

PLAN DU COURS

- ① Introduction
- ② La compression
 - Les méthodes de compression
 - La compression du son
 - La compression des images
 - La compression vidéo
- ③ La stéganographie
 - Le tatouage du son
 - Le tatouage des images
 - Le tatouage de la vidéo
- ④ Conclusion

147

STEGANOGRAPHIE

La stéganographie c'est quoi?

- ❑ Le mot stéganographie vient du grec 'steganos' (caché ou secret) et 'graphy' (écriture ou dessin) et signifie, littéralement, 'écriture cachée'.
- ❑ Technique de dissimulation d'informations à l'intérieur d'une donnée
 - ✓ cacher du texte dans du texte, une image, un son, une vidéo
 - ✓ cacher une image dans une image
 - ✓ cacher une image dans une vidéo (image subliminale)

Gary Gordon, expert à WetStone Technologies déclarait il y a quelques temps : "Nous pensons qu'il est hautement probable que Ben Laden et ses complices ont recours à la technique de la stéganographie, parce que leur utilisation est secrète et facile. Il est connu que des trafiquants de drogue, des pédophiles, des criminels et des terroristes utilisent cela pour communiquer secrètement".

Introduction

148

STEGANOGRAPHIE

A quoi ça sert ?

- ❑ Démontrer l'intégrité d'un document
- ❑ Protéger les droits d'auteur
- ❑ Confidentialité d'échange d'informations (en cachant le message dans un autre anodin)
- ❑ Protéger ses communications privées là où l'utilisation de la cryptographie n'est normalement pas permise ou soulèverait des suspicions.
- ❑ Contrebalancer toutes les législations ou barrières possibles empêchant l'usage de la cryptographie.
- ❑ Publier des informations ouvertement mais à l'insu de tous des informations qui pourront ensuite être révélées et dont l'antériorité sera incontestable et vérifiable par tous.

Introduction

149

STEGANOGRAPHIE

Cher ami,

Je suis toute émue de vous dire que j'ai bien compris l'autre jour que vous aviez toujours une envie folle de me faire danser. Je garde le souvenir de votre baiser et je voudrais bien que ce soit une preuve que je puisse être aimée par vous. Je suis prête à montrer mon affection toute désintéressée et sans calcul, et si vous voulez me voir ainsi vous dévoiler, sans artifice, mon âme toute nue, daignez me faire visite, nous causerons et en amis franchement je vous prouverai que je suis la femme sincère, capable de vous offrir l'affection la plus profonde, comme la plus étroite amitié, en un mot : la meilleure épouse dont vous puissiez rêver. Puisque votre âme est libre, pensez que l'abandon ou je vis est bien long, bien dur et souvent bien insupportable. Mon chagrin est trop gros. Accourez bien vite et venez me le faire oublier. A vous je veux me soumettre entièrement.



Georges Sand, dessinée par Alfred de Musset.

Quand je mets à vos pieds un éternel hommage, Voulez-vous qu'un instant je change de visage ? Vous avez capturé les sentiments d'un cœur Que pour vous adorer forma le créateur. Je vous chéris, amour, et ma plume en délire Couché sur le papier ce que je n'ose dire. Avec soin de mes vers lisez les premiers mots, Vous saurez quel remède apporter à mes maux.

Un exemple historique :

Échange de lettres coquines entre Georges Sand et Alfred de Musset

Votre poupée

Introduction

150

STEGANOGRAPHIE

Dans ses Histoires, Hérodote (486-425 av. J.C.) raconte comment vers 440 av. on rase la tête d'un esclave, puis on y tatoue un message qui devint invisible quand les cheveux ont repoussé.

Une adaptation moderne est toujours utilisée pour sécuriser les documents électroniques et se contente d'imprimer des points minuscules (très facile grâce aux imprimantes laser modernes) pour coder un numéro d'identification d'imprimante, un nom d'utilisateur, etc..

