



HAL
open science

Tatouage topologique des images numériques

Messaoud Mostefai, Samira Djebrani, Youssef Chahir

► **To cite this version:**

Messaoud Mostefai, Samira Djebrani, Youssef Chahir. Tatouage topologique des images numériques. Traitement du Signal, 2005, 22 (6), pp.575-590. hal-00324857

HAL Id: hal-00324857

<https://hal.science/hal-00324857>

Submitted on 19 Apr 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Tatouage topologique des images numériques

Messaoud Mostefai ¹, Samira Djebrani ¹, Youssef Chahir ²

¹ Institut d'informatique, Université de Bordj Bou Arréridj, BP 64, 34265, Algérie,
bbamos@wissal.dz – samirad76@yahoo.fr

² GREYC URA CNRS 6072, Université de Caen, BP 5186, 14032, France,
chahir@info.unicaen.fr

RESUME. Dans ce travail nous présentons une nouvelle approche pour le tatouage des images numériques basée sur la topologie des coupes. La technique proposée permet d'incruster une ou plusieurs marques dans une ou plusieurs parties de l'image localisées par un claque topologique contenant les composants connexes d'une coupe choisie. Le schéma de tatouage utilisé est spatial, additif et à clef secrète. Les expérimentations réalisées sur une base d'images importante montrent l'efficacité et la robustesse de la technique proposée.

ABSTRACT. In this work we present a novel watermarking scheme based on cross-section topology. The proposed technique allows to embed one or more watermarks on one or more places in the image localised by a topological cross-section which contains connexe components of a chosen cross-section. Used watermarking scheme is spatial, additive and with a secrete key. Experimental results on a representative database of images, shows the effectiveness and robustness of the proposed technique.

MOTS-CLÉS: Tatouage numérique – Topologie numérique – Topologie des coupes

KEYWORDS: Digital watermarking – Digital topology – Cross-section topology

1. Introduction

L'augmentation de la production et des échanges numériques via les réseaux ouverts comme Internet a favorisé l'exploitation illicites des travaux numériques, bafouant ainsi les droits de propriété intellectuelle.

Afin de contrer ce fléau, des chercheurs s'y sont mobilisés pour trouver des solutions numériques à ce problème qui est devenu actuellement un véritable axe de recherche appelé tatouage ou marquage (watermarking en anglais) [1][2][3].

Le principe commun aux différentes solutions proposées consiste à tatouer (signer ou marquer) le travail à protéger avec une signature imperceptible qui permet d'identifier le propriétaire tout en étant robuste aux attaques bien ou malveillantes [2].

Les différents systèmes de marquage proposés dans la littérature peuvent être classés dans une des deux catégories suivantes : Les systèmes qui agissent directement dans le domaine spatial [4][5][6], et ceux qui agissent dans le domaine fréquentiel [7][8][9]. Bien qu'ils présentent des avantages d'un point de vue simplicité de mise en œuvre et de calcul, les systèmes qui opèrent directement sur l'image sont généralement vulnérables face aux attaques géométriques. En effet, pour insérer une marque ces derniers utilisent des couples de pixels ou de blocs de pixels auxquels ils apportent de légères modifications (imperceptibles pour l'œil) qui respectent des règles de marquage établies d'avance. Toute transformation géométrique sur l'image tatouée conduit fréquemment à l'impossibilité d'extraire le tatouage.

A la différence des méthode spatiales, les méthode qui opèrent dans le plan transformé (Plan DCT, ondelettes, tourier...) permettent la construction de systèmes de marquage robustes face aux attaques de type géométrique (rotation, fenêtrage,...), ou de traitement du signal (compression, filtrage...) [2]. Ceci n'a pas freiné l'intéressement aux techniques spatiales qui restent de loin les plus rapides et les plus simples comparé aux techniques qui opèrent dans le plan transformé [4].

Nous présentons dans cet article une nouvelle approche de tatouage d'images qui s'appuie sur la topologie de l'image en niveaux de gris. La technique proposée permet d'incruster une ou plusieurs marques dans une ou plusieurs parties de l'image localisées par un calque topologique contenant les composants connexes d'une coupe choisie. Le schéma de tatouage utilisé est spatial, additif et à clef secrète. Contrairement aux méthodes de tatouage spatiales classiques, notre technique est robuste face aux transformations géométriques, car elle se base pour la localisation des points d'insertion sur le contenu de l'image (invariant face aux transformations géométriques) et non pas sur les coordonnées spatiales.

Dans ce qui suit, nous détaillerons notre démarche pour le tatouage topologique des images numériques, puis nous décrirons les algorithmes utilisés pour le tatouage et l'extraction de la signature, et en fin nous présenterons les résultats de tests de

robustesse effectués sur un ensemble d'images.

2. Notre démarche

L'approche proposée est basée sur les opérateurs topologiques de l'image qui demeurent les plus conservés quelque soit la nature de l'attaque (veillante ou malveillante) que peut subir l'image. Une ou plusieurs marques sont insérées dans une ou plusieurs parties de l'image originale suivant les propriétés topologiques des coupes choisies.

