traitement subi par l'image après son impression et son acquisition par un scanner. Il s'agit principalement de distorsions géométriques appliquées à l'image. Visuellement, Stirmark ne dégrade pas l'image. Pourtant l'algorithme applique de légères transformations géométriques (compositions de rotations et de translations) qui permettent de déplacer la signature afin que celle-ci ne soit plus synchronisée lors de la détection (cf Figure 3).

Il est à noter que si l'attaque StirMark génère une distorsion géométrique locale, les distorsions globales

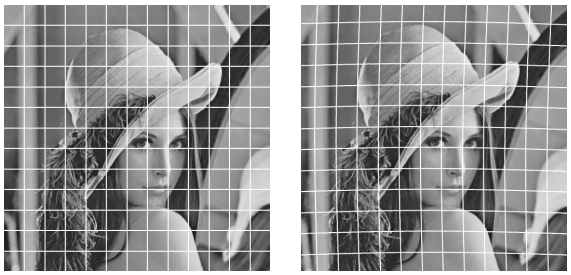

Figure 3: A gauche image originale, à droite image après Stirmark. En observant la grille, on peut voir apparaître de légères déformations.

telles que les rotations, translations, fenêtrage ou changements d'échelles sont tout aussi préjudiciables à la détection de la signature.

4 Tatouage fondé sur le contenu

Plusieurs approches ont été développées pour remédier aux problèmes de perte de synchronisation après une transformation géométrique. Certaines utilisent un domaine d'insertion invariant aux transformations affines [ORP98][LBC+00], d'autres des propriétés cycliques de la signature [Kut98][HSG99][DM00] ou encore l'insertion de mires [PP99]. Certaines méthodes s'appuient aussi sur l'image originale afin d'identifier la transformation encourue [DBHC99][SWD99][AT00].

Nous proposons une approche différente qui consiste à lier la signature au contenu de l'image. Le repère d'insertion n'est alors plus un repère artificiel mais un repère dépendant d'un descripteur du contenu de l'image.

Dans ce travail nous avons utilisé les détecteurs de points d'intérêts pour obtenir une description du contenu de l'image.

4.1 Détecteurs de points d'intérêts

Nous avons utilisé le détecteur de Harris pour obtenir un ensemble de points décrivant le contenu d'une image. Ce détecteur fut au départ développé pour permettre la reconstruction 2D/3D [HS88], il est simple d'implantation car il s'appuie sur les caractéristiques différentielles de l'image.

La réponse du détecteur de Harris s'écrie en fonction des dérivées partielles de l'image notées X et Y.

$$X = I \otimes [-1, 0, 1] \approx \delta I / \delta x \tag{4}$$

$$Y = I \otimes [-1, 0, 1]^T \approx \delta I / \delta y \tag{5}$$

L'expression de la réponse R_H est donnée par

$$R_H = Det(M) - kTr^2(M) \tag{6}$$

k étant une constante qui est définie préalablement afin de maximiser la robustesse des détecteurs de points d'intérêts et M est définie par:

$$M = \begin{bmatrix} A & B \\ B & C \end{bmatrix} \tag{7}$$

avec

$$A = X^2 \otimes w \tag{8}$$

$$B = Y^2 \otimes w \tag{9}$$

$$C = (XY) \otimes w \tag{10}$$

où w représente une fenêtre de voisinage circulaire de forme gaussienne. L'extraction des points d'intérêt s'effectue ensuite par seuillage de la réponse R_H suivie d'une recherche des maxima locaux. Dans notre étude nous avons décider de prendre un voisinage important (cercle de 36 pixel) afin d'obtenir une répartition homogène des points d'intérêts dans l'image.

4.2 Insertion de la signature

L'algorithme général d'insertion de la signature illustré sur la figure 4 est très proche d'un algorithme de tatouage additif opérant dans le domaine spatial. Contrairement aux schémas classiques, le repère d'insertion s'appuie sur la détection de points d'intérêts et est donc lié au contenu de l'image. La détection de point d'intérêts permet d'obtenir un partionnement triangulaire de l'image et la signature est insérée de manière additive dans chaque triangle. Il se décompose en plusieurs étapes:

1. Une signature de base est générée à l'aide d'un générateur de séquences aléatoires. Cette signature et composée d'une succession aléatoire de $+1$ et de -1 localisée dans un triangle isocèle rectangle de taille fixe. Nous avons choisi comme taille du carré englobant le triangle égale à 64×64. Nous désignerons par T_w ce triangle de référence.

2. Une détection de points d'intérêt est appliquée sur l'image originale. Nous utilisons une version modifiée du détecteur de Harris.

