Dix-septième colloque GRETSI, Vannes, 13-17 septembre 1999

Tatouage d'Images Résistant aux Transformations Géométriques

Patrick Bas, Jean-Marc Chassery
Laboratoire des Images et des Signaux (LIS), BP. 46 38402 Saint Martin d'Heres cedex
Patrick.Bas@imag.fr, Jean-Marc.Chassery@imag.fr

Résumé – Après avoir défini et présenté le contexte du Watermarking cet article propose une approche nouvelle en Watermarking qui n'utilise pas de signature de référence extérieure pour la détection. Elle permet d'être robuste aux transformations géométriques classiques. Pour cela elle s'appuie sur un détecteur de points d'intérêts et exploite une relation de similarités intra-blocs. Nous avons testé notre approche face à divers transformations géométriques.

Abstract – We present the area of Watermarking and a new scheme which does not use an external reference mark for the detection step of the mark. This scheme permits to be robust to classical geometric transformations. Is uses features points detector and an intra-blocs similarity relationship. We have confronted our scheme to different geometrical transformations.

1 Les Enjeux du Watermarking

Les images numériques sont des documents volatiles et difficiles à contrôler.

• Une image numérique peut être facilement copiée et cela sans aucune perte. Cela rend difficile la protection d'une image numérique en terme de droits d'auteurs.

• Une image numérique peut être représentée sous des formats multiples, ce qui condamne toute transmission d'in-formations annexes (entêtes, fichiers attachés).

• Une image numérique peut subir des opérations de filtrage, de compression ou de retouche qui peuvent changer le contenu sémantique de l'image sans que cela soit décelable.

Le Watermarking (traduction française: tatouage d'images) a pour objectif d'insérer dans l'image une information permettant de répondre à ces problèmes.
La marque peut contenir:
• un numéro d'identification pour mettre en oeuvre un système de copyright;
• une description du contenu permettant son indexation;
• une information "fragile" qui permettra son authentification.

Il existe deux principales contraintes en Watermarking: 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 difficile de l'enlever.
Cette deuxième condition implique de nombreuses contraintes. Dans le cas du copyright par exemple la marque doit être robuste aux opérations classiques de sous/sur quantification, aux opérations de compression (Jpeg, Jpeg-2000 basée sur les ondelettes), de conversion N-A/A-N (impression et acquisition), aux opérations de filtrage (rehaussement de contours, lissage) et aux transformations géométriques. Dans le cas de l'authentification la marque doit pouvoir aider à déceler le moindre changement du contenu de l'image.
Nous allons présenter dans ce document une méthode de Watermarking permettant d'être robuste à certaines transformations géométriques comme le fenêtrage, les rotations ou les translations.

1.1 Etat de l'art et schémas classiques

Dans les schémas classiques le mode d'insertion est inspiré des techniques d'étalement de spectre utilisées en télécommunications: une signature provenant d'un signal de référence généré à l'aide d'une clef est ajouté aux composantes de l'image.
L'insertion peut se faire dans le domaine spatial [9] ou transformé (coefficients DCT de l'image [3] blocs $8*8$ [10], ondelettes [6]). L'insertion peut aussi prendre en compte les propriétés psychovisuelles du système visuel humain [4].
Classiquement la détection s'effectue a l'aide d'une corrélation entre la signature de référence et les coefficients de l'image qui ont été marqués.
Lors de l'étape de détection, ces différents schémas sont très sensibles aux transformations géométriques. Par exemple si l'image marquée est modifiée par une translation, les coefficients marqués le sont aussi mais la signature de référence reste inchangée. La corrélation entre les deux signaux ne révèle plus la présence de la marque car ils ne sont plus synchronisés. Le logiciel *Stirmark* [8] permet ainsi de contrer de nombreux schémas de tatouage et constitue une référence en matière d'attaques.
Le schéma que nous présentons a pour but de s'affranchir de ces contraintes géométriques. Il existe également d'autres méthodes de cette catégorie. La méthode proposé par M.Kutter utilise la fonction d'auto-corrélation de la prédiction de la signature pour retrouver la transformation géométrique inverse [7]. Ruanaidh utilise la transformation de Fourier-Mellin qui est invariante aux rotations et

aux réduction d'échelle[5].F. Hartung propose une méthode quasi-exhaustive qui parcourt localement l'espace des transformations[1].