Le procédé de tatouage topologique (décrit dans la figure 1) est comme suit :

1. Extraction de l'image en niveaux de gris à partir de l'image d'origine en couleur.
2. Choix d'une ou plusieurs coupes parmi l'ensemble des coupes de l'image en niveau de gris en fonction des besoins du tatouage en quantité d'informations à insérer. Le choix de la coupe est aussi important, car il complique d'avantage la tâche d'extraction illicite de la marque.
3. Extraction des composants connexes de la coupe choisie qui serviront de guide pour la localisation des points d'insertion dans l'image originale. Ces derniers possèdent des composantes basses-fréquences importantes et par conséquent sont robustes face aux techniques de compression.
4. Génération d'une clef avec les paramètres d'insertion utilisés.
5. Insertion de la marque dans l'image originale (autour des composants connexes).

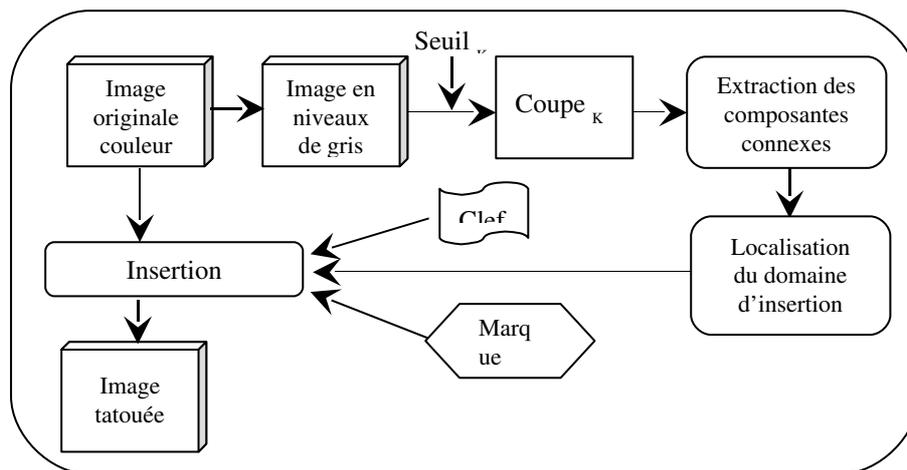


Figure 1. Notre démarche

3. Extraction des coupes

Une image en niveaux de gris est considérée comme l'empilement de plusieurs images binaires, appelées coupes [10] [11]. Chaque coupe est un seuil de l'image à un niveau de gris donné (K). Les valeurs binaires (0 ou 1) des éléments de la coupe K sont obtenues de la manière suivante :

$$\begin{aligned} \text{Si } P(x,y) \geq K \text{ alors } P_k(x,y) &= 0 \\ \text{Sinon } P_k(x,y) &= 1 \end{aligned} \quad (1)$$

$P(x,y)$ représente un pixel de l'image en niveau de gris avec les coordonnées x et y , et $P_k(x,y)$ un pixel binaire de la coupe K .

La figure 2 montre un exemple d'extraction de coupes d'une image en niveau de gris. Dans (2a) nous avons la représentation par pixels avec le niveau de gris de chaque point. Dans (2b) nous avons la représentation en relief topographique. Les figures (2c et 2d) représentent deux coupes de l'image (a).