3. Un partitionnement triangulaire de Delaunay [Dav95] est appliqué à partir de l'ensemble de points d'intérêt. Nous obtenons alors un ensemble de triangles: $T = \{T_i\}, 0 \leq i < N$.
   La signature est insérée dans chacun des triangles $T_k \in T$.

4. Le triangle T_w est transformé en un triangle $T_m = \mathcal{A}(T_w)$ en utilisant une transformation affine $\mathcal{A}$. Cette transformation est construite de telle sorte que T_m et T_k aient la même géométrie. La valeur des pixels qui se trouvent à l'intérieur de T_m est obtenue par interpolation spline-cubique[MN88].

5. Le triangle T_m est multiplié par un masque de pondération psychovisuelle qui est fonction du triangle T_k. Nous obtenons alors le triangle T_p. L'objectif du masque psychovisuel est de prendre en défaut le système visuel humain (SVH) et d'exploiter les différentes propriétés de masquage de l'oeil. Dans ce schéma, le masque est simplement obtenu en filtrant l'image par un masque Laplacien.

6. Le triangle marqué T_s est obtenu en calculant la somme entre T_k et T_p:

$$T_s = T_k + T_p$$

7. L'image tatouée est finalement créée en remplaçant chaque triangle T_k de la partition T par le triangle T_s.

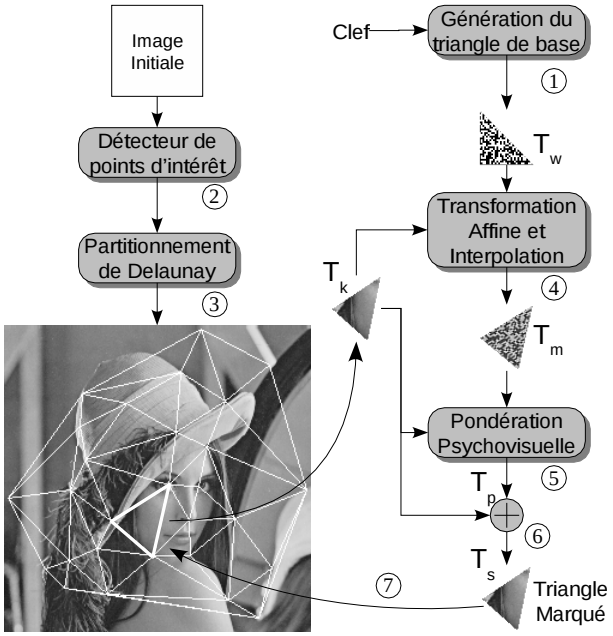

Figure 4: Principe du schéma d'insertion présenté.

4.3 Détection de la signature

Le principe de l'algorithme de détection est illustré sur la figure 5. Il se décompose en plusieurs étapes, les trois premières (génération du triangle aléatoire de base, détection des points d'intérêts et partitionnement de Delaunay) étant identiques au schéma d'insertion de la signature:

1. Le triangle T_k provenant de l'image est transformé en un triangle $T_\llcorner = \mathcal{A}(T_k)$ en utilisant une transformation affine $\mathcal{A}$. $\mathcal{A}$ est choisie de telle sorte que $T_\llcorner$ soit un triangle isocèle rectangle de taille 64×64, c'est à dire de même géométrie que le triangle de base.

2. A partir du triangle $T_{\llcorner}$, nous procédons à une prédiction de la signature par un filtrage de Wiener. Nous obtenons le triangle $\hat{T}_w$. Ce filtrage a pour objectif de séparer les composantes du triangle marqué qui sont rattachées à la signature et au triangle original [HPG99].

   Lorsque le triangle marqué est texturé, le rapport signal/bruit est plus élevé et la détection de la signature en utilisant la corrélation entre le triangle T_w et le triangle marqué $T_{\llcorner}$ est plus difficile. Le filtrage par prédiction de Wiener permet de diminuer la contribution du triangle $T_{\llcorner}$ lors de la corrélation.

3. Nous calculons ensuite la corrélation entre le triangle prédit et le triangle T_w.

4. La détection de la signature peut se faire à deux niveaux. Une première décision locale est effectuée en fonction de la valeur de corrélation obtenue pour chaque triangle. La corrélation $corr(T_w; \hat{T}_w)$ nous permet de décider si la signature est ou non présente dans l'image. Une signature ne peut être détectée que sous une probabilité de fausse alarme. La probabilité de fausse alarme P_{fa} représente la probabilité qu'une signature soit détectée dans une image alors que l'image n'a pas été tatouée.

   La signature sera détectée dans un triangle si:

$$corr(T_w; \hat{T}_w) \geq \eta(P_{fa}) \tag{11}$$

   où $\eta(P_{fa})$ est un seuil qui dépend de la probabilité de fausse alarme souhaitée.