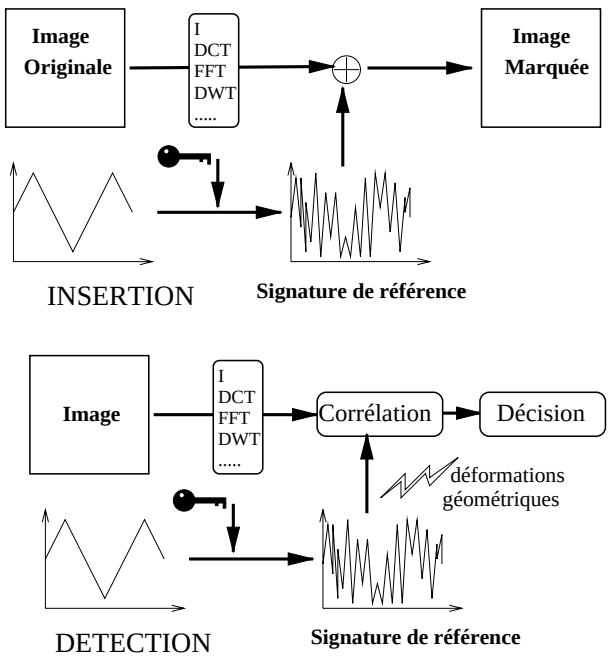

FIG. 1: Insertion Classique et Détection de la marque. L'insertion s'effectue par addition d'une signature de référence sur les coefficients de l'image. La détection s'effectue par corrélation entre la signature de référence et les coefficients tatoués. Cette étape est très sensible aux déformations géométriques.

2 Un schéma utilisant les similarités

Le schéma proposé n'utilise pas de signature de référence extérieure. La signature est "portée" par l'image. Le lien entre la signature de référence et la signature insérée est une relation de similarité. Ainsi si l'image subit des transformations géométriques, les relations de similarité demeurent conservées.
Des points d'intérêts (coin d'une images par exemple) servent de repères pour l'insertion des similarités. Si l'image subit des distorsions géométriques la majorité des points d'intérêts suivra ces distorsions.
L'insertion de la signature se décompose alors en deux étapes:
• la détection de points d'intérêts,
• l'insertion des similarités autour des points d'intérêts.

2.1 Sélection des blocs d'intérêts

La sélection de blocs d'intérêts permet de localiser des blocs qui seront invariants après une transformation géométrique. Ces blocs doivent contenir des composants géométriques de l'image. Nous avons donc utilisé le détecteur de Stephen-Harris qui permet de localiser les coins et les bords d'une image [2].A chaque point d'intérêts est associé un bloc. Les points d'intérêts génèrent alors un ensemble de blocs $\{D\} = \{D_1, ..., D_n\}$.

Le détecteur de Stephen-Harris calcule pour chaque pixel $I(x, y)$ la matrice suivante:

$$M = \begin{pmatrix} \frac{\delta I}{\delta x} \otimes G_w(x,y) & \frac{\delta I}{\delta x \delta y} \otimes G_w(x,y) \\ \frac{\delta I}{\delta x \delta y} \otimes G_w(x,y) & \frac{\delta I}{\delta y} \otimes G_w(x,y) \end{pmatrix}$$

ou $G_w(x, y)$ est un masque gaussien .
Le critère de sélection est la combinaison de deux invariants rotationnels de la matrice:

$$I_c = Det(M) - kTrace(M)^2$$

Les points d'intérêts sont alors sélectionnés par seuillage de I_c. La figure Fig 2 illustre l'efficacité du détecteur de Harris.