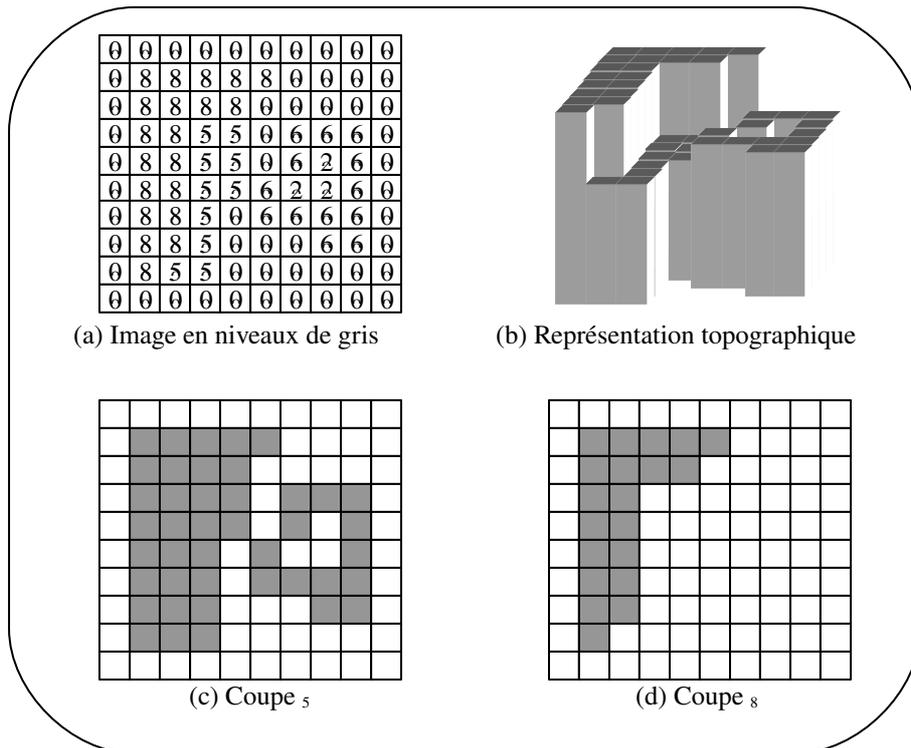


Figure 2. Exemple de coupes

4. Insertion de la marque

4.1. Extraction des composants connexes et génération de la clef

Une fois la coupe choisie, on procède à l'application d'opérateurs topologiques pour l'extraction des composants connexes [11] [12]. La taille de ces dernières ainsi que leur nombre déterminent la quantité d'information que l'on peut insérer. Pour l'automatisation du choix des composants connexes à marquer, un module de calcul statistique est développé. Ce dernier permet de classer les composants connexes de la coupe en fonction du nombre de points utilisés et de leur centre (figure 3). Il en résulte un calque que l'on applique directement sur l'image originale pour insérer la marque à l'aide d'une clef secrète K.

La génération de la clef K dépend des éléments suivants :

- ✓ étiquette du composant connexe utilisé,
- ✓ la taille de la marque,
- ✓ le domaine d'insertion choisi,
- ✓ le numéro de la coupe marquée,
- ✓ les paramètres statistiques des blocs de points à marquer.

Une fois la clef générée, on insère la marque ou le message M aux points designés par le calque qu'on a extrait précédamment. A la fin on obtient une image tatouée d'une façon topologique.

Afin d'améliorer la robustesse du marquage contre les déformations géométriques (rotation, fenêtrage...), les points d'insertion sont triés en fonction de leur distance du centre du composant connexe (figure 3). Ces valeurs restent inchangées s'il y a attaque de nature géométrique. Un code d'entête est rajouté au message à insérer pour indiquer le sens de la lecture lors de l'extraction de la marque.

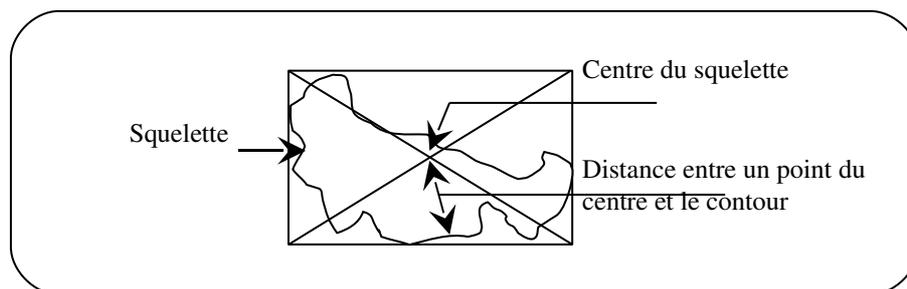


Figure 3. Paramètres d'un composant connexe

4.2. Algorithme de tatouage

Le tatouage consiste à former à l'aide de la liste triée des points d'insertion, des couples de blocs de taille fixe (4x4). L'insertion d'un bit de la marque est faite en modifiant la différence de moyenne entre deux blocs voisins sans les altérer.

La différence des moyennes M_{diff} entre deux blocs A et B doit être égale à l'une des deux valeurs spécifiques d_0 ou d_1 . La première indique qu'un 0 est inséré et la deuxième indique l'insertion d'un 1.

d_0 est un nombre pseudo-aléatoire généré par la clef secrète K , Alors que d_1 est la somme de d_0 et $R/2$, où R est le degré de résistance contre les attaques Haute Fréquence (figure 4).

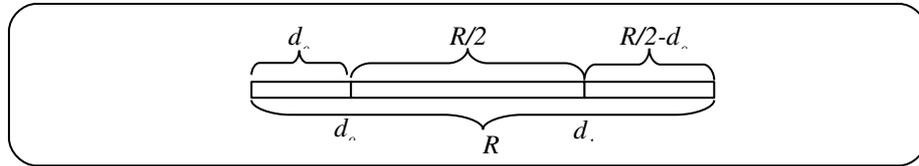


Figure 4. Relations entre d_0 , d_1 et R ,

Soit M_A la moyenne du bloc A , et M_B celle du bloc B , alors :

$$M_{diff} = (M_A - M_B + R \times 256) \bmod R \quad (2)$$

Le terme $R \times 256$ garantit une valeur de M_{diff} toujours positive. Pour que la différence entre les blocs soit conforme aux règles de marquage, une valeur notée δ est ajoutée à chaque pixel du bloc A , et soustraite de chaque pixel du bloc B . Si la valeur de δ n'est pas un entier, une procédure de diffusion d'erreur est déclenchée après l'addition/soustraction de δ aux deux blocs [4].