5. Une décision globale est ensuite effectuée à partir de la moyenne des corrélations obtenues. Elle permet de pouvoir détecter la présence de la marque lorsque les corrélations calculées en chaque triangle sont toutes inférieures au seuil $\eta(P_{fa})$ mais que leurs valeurs cumulées sont suffisamment importantes pour attester la présence de la signature. Comme dans l'étape précédente, cette valeur est a nouveau comparée à un seuil.

6. La décision finale est obtenue à partir des deux décisions précédemment calculées: la signature est détectée dans une image si elle est détectée dans au moins un triangle ou/et si elle est détectée de

manière globale.

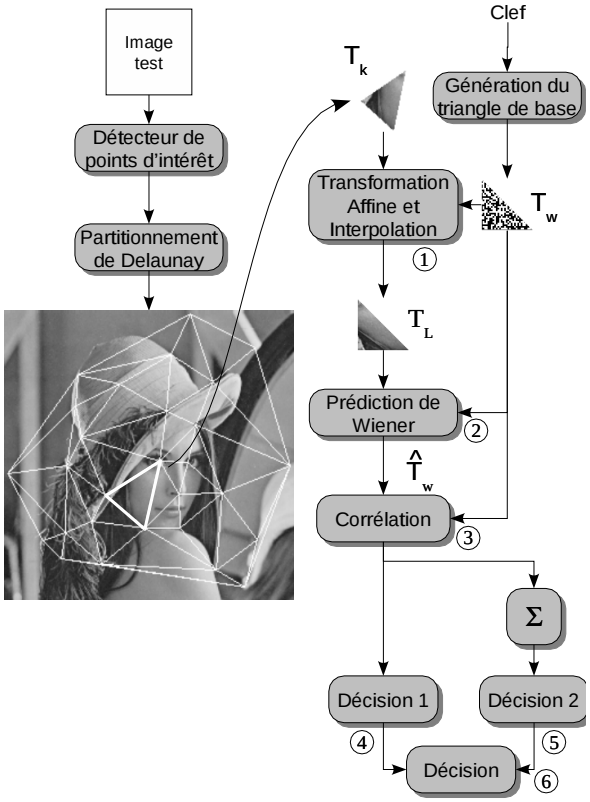

Figure 5: Principe du schéma de détection.

4.4 Résultats

Afin d'évaluer la robustesse du système de tatouage qui a été présenté dans ce chapitre, nous avons appliqué divers traitements sur 4 images test (*lena*, *tree*, *water* et *baboon*) de contenus très différents.

Dans chacun de nos tests, la marque insérée n'est pas perceptible sur l'écran, même lorsque l'on alterne l'image originale et l'image tatouée. La probabilité de fausse alarme nécessaire lors des étapes de décision est égale à 10^{-4}.

Le tableau Tab 1 représente le nombre de triangles détectés après l'attaque StirMark3.0. La figure 6 montre l'évolution de la partition après l'attaque. On note que la partition triangulaire suit majoritairement la déformation géométrique, ce qui permet de détecter la présence de la signature. L'utilisation de notre

schéma permet de contrer l'attaque Stirmark. En effet, la signature a pu être détectée sur chacune des images et chacune des partitions. On peut remarquer que la détection est plus aisée lorsque l'image est peu texturée (cas de *lena* et *water*). Cela peut s'expliquer par le fait que dans les images texturées la corrélation est souvent plus faible et le détecteur de points moins robuste.

	lena	*tree*	*water*	*baboon*
Local	23/66	3/66	21/65	3/62
Global	Ok	Ok	Ok	Ok

Table 1: Robustesse du schéma à l'attaque Stirmark.

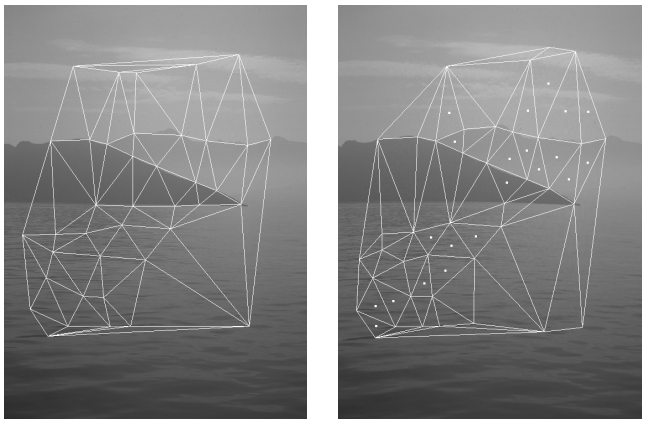

image originale et tessellation

image marquée après l'attaque StirMark

Figure 6: Effet de l'attaque StirMark3.0 sur l'image *water*. La marque a pu être détectée sur 21 triangles dans une partition qui en contient 65.