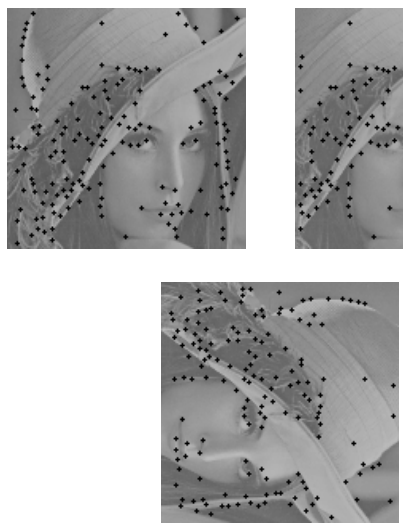

FIG. 2: Représentation des points d'intérêt en utilisant le détecteur de Harris. Les points d'intérêts sont en grande partie conservés après rotation et translation.

2.2 Insertion de la signature

La marque insérée est composée de portions de l'image afin d'obtenir des relations de similarités.
Le calcul de la marque insérée W_j et du bloc marqué $\hat{R_j}$ à partir du bloc sélectionné D_j se fait comme suit:

$$W_j = \alpha * Dyn(D_j) = \alpha * \frac{D_j - \bar{D_j}}{max(D_j - \bar{D_j})} \quad (1)$$

$$\hat{R_j} = Quant_s(R_j) + W_j + \frac{s}{2} \quad (2)$$

ou $Quant_s(R_j) = int(\frac{R_j}{s}) * s$, $\bar{D_j}$ représente la moyenne du bloc D_j, α est un paramètre qui décrit la force de l'insertion, s est le pas de quantification. $\hat{R_j}$ représente le bloc inséré issu de la relation de similarité entre D_j et R_j. Le réel $\frac{s}{2}$ permet de diminuer l'erreur de quantification

pendant la détection.

Le schéma d'insertion doit être robuste aux opérations de fenêtrage. Les similarités sont donc insérées localement autour de chaque bloc D_i. On peut décomposer cette partie en deux étapes (cf fig 3):

1. L'ensemble des blocs D est sélectionné en utilisant le détecteur de Harris.
2. Pour chaque bloc D_i, une similarité est insérée dans l'un des N blocs de la fenêtre locale. L'image marquée est ainsi créée. Dans notre étude nous avons arbitrairement choisi une dimension 4×4 pour chaque bloc D_i et $N = 16$ (fenêtre de taille 16×16).

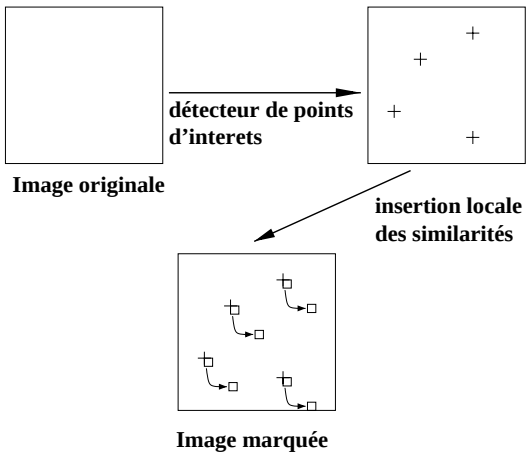

FIG. 3: Schéma d'insertion de la signature: détection des points d'intérêts grâce au détecteur de Harris. Insertion locale des similarités autour des blocs d'intérêts

2.3 Détection de la signature

L'ensemble des blocs domaine $\{D\} = \{D_1, ..., D_n\}$ est construit à partir de la détection des points d'intérêts de l'image traitée. On calcule ensuite le bloc W_j de la manière suivante:

$$W_j = \alpha * Dyn(D_j) = \alpha * \frac{D_j - \bar{D_j}}{max(D_j - \bar{D_j})} \quad (3)$$

Ensuite pour chaque bloc R_i appartenant au voisinage de D_j (fenêtre 4×4) le bloc $\hat{W_i}$ est construit:

$$\hat{W_i} = R_i - (Quant(R_i) + \frac{s}{2}) \quad (4)$$

ou $Quant(R) = int(\frac{R}{s}) * s$.

On extrait ensuite pour chaque bloc D_j le bloc dont l'erreur quadratique est la plus faible. On récupère la position relative du bloc par rapport à D_j.