Les photocopieurs émettent un fort rayonnement ultra-violet. Pour éviter la reproduction d'un billet par un photocopieur, certains motifs sont dessinés à l'aide d'une encre qui devient visible lors de l'exposition aux ultra-violets.

On raconte que dans les années 1980, Margaret Thatcher était ennuyée car des documents du gouvernement apparaissaient dans la presse. Afin d'identifier la source de la fuite, elle fit modifier les traitements de texte de ses ministres afin que l'espacement des mots soit caractéristique de chacun d'eux. Cette manipulation lui permit de déterminer l'origine de la fuite.

Introduction

151

STEGANOGRAPHIE

Le texte : méthodes des espaces
rajouter des espaces suivant une convention établie

exemple de convention :

- un espace entre 2 mots suivi de deux espaces entre les 2 mots suivants => 0
- deux espaces entre 2 mots suivi d'un espace entre les 2 mots suivants => 1

Ceci est un essai de texte caché dans un texte hôte.

__ : 0

__ : 1

__ : 1

__ : 0

__ : 1

=> 01101 : message caché

facile à réaliser mais assez visible

Introduction

152

STEGANOGRAPHIE

Méthode de la position géométrique

définir des positions dans la page des mots du message

ex : La pêche en ce 9 juin fut fructueuse. L'espadon est la cible préférée de ces passionnés. Il est 7 heures quand le bateau rentre au port avec pas moins de 2 prises de plus de 50kg.

Méthode de l'écartement des lignes

modification très légère de l'écartement des lignes d'un texte

La pêche en ce 9 juin fut fructueuse. L'espadon est la cible préférée de ces passionnés. } Écartement différent

Différence d'écartement imperceptible à l'œil nu mais pouvant être codée pour transmettre un message caché

Introduction

153

STEGANOGRAPHIE



Tatouage numérique

Tatouage visible



Tatouage invisible

Marque aléatoire

Marque reconnaissable

Marque :

Nombre ID (nombre aléatoire)

Vérification :

Mesure quantitative

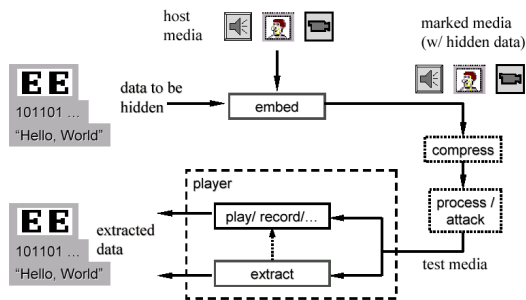
Motif reconnaissable

Motif extrait et mesure quantitative

Introduction

154

STEGANOGRAPHIE



Introduction

155

STEGANOGRAPHIE

Les caractéristiques d'un bon marquage :

- **imperceptibilité** : impossibilité pour un non-expert de voir ou d'entendre la marque (si le tatouage est en mode invisible)
- **spécificité** : clairement identifiable lors de son extraction
- **robustesse** : la marque doit être identifiable malgré des transformations (numérisation, transmission..)
- **résistance aux attaques** : la marque doit persister malgré les différentes attaques menées par les pirates

Introduction

156

STEGANOGRAPHIE

2 grands types d'attaques possibles :

- extraire l'information cachée (espionnage)
- supprimer l'information dissimulée (copyright)

Leçon du passé

En 1883, Auguste Kerckhoffs a énoncé le premier principe de la cryptographie moderne. Il affirma qu'il fallait supposer connue de l'ennemi la méthode de chiffrement et que, par conséquent, la sécurité du système ne devait résider que dans le choix de la clé utilisée pour le chiffrement.

Il faut qu'un pirate, connaissant la méthode de stéganographie mais pas la clé, ne puisse obtenir aucun indice sur les informations dissimulées.



