2014

Le Watermarking

Sécurité Informatique

LE TATOUAGE Numérique ou "Digital Watermark"

AZZOUNI NAZIH & GARIDI IMENE
1CS, Section B, groupe 07
04/05/2014

Table des matières

➢ Introduction

1.1. L'ère de technique digitale et le problème du copyright :

Avec le développement continu de l'Internet, de produits digitaux comme des produits de stockage, des produits de communication, l'ère de technique digitale a se formé. La plupart d'information actuelle est stockée sous la forme digitale avant d'être un produit comme livre ou magasine.

L'échange, distribution et traitement de ces produits sont de plus en plus facile et à l'extérieur de contrôle de gouvernement. Ainsi, l'état de l'utilisation sans permis a lieu dans beaucoup de pays. En 3/1998 à Hong Kong, le gouvernement a confisqué des CDs contrebandières qui ont coûté 85 millions de dollars et en 6/1998, en Allemande, on a confisqué des logiciels contrebandiers coûtant 1.9 millions de dollars.

Cette situation se passe au Viet Nam aussi. De nos jours, quand le gouvernement vietnamien a signé un contrat de protection de copyright avec celui d'états unis, le problème de copyright devient le plus important.

Tous ces faits s'expriment une nécessité d'expédient pour prévention l'utilisation sans permis des produits digitaux.

Une méthode qui permet de déterminer de l'auteur de produits digitaux a été née.

1.2. Watermarking – une méthode aidant la résolution de problème du copyright :

C'est une méthode basant plusieurs domaines différents comme cryptographie, communication, traitement des signaux… Le contenu de celle est constitué par l'insertion une quantité de l'information et cette information est appelée « tatouage » en français ou « Watermarking » en anglais. Cette méthode a construit un nouveau secteur de recherche et actuellement, beaucoup d'articles dans ce domaine ont apparu et nous recevons beaucoup de résultats actifs.

Tatouage est utilisé afin de déterminer une utilisation sans permis d'un produit digital. Tatouage peux s'appliquer au copyright, à la prévention de copier et à distinguer la falsification.

➢ Définition

Le tatouage numérique (en anglais digital Watermark, « filigrane numérique ») est une technique permettant d'ajouter des informations de copyright ou d'autres messages de vérification à un fichier ou signal audio, vidéo, une image ou un autre document numérique. Le message inclus dans le signal hôte, généralement appelé marque ou bien simplement message, est un ensemble de bits, dont le contenu dépend de l'application. La marque peut être le nom ou un identifiant du créateur, du propriétaire, de l'acheteur ou encore une forme de signature décrivant le signal hôte. Le nom de cette technique provient du marquage des documents papier et des billets.

Watermarking, stéganographie, cryptographie?

1. Qu'est-ce que le tatouage d'images?

Le tatouage d'images est une technique qui est en fait issue directement d'un art appelé la stéganographie. Cet art n'a pour ainsi dire qu'un but précis, qui est de cacher au sein d'un message primaire, un message secondaire.

Bien entendu il faut que le message primaire soit lisible par tout un chacun, et qu'il reste visuellement inchangé par rapport à ce qu'il était avant introduction du message secondaire. Le message secondaire se doit d'être parfaitement invisible, mais uniquement accessible par des personnes propriétaires d'une information secrète, une "clef" par exemple qui permettrait son extraction.

2. Différences avec la cryptographie

En cryptographie, l'objectif n'est pas de dissimuler des informations dans d'autres, mais plus simplement de rendre l'information que l'ont désire transmettre complètement illisible à toute personne ne possédant pas la donnée nécessaire a son décodage. De plus en cryptographie si le message primaire est modifié, il devrait être impossible de le recouvrer, tandis qu'en **stéganographie**[1]**,** le message secondaire est supposé rester accessible et ce même après de multiples recopies et manipulations diverses du message primaire.