2.3.1 Décision

Quand un bloc R_i^* est détecté, le nombre de blocs détectés à cette position est incrémenté. Une fois que l'ensemble des blocs $\{R\}$ est entièrement testé, la décision est prise en examinant l'incrément maximum parmi les 16 positions de la fenêtre locale. Ce maximum est ensuite comparé à un seuil T pour déterminer si une marque est présente dans l'image. Le tableau suivant construit à partir de simulations permet de fixer le seuil T du nombre de blocs détectés permettant d'avoir une probabilité de fausse alarme inférieur à 10^{-3} et 10^{-5}. T est fonction du nombre total de blocs.

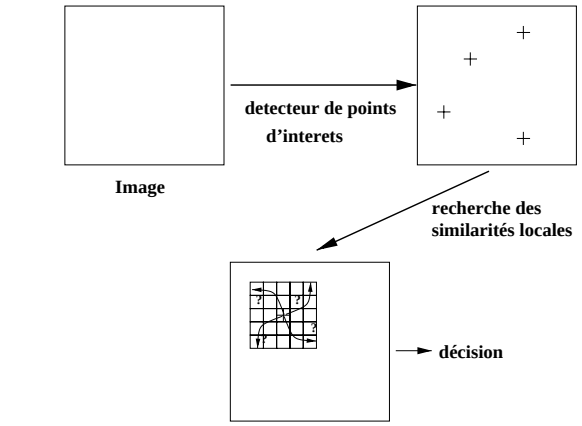

FIG. 4: Schéma de détection de la signature: on procède premièrement à une recherche des blocs d'intérêts, ensuite on effectue une recherche locale des similarités pour permettre une décision sur l'existence ou non de la marque.

nb de blocs	20	40	60	80	100	120	140	160	180
T $P_{fa} = 10^{-3}$	7	10	13	15	17	20	22	24	27
T $P_{fa} = 10^{-5}$	9	12	15	18	20	23	26	28	29

2.4 Résultats et Perspectives

Nous avons testé notre schéma face aux transformations géométriques classiques: rotations de 90 degrés, translations, effets miroir, fenêtrage (cf FIG:5). Dans chacun de ces cas la détection de la marque a pu être réalisée.
Notre schéma n'est cependant pas encore robuste aux rotations qui ne sont pas multiples de 90 degrés, ni à l'attaque menée par *Stirmark*.

Le point critique du schéma présenté porte sur la fiabilité du détecteur de point d'intérets. Nous sommes actuellement préoccupé par l'adaptation du détecteur et l'insertion de la signature en utilisant des méthodes d'étalement de spectre afin que le schéma global soit plus sensible aux transformations fines.

3 Conclusion

Nous avons présenté une approche nouvelle en Watermarking qui n'utilise pas de signature de référence extérieure. Elle permet d'être robuste aux transformations géométriques classiques. Pour cela elle s'appuie sur un détecteur de points d'intérêts qui permet de synchroniser la signature avec la marque de référence contenue dans l'image. La signature est basée sur une relation de similarité qui permet aussi d'être invariant aux transformations géométriques.
Ce travail a été réalisé dans le cadre du projet RNRT *Aquamars*.

(1)

(2)

(3)

(4)

FIG. 5: (1): image originale (lena $256 * 256$), dans tous les cas la marque a été retrouvée. (2) image marquée après rotation, (3) image marquée miroir, (4) fenêtrage de l'image marquée.

Références

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

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

[3] T. Leighton I. Cox, J. Killian and T. Shamoon. Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing*, 6(12):1673–1687, December 1997.

[4] B. Macq J.F. Delaigle, C. De Vleeschouwer. Watermaking algorithm based on a human visual model. *Signal Processing*, 1998.

[5] T Pun JJK Ruanaidh. Rotation, scale and translation invariant spread spectrum digital image watermarking. *Signal Processing*, pages 303–317, 1998.

[6] D. Kundur and D. Hatzinakos. Digital watermarking based on multiresolution wavelet data fusion. In *Special Issue on Intelligent Signal Processing*. IEEE, 1997.

[7] 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.

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

[9] D. Gruhl W. Bender and Morimoto. Techniques for data hiding. In *Proc. SPIE*, volume 2420, page 40, February 1995.

[10] J. Zhao and E. Koch. Towards robust and hidden image copyright labelling. In *Workshop on Nonlinear Signal and Image Processing*, Neos Marmaras, Juin 1995. IEEE.