Les règles de calcul de δ sont comme suit :

Dans le cas d'insertion d'un 1, la règle utilisée est la suivante :

$$\begin{aligned} & \text{Si } (M_{diff} < d_0) \text{ alors} \\ & M_{diff} = M_{diff} + R \\ & \text{et } \delta = (d_1 - M_{diff})/2 \end{aligned} \quad (3)$$

Dans le cas d'insertion d'un 0, la règle utilisée est la suivante :

$$\begin{aligned} & \text{Si } (M_{diff} > d_1) \text{ Alors} \\ & M_{diff} = M_{diff} - R \\ & \text{et } \delta = (d_0 - M_{diff})/2 \end{aligned} \quad (4)$$

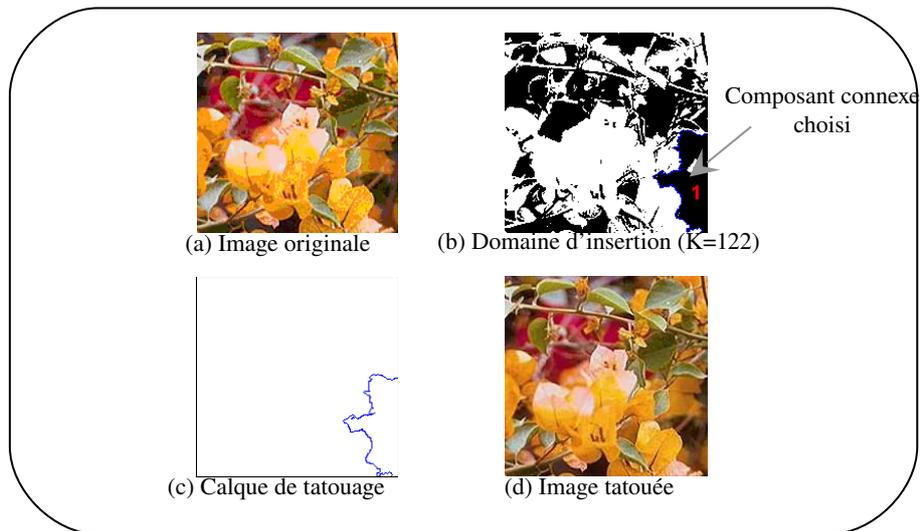
Après l'insertion d'une signature, le composant concerné est étiqueté pour mentionner son marquage et éviter ainsi de le marquer une seconde fois.

4.3. Choix de l'espace d'insertion

L'espace d'insertion utilisé repose sur les composantes de luminance et/ou de chrominance de l'image couleur à tatouer. Nous rappelons que si l'utilisation des composantes de chrominance pour le tatouage reste intéressante pour des facteurs de qualité relativement élevés, la robustesse de ce type d'insertion face à la compression JPEG devient de plus en plus faible lorsque le facteur de qualité diminue et il est alors plus intéressant de tatouer la composante de luminance. Ce phénomène s'explique par le fait que la compression JPEG quantifie les composantes de chrominance d'une façon plus grossière que les composantes de luminance. Nous retiendrons cependant que pour un taux de compression faible, l'insertion sur une composante de chrominance offre une imperceptibilité plus importante par rapport à la luminance [13][14]. Pour une première approche nous avons travaillé seulement avec la composante luminance.

4.4. Exemple de tatouage

L'exemple suivant illustre notre démarche : En premier l'image de la figure 5.a est convertie en niveaux de gris (256 NG). On extrait la ou les coupes qui nous permettront d'insérer la marque dans l'image originale. Le choix de la coupe se fait manuellement ou automatiquement. Dans le premier cas l'utilisateur fixe la ou les coupes à marquer, dans le deuxième cas un procédé de recherche automatique est déclenché pour désigner la ou les coupes qui répondent aux besoins du tatouage (quantité d'information à insérer). Dans cet exemple le marquage a nécessité l'utilisation de la coupe K (avec $K = 122$) choisie automatiquement en fonction de la taille de la marque à insérer et qui est de 64 bits.



L'incrustation de la marque dans l'image d'origine introduit une dégradation que l'on peut évaluer avec le rapport signal/bruit noté PSNR. La figure 6 présente pour ($R = 9$) les PSNR obtenus après tatouage des différentes images de test. Le plan d'insertion est choisi en fonction des propriétés topologiques de l'image et la taille de la marque qui dans cet exemple est de 256 bits.