Introduction

157

STEGANOGRAPHIE

1 – Tatouage du son

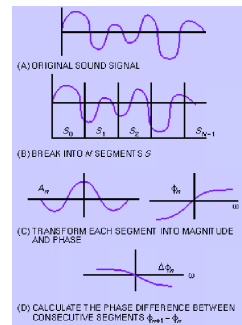
TATOUAGE DU SON

Plusieurs techniques :

- ☐ Codage de phase
Insertion de données par substitution de la phase d'un signal audio,
- ☐ Méthode spectrale
Le marquage est inséré dans les bandes fréquentielles du signal audio et camouflé par un bruit additif,
- ☐ Méthodes perceptuelles
Exploitation de la psychoacoustique,
- ☐ ...

159

TATOUAGE DU SON



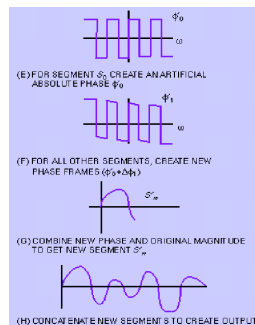
- ☐ Utilisation de la phase pour cacher une information dans un signal audio,
- ☐ Marque insérée reconnaissable,
- ☐ Découpage du signal en N échantillons et remplacement de la phase du premier par la donnée à cacher

méthode de codage de phase

160

TATOUAGE DU SON

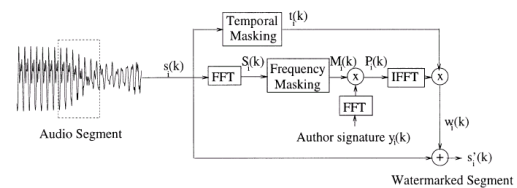
- ☐ Altération des échantillons suivants (phase)
- ☐ Marque facile à récupérer en déterminant la phase du premier échantillon



méthode de codage de phase

161

TATOUAGE DU SON



- ☐ Marque insérée aléatoire (nécessité d'avoir l'original pour la vérification),
- ☐ Utilisation de la psychoacoustique (masquage de fréquentiel et temporel)

méthode perceptuelle

162

TATOUAGE DU SON

Plusieurs logiciels existent pour le tatouage du son :

- ☐ Xidie (commercial) : WAV
- ☐ InvisibleSecrets (shareware) : WAV
- ☐ CryptArkan (shareware) : WAV
- ☐ SecureEngine4.0 (freeware) : WAV
- ☐ WeavWave (freeware) : WAV
- ☐ MP3Stego (freeware) : MP3, WAV
- ☐

Les logiciels

163

STEGANOGRAPHIE

2 – Tatouage des images

164

TATOUAGE DES IMAGES

L'image : tatouage ou Watermarking

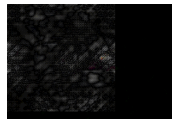
techniques issues du traitement du signal et des images (ex : transformée de Fourier ou DCT)



Image originale



Image tatouée



différence * 15

Exemple de tatouage d'une image :

Marquage sur un carré (de taille 2^n) dans l'image

165

TATOUAGE DES IMAGES

La méthode de marquage des bits de poids faibles (LSB)

utilisation du bit de poids faible du niveau de gris d'un pixel pour le codage du marquage

justification

l'œil ne discerne pas en général le changement du niveau de gris d'une valeur de + ou - 1.

Principe : insertion d'un filigrane sous la forme d'une image binaire

- mise à zéro du bit de poids faible du niveau de gris de chaque pixel de l'image
- codage du filigrane binaire sur ce bit de poids faible

166

TATOUAGE DES IMAGES



Image originale (8 bits)



Image codée sur 7 bits



Image tatouée



filigrane

Tatouage d'une image par la méthode des bits de poids faibles

167

TATOUAGE DES IMAGES

Plusieurs variantes :

- ☐ motif caché répété à différents endroits de l'image
- ☐ emplacement du motif à un endroit aléatoire
- ☐ dissimulation d'un texte en prenant chaque bit de codage d'un caractère (code ASCII sur 8 bits)
- ☐ chiffrement des données cachées (cryptographie)