[1] La stéganographie est l'art de la dissimulation : son objet est de faire passer inaperçu un message dans un autre message. Elle se distingue de la cryptographie, « art du secret », qui cherche rendre un message inintelligible à autre que qui-de-droit. Pour prendre une métaphore, la stéganographie consisterait à enterrer son argent dans son jardin là où la cryptographie consisterait à l'enfermer dans un coffre-fort — cela dit, rien n'empêche de combiner les deux techniques, de même que l'on peut enterrer un coffre dans son jardin.

3. A quoi ça sert?

Et bien comme tout le monde le sait, de nos jours presque tous les types de médias (images, sons, vidéos, etc.) sont stockés sous forme de données numériques, et leur libre accès pose de nombreux problèmes de droits d'auteur. Cela vient principalement du fait de la banalisation des connexions internet haut débit, et des graveurs de CD/DVD qui représente un manque à gagner et des préjudices importants pour les grandes industries de médias.
Le "Watermarking" est certainement un moyen efficace de résoudre ces problèmes.
C'est la raison pour laquelle beaucoup se tournent vers cette technologie récente et sophistiquée.

➢ Historique

L'apparition de la stéganographie est très ancienne, elle remonte à l'antiquité.

En effet, les premiers exemples connus nous viennent directement des Grecs. Ils rasaient les cheveux d'un esclave, puis tatouaient sur son crâne un message. Une fois les cheveux repoussés, l'esclave pouvait traverser les territoires ennemis sans éveiller les soupçons. Une fois à destination, il suffisait de raser à nouveau le crâne pour récupérer le message. Bien sûr, il ne fallait pas être pressé...

Au cours de l'histoire, les techniques ont évoluées sans cesse, et on a vu au fur et à mesure du temps la naissance de nouveau procédés plus efficaces. Par exemple les encres sympatriques, qui fut la méthode la plus utilisée au cours des siècles. On écrit, au milieu des textes écrits à l'encre, un message à l'aide de jus de citron, de lait ou de certains produits chimiques. Il est invisible à l'œil, mais une simple flamme, ou un bain dans un réactif chimique, révèle le message (figure 1.1).

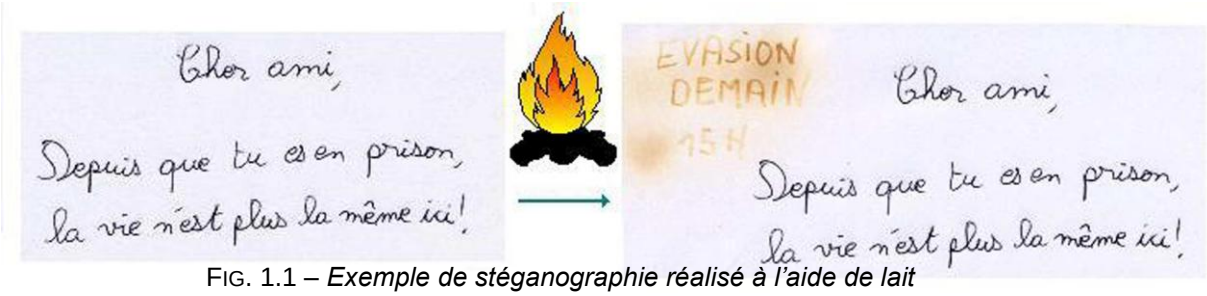


FIG. 1.1 – *Exemple de stéganographie réalisé à l'aide de lait*

Il a donc fallu attendre jusqu'en 1992 pour voir les premières apparitions commerciales du Watermarking, ou du moins ce fut la première année ou des articles commençaient à paraître sur le sujet. En effet, il semblerait que l'ont eu recours aux tatouages de certains documents bien avant cette date. On raconte qu'en 1986, Margaret Thatcher, ne supportant plus que certains de ses ministres vendent des informations à la presse, exigea que tous les traitements de textes de son cabinet soient programmés afin que l'identité des utilisateurs soit encodée dans les espaces de leurs textes. Si une fuite advenait, on pouvait alors identifier le coupable.