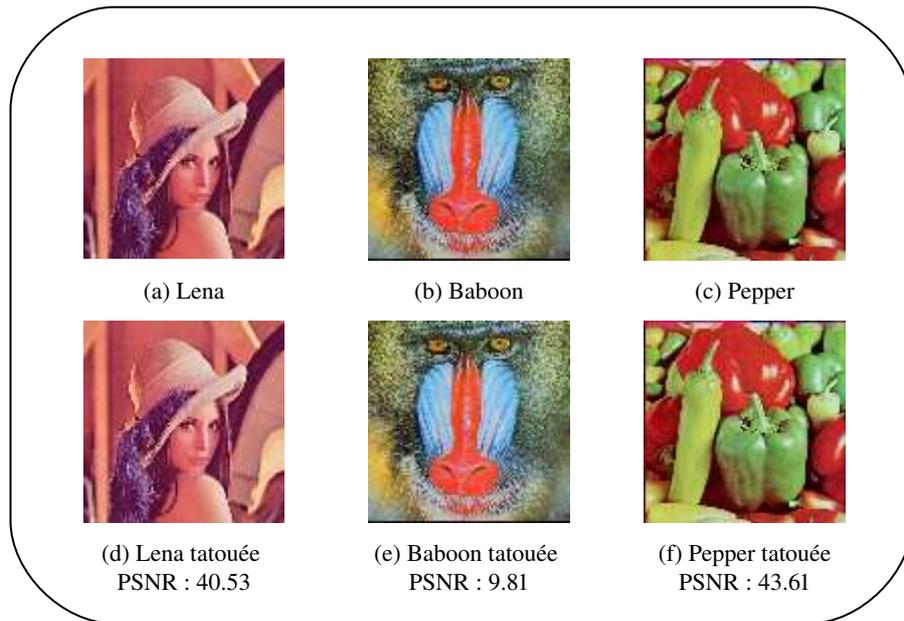


Figure 6. Images tatoués ($R=9$)

Le choix de la valeur de R a un impact sur la robustesse du tatouage et la qualité de l'image tatouée. Plus cette valeur est importante, plus le tatouage est robuste et plus les dégradations sur l'image tatouée sont perceptibles (figure 7).

Valeur de R	Lena	Baboon	Pepper
7	46.35	45.17	47.27
8	44.70	42.30	45.33
9	40.53	39.81	42.61
10	39.70	38.20	40.57
11	37.83	36.11	48.66

Figure 7. Impact de R sur la qualité des images tatouées

5. Extraction de la marque

La figure 8 montre le processus d'extraction de la marque. Si la clef est juste, elle contient toutes les informations relatives à l'environnement d'insertion. Après l'extraction de la coupe marquée, des traitements topologiques sont effectués pour définir le domaine d'insertion de la marque et reformer les blocs utilisés pour l'insertion de la marque. Connaissant les paramètres statistiques (d_0 , R), la marque peut être alors régénérée.

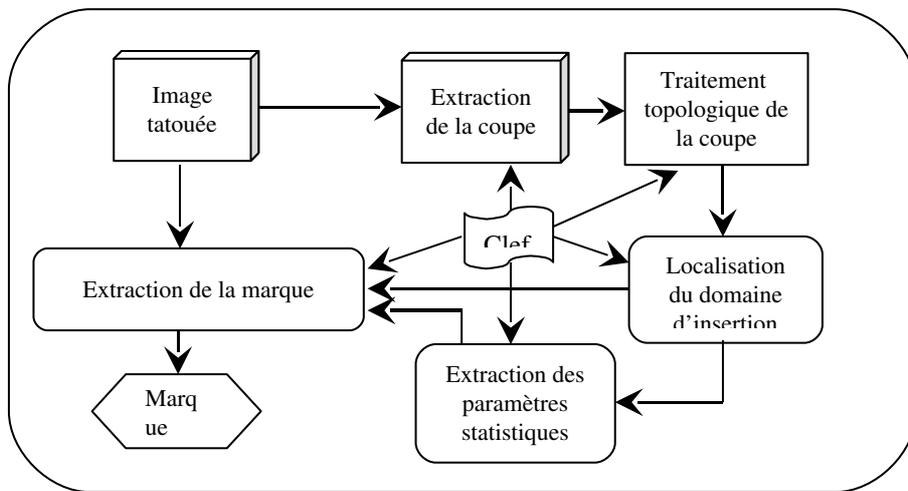


Figure 8. Extraction de la marque

Pour l'extraction du bit embarqué, nous calculons la différence des moyennes entre deux blocs voisins reconstruits. Si cette différence est proche de d_0 alors la valeur « 0 » est extraite, sinon un « 1 » est extrait.

Les règles suivantes sont utilisées pour l'extraction du bit embarqué:

$$\begin{aligned} \text{Si } |M_{diff} - d_t| < R/4 \text{ alors un « 1 » est extrait} \\ \text{sinon « 0 » est extrait} \end{aligned} \quad (5)$$

Pour tester la robustesse du tatouage face aux différents types d'attaques, on compare la marque extraite après attaque à la marque originale et un pourcentage d'erreur est calculé. Pour cela un module spécial contenant une variété d'attaques (compression, filtrage et transformations géométriques) est développé.

6. Structure de l'application

Notre application (développée avec Builder C++) est un atelier de marquage topologique composé de quatre modules principaux (figure 9) qui communiquent entre eux :

- ◆ Un module de prétraitement destiné aux opérations élémentaires sur l'image : ouverture, sauvegarde et passage en niveaux de gris.
- ◆ Un module topologique destiné aux différents traitements topologiques : extraction des coupes et des composants connexes, extraction des points simples et non simples.
- ◆ Un module de tatouage topologique qui permet d'effectuer les calculs statistiques relatifs aux blocs porteurs de la marque. Ce module offre également la possibilité de changer les paramètres du tatouage.
- ◆ Un module de test qui permet d'appliquer différents types d'attaques sur l'image tatouée et de tester ainsi la robustesse du marquage. Il est aussi possible de consulter un recueil d'informations et de statistiques afin de valoriser le travail réalisé.