Nous avons également testé la robustesse de notre schéma face à des transformations géométriques globales (rotations, changement d'échelle, fenêtrage) mais aussi à des transformations plus classiques (compression Jpeg, impression et acquisition), dans chacun des cas la signature à pu être détectée.

5 Conclusion et perspectives

Nous avons proposé une approche nouvelle en tatouage fondée sur le contenu des images. Le schéma de tatouage présenté entre dans la catégorie des schémas de deuxième génération [KBE99] où ce n'est pas un tableau de pixels qui est tatoué mais les différents éléments de l'image. L'utilisation des points d'intérêt permet ainsi de lier la signature au contenu de l'image, mais aussi de marquer séparément les différents éléments de l'image.

Cette approche originale dégage de nouvelles perspectives dans le domaine du tatouage. Nous pouvons notamment utiliser d'autres descripteurs de contenus tels que les outils de segmentations qui permettront de tatouer les différents objets d'une image ou d'une séquence d'images.

References

[AT00] M. Alghoniemy and A. H. Tewfik. Geometric distortion correction in image watermarking. In *Proc. SPIE*, pages 82–89, January 2000.

[Bas00] P. Bas. *Méthodes de tatouages d'images fondées sur le contenu.* PhD thesis, Thèse de l'Institut National Polytechnique de Grenoble, France, 2000. manuscrit avaible on http://cepax6.lis.inpg.fr/these/Th_Bas.html.

[Dav95] F. Davoine. Compression d'images par fractales basée sur la triangulation de Delaunay. *Thèse de l'Institut National Polytechnique de Grenoble, France*, 1995.

[DBHC99] F. Davoine, P. Bas, P-A Hebert, and J-M Chassery. Watermarking et résistance aux déformations géométriques. In *Coresa99*, Institut-Eurecom, Sophia Antipolis, France, June 1999.

[DM00] D. Delanay and B. Macq. Generalized 2-d cyclic patterns for secret watermark generation. In *Proc. ICIP*, volume 2, pages 77–80, Sept 2000.

[HPG99] J. R. Hernandez and F. Perez-Gonzalez. Statistical analysis of watermarking schemes for copyright protection of images. *Proceedings of the IEEE*, 87(7):1142–1143, july 1999.

[HS88] C. Harris and M. Stephen. A combined corner and edge detector. In *4th Alvey Vision Conf*, pages 147–151, 1988.

[HSG99] F. Hartung, J.K. Su, and B. Girod. Spread spectrum watermarking: Malicious attacks and counter-attacks. In *Proc. of SPIE: Security and Watermarking of Multimedia Contents*, volume 3657, pages 147–158, San Jose CA, January 1999.

[KBE99] M. Kutter, S. K. Bhattacharjee, and T. Ebrahimi. Towards second generation watermarking schemes. In *IEEE-ICIP'99*, volume I, pages 320–323, Kobe (Japan), October 1999.

[Kut98] M. Kutter. Watermarking resisting to translation, rotation and scaling. In *Proc. of SPIE: Multimedia systems and applications*, volume 3528, pages 423–431, Boston, November 1998.

[LBC+00] C.-Y. Lin, J. A. Bloom, I. J. Cox, M. L. Miller, and Y.M. Lui. Rotation-, scale-, and translation-resilient public watermarking ofr images. In *Proc. SPIE*, pages 90–98, January 2000.

[MN88] D.P. Mitchel and A.N. Netravali. Reconstruction filters in computer graphics. *Computer Graphics*, 22(4):221–228, August 1988.

[ORP98] Joseph J. K. Ó Ruanaidh and Thierry Pun. Rotation, scale and translation invariant spread spectrum digital image watermarking. *Signal Processing*, 66(3):303–317, May 1998.

[PP99] Shelby Pereira and Thierry Pun. Fast robust template matching for affine resistant image watermarking. In *International Workshop on Information Hiding*, volume LNCS 1768 of *Lecture Notes in Computer Science*, pages 200–210, Dresden, Germany, 29 September –1 October 1999. Springer Verlag.

[RJA98] F. Petitcolas R. J. Anderson. On the limits of steganography. *IEEE Transactions on Selected Areas in Communiactions*, 16(4):474–481, May 1998.

[SWD99] Q. Sun, J. Wu, and R. Deng. Recovering modified watermarked image with reference to originale image. In *Proc. SPIE*, pages 415–424, January 1999.