➢ Notion de Base

1. Différentes définitions

Notion de pixel, valeur : un pixel, (*picture element*) est l élément indivisible permettant de coder l information relative a la luminosité en une certaine position pour les images en teinte de gris. Sa valeur correspond alors à un nombre binaire codé généralement sur 8 bits, de 0 à 255 (du plus foncé au plus clair). Pour les images colorées, le cas le plus courant est un codage de 8 bits pour chaque intensité lumineuse R G B (rouge, vert, bleu) ce qui correspond à un codage sûr 24 bits. La valeur de chaque pixel correspond, par conséquent, à un nombre entier, souvent représenté en hexadécimal pour les images colorer (de 000000 a FFFFFF).

Une représentation isomorphe est la représentation (Y, U, V) où Y désigne la luminance du pixel et U et V définissent sa chrominance. Plus la luminance est forte, plus le pixel est clair.

Domaine spatial : Le domaine spatial est le domaine classique où chaque valeur en (x,y) correspond à la valeur des pixels ; nous pouvons alors la visualiser dans un espace a 3 dimensions ou les axes X et Y représentent les deux dimensions de l'image, et l'axe Z représente la valeur des pixels (figure 1.2).

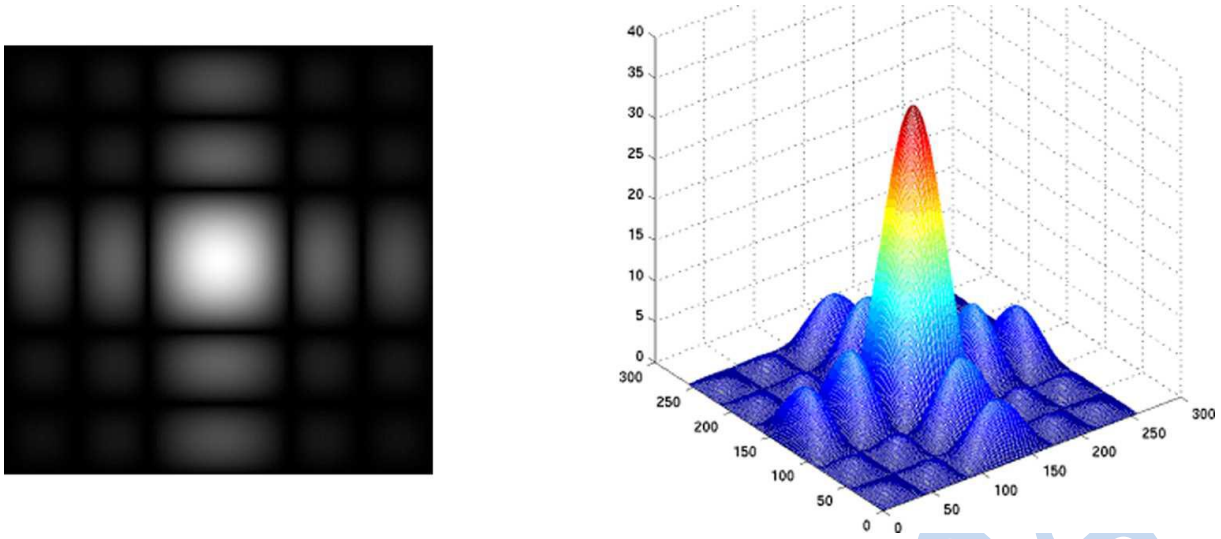


FIG. 1.2 – *Exemple de représentation tridimensionnelle dans le domaine spatial*

Domaine fréquentiel : Le domaine fréquentiel est un espace dans lequel l'image sera considérée comme une somme de fréquences de différentes amplitudes

Filtre de Convolution : Sans entrer dans les détails, une convolution sur des blocs de 3*3 permet de modifier le pixel courant par différentes opérations sur les valeurs des pixels du voisinage (par exemple une matrice rempli de 1 changera le pixel courant par la moyenne des 8 autre pixels du bloc 3*3).