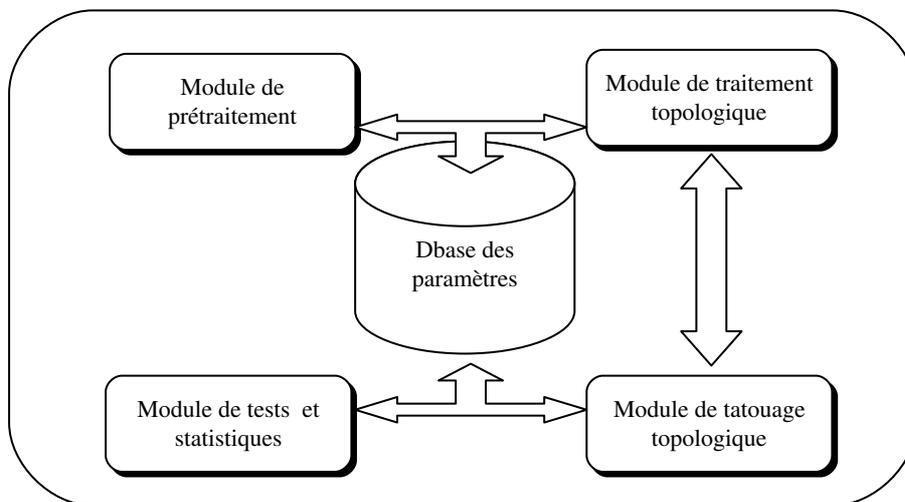


Figure 9. Structure de l'application

7. Tests de robustesse

Dans cette partie nous présentons les tests effectués pour étudier la robustesse du tatouage face aux différentes attaques de type traitement du signal : compression, filtrage ajout de bruit ainsi que les transformations géométriques. Les tests sont effectués sur l'image lena pour laquelle nous avons porté une marque d'une taille de 256 bits.

7.1. Robustesse face à la compression

Nous nous intéressons ici plus particulièrement à la compression JPEG. La figure 10.b montre pour différentes valeurs de R la robustesse de la méthode face à cette attaque. Nous avons réussi à décoder le message en considérant des attaques JPEG de l'ordre de 50%. Les figures 10.c, 10.d et 10.e présentent les résultats obtenus avec l'image lena pour différents taux de compression et avec une valeur de R fixée à 9.

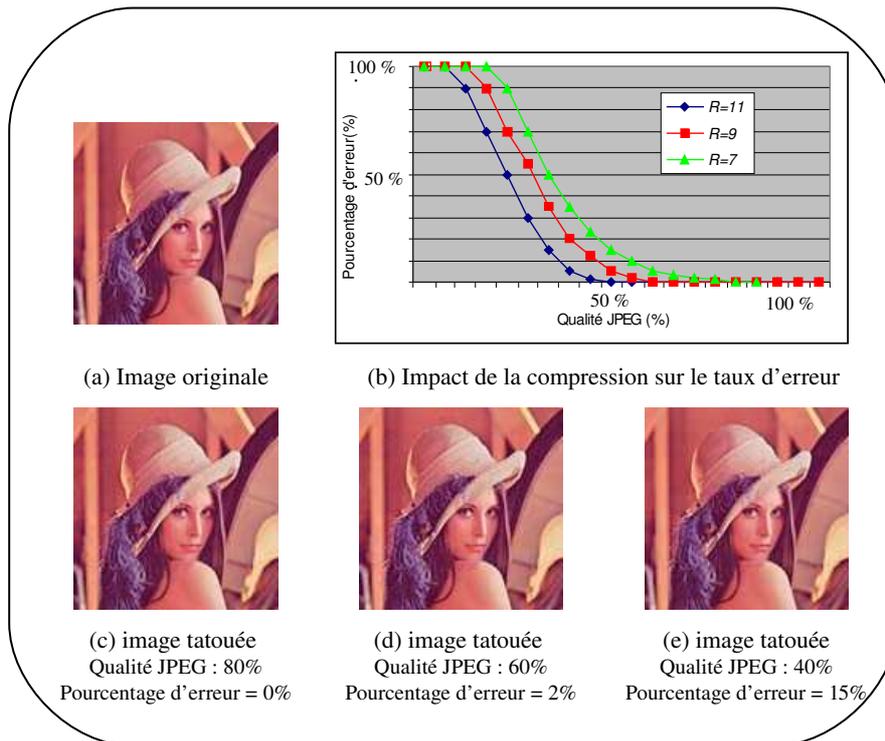


Figure 10. Tests de robustesse face à la compression JPEG

7.2. Robustesse face à un filtrage passe bas répétitif

Un filtrage passe bas (figure 11.a) est appliqué sur l'image tatouée de façon répétitive. Après chaque passage du filtre, on teste la robustesse du marquage face à cette attaque. Comme on peut le constater dans la figure 11.b, le filtrage répétitif affecte considérablement la marque après la deuxième itération. Ceci est dû au fait d'avoir choisi de travailler seulement avec la composante luminance. De nettes améliorations peuvent être apportées si on inclut les composantes de chrominance dans le processus de tatouage [14].

7.3. Robustesse face à l'ajout d'un bruit

Pour cette attaque, un bruit blanc gaussien avec une moyenne nulle et une déviation variable σ est ajouté à l'image tatouée. La figure 11.c présente pour différentes valeurs de σ le taux d'erreur sur la marque extraite. Nous avons réussi à décoder le message pour des valeurs de σ allant jusqu'à 60 (figure 11.d), au delà, la marque est perdue.

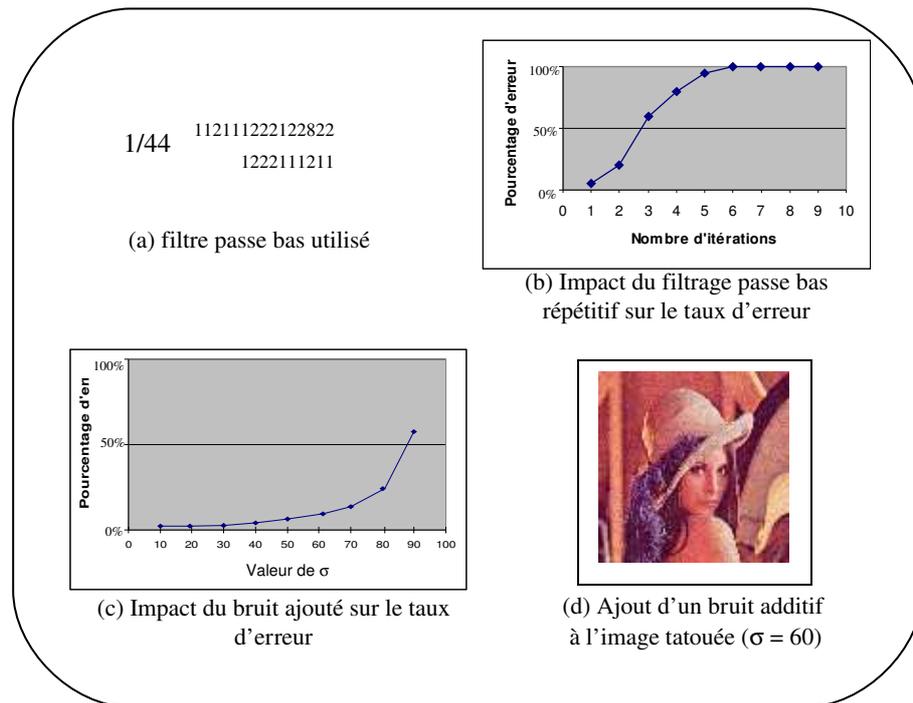


Figure 11. Tests de robustesse face au filtrage et à l'ajout d'un bruit additif

7.4. Robustesse face aux transformations géométriques

Nous avons testé notre schéma face aux transformations géométriques classiques comme la rotation, effets miroir et fenêtrage. Dans chacun de ces cas la détection de la marque a pu être réalisée.

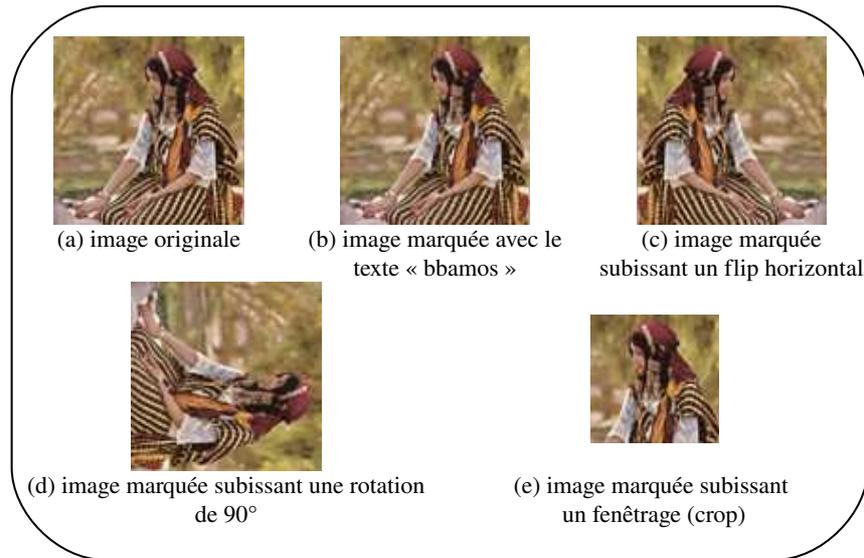


Figure 12. Attaques de type géométrique

Dans le cas du fenêtrage la marque doit impérativement se trouver dans la zone sélectionnée. Pour cela il est préférable de marquer manuellement les principales zones de l'image. Il est aussi possible de dupliquer la marque sur plusieurs zones en utilisant une ou plusieurs marques avec une ou plusieurs coupes.