Ces filtres de convolution s'appliquent dans le domaine spatial. En fréquentiel, cela se résume a multiplier 2 fonctions.

2. Transformée de Fourrier

Elle permet simplement de passer du domaine spatial au domaine fréquentiel. Cette transformée rend donc visible les composante en fréquence

$$F(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} f(t) * e^{-1\omega * t}.dt \qquad (1.1)$$

Il est intéressant de noter que nous pouvons revenir au domaine spatial via la transformée de fourrier inverse. Une application brute de cette formule étant extrêmement longue, Une autre

façon d'effectuer ce calcul permet de limiter considérablement la durée de cette transformation. C'est ce que l'on appelle la FFT (Fast Fourier Transform).

3. Transformée et domaine DCT

La DCT (Discret Cosinus Transform) est une transformée fort semblable à

la FFT, travaillant sur un signal discret. Elle prend un ensemble de points d'un domaine spatial et les transforme en une représentation équivalente dans le domaine fréquentiel. La DCT transforme un signal d'amplitude (chaque valeur du signal représente l' "amplitude d'un phénomène discret bidimensionnel en une information bidimensionnelle de "fréquences". La formule de la DCT est détaillée ci-dessous.

$$F(u,v) = \frac{2}{N} c(u).c(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} Img(x,y). \cos\left[\frac{\pi}{N} u(x+\frac{1}{2})\right]. \cos\left[\frac{\pi}{N} v(y+\frac{1}{2})\right] \quad (1.2)$$

Voici son inverse (connue aussi sous le nom de IDCT).

$$Img(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} c(u).c(v).F(u,v). \cos\left[\frac{\pi}{N} u(x+\frac{1}{2})\right]. \cos\left[\frac{\pi}{N} v(y+\frac{1}{2})\right] \quad (1.3)$$

$$\text{ou} \begin{cases} c(0) = (2)^{-\frac{1}{2}} \\ c(w) = 1 \qquad \text{pour } w = 1, 2, \ldots, N-1 \end{cases} \quad (1.4)$$

Cette transformation étant très lourde, elle s'applique généralement en bloc de 8x8 (compression Jpeg). Concrètement, et en terme simple, cette transformation va essaye de faire correspondre des blocs de 8x8 de l'image en une somme de fonction basique qui sont donnée dans la matrice 8x8 de la DCT (DCT matrix).

Un exemple est donné dans la figure 1.3. Les valeurs de la matrice de la transformée corresponde par conséquent à l'intensité lumineuse pour chaque fonction de la matrice.

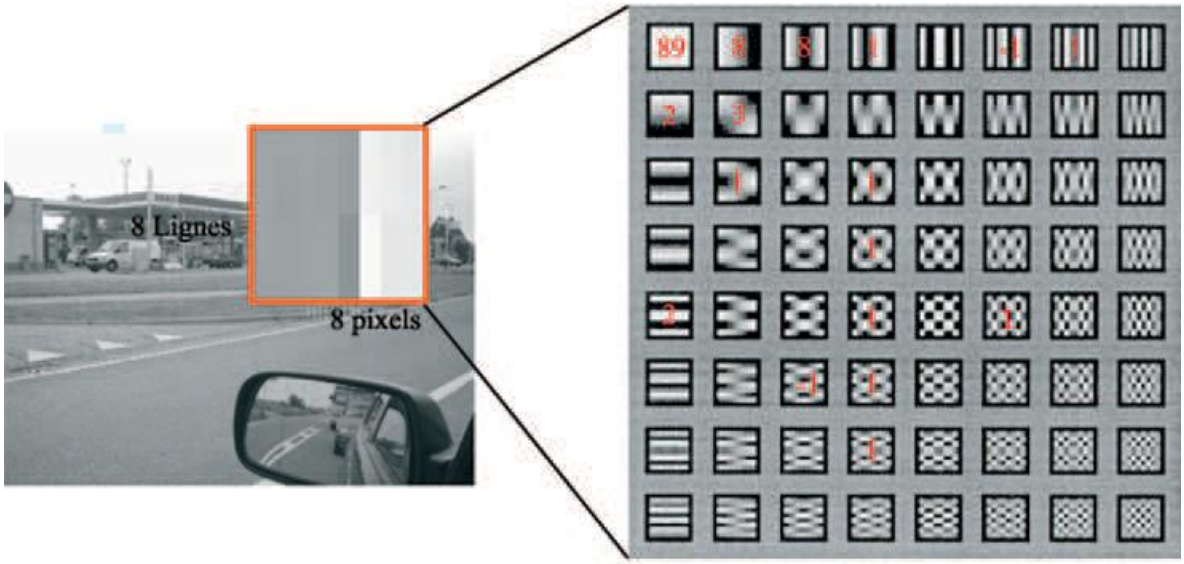


FIG. 1.3 – *Exemple concret de transformation en domaine DCT*

Différence entre le FFT et le DCT le DCT est actuellement une version simplifiée de la FFT :

– Seule la partie réelle de la FFT est conservée

– Beaucoup plus simple en termes de coup de programmation

– la DCT est efficace dans la compression de multimedia (Jpeg)

– DCT Beaucoup plus utilisée.

4. Un peu de terminologie

Pour nommer le tatouage d'images dans le monde, on utilise généralement le mot anglais "Watermarking", ou plus exactement «digital watermarking ». Ce terme anglo-saxon, signifiant "filigramme" à la base, correspond dorénavant au fait même de masquer des données sur un autre support. Cela regroupe par conséquent des notions plus précises et

restrictives de marques, invisibles et robustes, appliquées au service de protection des droits d'auteurs. Ce qui nous amène donc à employer une expression associant davantage cette idée d'enfouissement de données, le "data embedding".

➢ Etude générale du Watermarking

Il existe plusieurs formes de l'information : une séquence de binaire aléatoire, une petite image…

Image avec tatouage numérique visible. Le texte "2006" apparaît au centre de l'image.

1. Approche

Selon la visibilité de la marque, on peut classifier « tatouage » en deux types : tatouage imperceptible et tatouage perceptible.

1.1. Tatouage imperceptible

Dans ce type, on n'observe pas l'existence de la marque. En conséquence, elle n'affecte pas la qualité de l'image et l'image elle-même a encore la qualité commerciale.

1.2. Tatouage perceptible

Par contre, dans ce type de tatouage, on peut observer bien la marque dans l'image. Bien sûr que c'est clairement de permet d'une authenticité de la propriété de l'image. Il est utilisé plus dans l'application non commerciale.

2. Applications de tatouage sur l'image

2.1. Protection de copyright

Afin d'utiliser le tatouage pour protéger le copyright, l'auteur de produit va insère une marque à l'image pour que les autorisations puissent baser sur le résultat de détection cette marque pour déterminer qui a le droit de possession.

Il est possible d'insérer une autre marque en vue de distinguer des utilisateurs de produit.

Un exemple de l'application commerciale est Digimarc, http://www.digimarc.com/, qui est réalisée par Digimarc Corporation ImageBridge Solution.

2.2. Protection de copie

Cette application de tatouage permet d'interdire la copie illégale. Par l'insertion une marque au contenu digital, on peut contrôler la copie de disc. Cependant, il est clairement que l'équipement de copie doit s'installer le détecteur de marque.

2.3. Authenticité

Le tatouage peux s'appliquer afin d'authenticité de l'image et détecter la falsification. De nos jours, des images sont de plus en plus des preuves devant la loi, et un problème

nécessitant une réponse est la légalité de ces images. Tatouage est pris en charge de déterminer qu'est ce qu'il y a des modifications sur l'image et où sont ces régions.