8. Coûts en temps de calcul

Bien qu'elle soit robuste contre les attaques géométriques, l'approche proposée rajoute (comparé aux méthodes spatiales classiques) une couche de calcul supplémentaire pour l'extraction des calques topologiques. En effet, cette étape consiste à rechercher la ou les coupes adéquates, extraire les composants connexes, et constituer les blocs porteurs de la marque. Une bonne exploitation de la récursivité dans les calcul nous a permis de réduire considérablement les temps de calculs. Le tableau de la figure suivante présente les temps nécessaire pour l'insertion et l'extraction d'une marque à taille variable sur l'image lena.

Taille de la marque (bits)	Tatouage (s)	Extraction de la marque (s)
64	0.12	0.02
128	0.25	0.07
256	1.07	0.16
512	1.53	0.5

Figure 13. Temps nécessaire pour le tatouage et l'extraction la marque

9. Conclusion

Nous avons présenté dans cet article un schéma de tatouage original basé sur la topologie des coupes. Les points d'insertion de la marque sont localisés par un calque constitué de composants connexes d'une ou plusieurs coupes choisies en fonction des besoins du tatouage (quantité d'informations et robustesse). Ce nouveau procédé permet d'effectuer un tatouage multiple sur plusieurs parties de l'image. La duplication de la marque est aussi possible, rendant ainsi le marquage robuste face aux attaques qui ciblent des parties de l'image.

Pour améliorer la robustesse du marquage face aux attaques de type géométrique, les points d'insertion sont triés en fonction de leur distance par rapport au centre du composant connexe. Cet invariant géométrique est insensible aux attaques de type rotation ou fenêtrage. L'utilisation d'une clé secrète qui contient les informations relatives à la coupe et aux règles de tatouages utilisées complique d'avantage les tentatives d'extraction illicite de la marque.

Cette étude a mis en évidence l'intérêt d'utiliser la topologie numérique pour la construction de systèmes de tatouage spatiaux robustes. IL reste néanmoins deux améliorations principales à apporter à notre schéma de tatouage : la sélection automatique et optimale de l'espace d'insertion, avec la possibilité de tatouer le flux vidéo, et plus particulièrement les objets vidéo. Ces améliorations font l'objet de nos travaux actuels.

10. Références

- [1] J. Cox, M. L. Miller, J. A. Bloom, «Digital watermarking», Morgan Kofmann publisher, 2002.
- [2] C. I. Podilchuck, E. J. Delp, «Digital Watermarking Algorithms and Applications», IEEE Signal Processing magazine, pp. 33-46, july 2001.
- [3] N. Johnson, Z. Duric, S. Jajodia, «Information Hiding: Steganography and Watermarking: Attacks and contremeasures », Kluwer Academic Publisher, 2000.
- [4] J. C. Liu, S. Y. Chen, « Fast two layer image watermarking without referring to the original image and watermark », Image and Vision Computing, 19, pp. 1083-1097, 2001.
- [5] Q. Cheng, T. S. Huang, « Blind Digital Watermarking for images and videos and performance analysis », IEEE International Conference on Multimedia and Expo, volume 1, pp. 389-392, 2000.
- [6] C. T. Hsu, J. L. Wu, « Hidden digital watermarks in images », IEEE Transaction on Image Processing, 8(1), pp. 58-68, 1999.
- [7] M. Barni, F. Bartolini, V. Cappellini, A. Piva, « A DCT domain system for robust image watermarking », Signal processing, 66(3), pp. 357-372, 1998.
- [8] I. J. Cox, J. Kilian, F. T. Leighton, T. Shamoan, « Secure spread spectrum watermarking for multimedia », IEEE Transaction on Images Processing, 6(12), pp. 1673-1687, 1997.
- [9] S. P. Mohanty, K. R. Ramakrishnan, M. S. Kankanhalli, « A DCT domain visible watermarking for images », IEEE International Conference on Multimedia and Expo, volume 2, pp. 1029-1032, 2000.
- [10] T. Y. Kong, A. Rosenfeld, « Digital Topology : introduction and survey », Computer Vision, Graphics and image processing, N° 48, pp. 357-393, 1989.
- [11] G. Bertrand, J. C. Evrat, M. Couprie, « Image segmentation through operators based upon topology », Journal of Electronic Imaging, 6(4), pp. 1067-1076, 1997.
- [12] F. N. Bezerra, « Opérateurs topologiques pour le traitement d'images en niveaux de gris », Thèse de Doctorat, Université Marne la Vallée, France, novembre 2001.
- [13] M. Couprie, G. Bertrand, « Topological grayscale watershed transformation », SPIE Vision Geometry Proceedings, Vol. 3168, pp. 136-149, 1997.
- [14] E. Sayrol, J. Vidal, S. Cabanillas, S. Santamaria, « Optimum watermark detection for color images », IEEE International Conference on image processing, volume 2, pp. 231-235, 1999.
- [15] M. Kutter, F. Jordan, F. Bossen, « Digital watermarking for color images using amplitude modulation », Journal of Electronic Imaging, 7 (2), pages 326 – 332, 1998.
- [16] J. O. Limb, C. B. Rubinstein, J. E. Thompson, « Digital coding of color video signals – a review», IEEE transaction on communications, 25, pp. 1349-1384, 1997.