2.3. **Cache de données et marquage d'image**

Pour transférer en secret des informations, on peut les cacher sous une image. C'est une autre application de tatouage. Quand on transfère une image, des attaquantes n'observent pas l'existence de données, ils peuvent observer seulement cette image.

Cette application a utilisé à Viet Nam afin de transférer des sujets d'un exercice du ministère d'éducation à des bureaux d'éducation en province.

3. Exigences sur le tatouage

Il y a des exigences différentes pour chaque application de tatouage.

3.1. Invisibilité

D'abord, une marque tatouée doit être invisible pour n'abaisser pas la valeur commerciale de l'image. L'utilisateur ne sent pas l'existence de marque dans l'image. En utilisant l'impact de masques psy-chovisuels, une marque avec la taille grande peut être insérée sans dégrader la qualité de l'image.

3.2. Robustesse

La deuxième exigence concerne la robustesse de la marque en face des attaques… Selon le différent type d'application de tatouage, la robustesse est variable aussi.

Les attaques innocentes s'inclurent la compression, la transformation AD et D-A, l'échantillon, filtrage. Par contre, l'attaque intentionnelle apparaît dans le cas les attaquants veulent nettoyer, détruire ou falsifier la marque.

3.3. Capacité de transférer des informations

Afin d'être robuste contre des attaques, il faut le nombre de bits inséré être suffisant pour opposer des attaques.

3.4. Liens entre trois exigences

Cependant, il paraît difficile à satisfaire tous les trois liens. Pour implémenter le tatouage, on doit modifier le contenu d'image. Afin d'augmenter la robustesse du tatouage, un procédé utilisé souvent est l'augmentation de nombre d'informations cachées. Cependant, elle pût conduire à la visibilité de tatouage, contrairement à l'invisibilité. Par contre, si on modifie une partie insignifiante du contenu d'image, le tatouage soit effacé facilement par les attaques. En conséquence, il y a un changement entre la robustesse et l'invisibilité de la marque.

➢ Attaques

On distingue deux types d'attaques, celles passives et celles actives. Les premières visent simplement à déceler la présence d'un tatouage invisible caché dans l'image. Les secondes attaques cherchent à éliminer cette marque.

Ces deux attaques ont des buts différents. L'attaque passive s'applique davantage à la stéganographie, on cherche à déterminer si une image contient un message ou pas.

L'attaque active est, en général, malveillante et vise à supprimer d'un média le tatouage (copyright, fingerprint) afin de pouvoir l'utiliser sans autorisation préalable de l'auteur par exemple.

Technique

Il existe différentes méthodes d'insertion de la marque, on distingue généralement celles travaillant dans le domaine spatial, et celles travaillant dans le domaine spectral. Les techniques purement spatiales résistent mal à certaines attaques comme le zoom et le recadrage, tandis que la plupart des techniques opérant dans le domaine des fréquences et le domaine mixte résistent bien à ce type d'attaques.

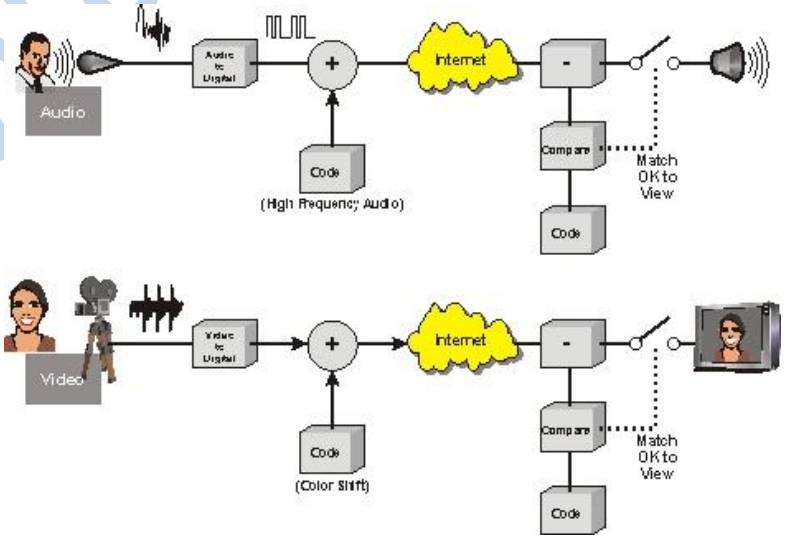
L'insertion d'un tatouage numérique peut être considérée comme un exercice de communication numérique. Les bits du message sont encodés et transmis sur un signal porteur approprié. Les caractéristiques souhaitées du tatouage numérique, comme l'indétectabilité, la résistance au bruit et à l'édition d'images tel le recadrage et la rotation déterminent le choix du signal porteur. Dans le cas des tatouages robustes, il s'agit d'un signal de faible amplitude (indétectabilité) et de large bande passante (les images étant généralement de taille assez importante). La taille du message, relativement courte, impose l'utilisation de techniques d'étalement de spectre pour l'encodage des bits du message. Les techniques de tatouage basées sur l'étalement de spectre sont parmi les plus robustes aux attaques communes.

Les techniques de compression d'images, comme JPEG, inspirèrent l'utilisation du domaine fréquentiel pour insérer des tatouages numériques indétectables dans les images. La première technique opérant dans ce domaine fut conçue par Scott Burgett, Eckhard Koch et Jian Zhao en 19957 et utilisait le domaine DCT. D'autres transformées sont aussi utilisés, comme la transformée en ondelettes, ou la transformée de Fourie

Applications

Un tatouage numérique peut être en général considéré comme une forme de stéganographie. Le terme tatouage numérique est utilisé pour décrire ce qui peut permettre de différencier des copies d'un même fichier ou signal d'origine, le tout d'une manière imperceptible. Le principe des tatouages invisibles est que toute tentative de les effacer aboutisse à une dégradation de la qualité du contenu du fichier.

Comme dans le cas de la recherche d'aiguilles dans une botte de foin, on peut utiliser un aimant très puissant pour retrouver les aiguilles ou on peut simplement brûler la botte si les aiguilles en valent la peine (le message porté par le tatouage numérique pouvant avoir plus de valeur que le signal marqué).



➢ Conclusion et Perspective

Conclusion

La méthode de tatouage dans le domaine transformé est très utilisée. Par rapport le domaine spatial, des algorithmes utilise ce domaine ont plusieurs caractéristiques qu'on peut exploiter :

- Le modèle psychovisuel humain.

- Exploiter des caractères locaux d'image.

- Exploiter les caractères de haute fréquence et basse fréquence, multirésolution…

- Exploiter aussi des caractéristiques de transformation.

Parmi des transformations, la transformation TWD est reçue l'intérêt par des chercheurs car elle se compose plusieurs bons caractères : multi résolution, calcul efficace, proximité du modèle HVS …

Cependant, les algorithmes existants ne sont pas très robustes contre des attaques étudiées. Pour résoudre ce problème, nous pouvons prendre des idées suivantes :

_ Enregistrement d'image

_ Taux d'information.

_ Fort cryptage

_ Utiliser et combiner des transformations pour rendre la robustesse contre des attaques.

Etat d'art et Perspective

Au Vietnam, des chercheurs ont travaillé dans ce domaine depuis quelques années. Ils concentrent à l'application de cacher de données (envoyer des exercices d'examen), détecter le changement (la carte d'arme), et protection du copyright. Cependant, dans les années récents, il n'y pas beaucoup d'activité de recherche concernant ce domaine

2000	2001	2002	2003	2004	2005	2006
86	94	95	58	37	12	4

Nombre d'article cité par année (citeseer)

Références :

http://en.wikipedia.org/wiki/Spread_spectrum#Spread_spectrum_telecommunications

http://stealthencrypt.com/watermk.html

http://www.watermarkingworld.org

www.petitcolas.net/fabien/watermarking/stirmark/

www.wekipedia.com