Tatouage d'une image par la méthode des bits de poids faibles

168

TATOUAGE DES IMAGES

La méthode de marquage des n bits de poids faibles

généralisation de la méthode précédente au n bits de poids faible



Image originale

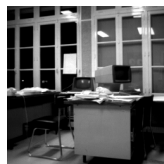


Image à masquer



Image tatouée

Tatouage d'une image (4 bits de poids faible)

169

TATOUAGE DES IMAGES



Image originale



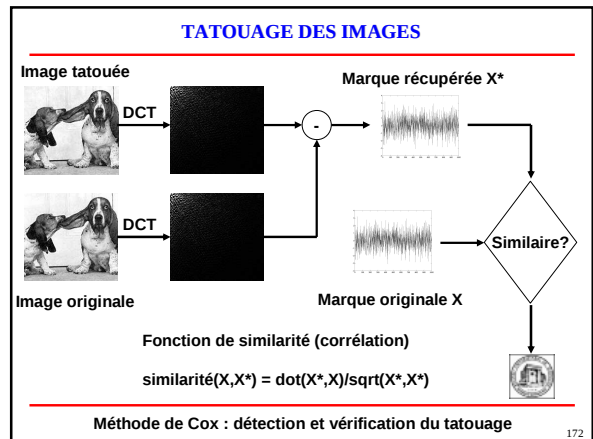
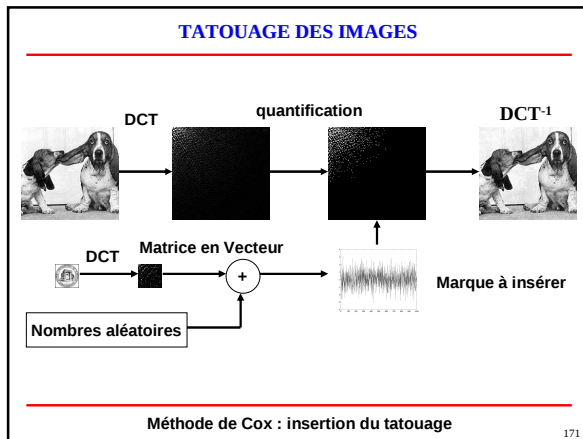
Image à masquer



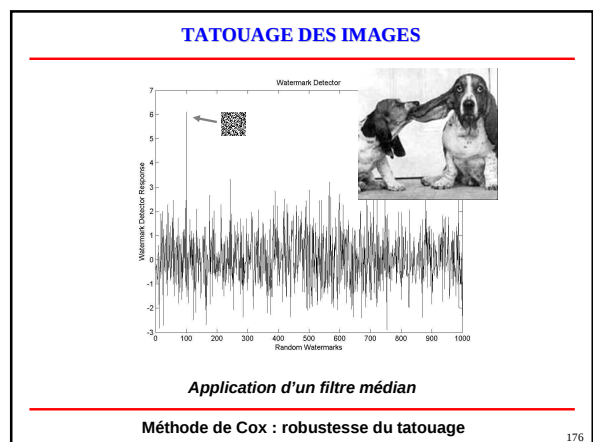
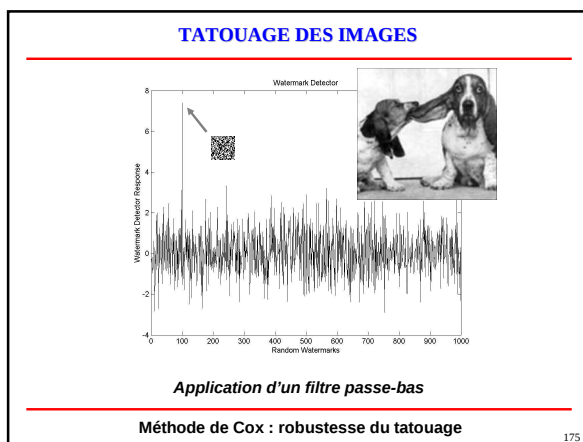
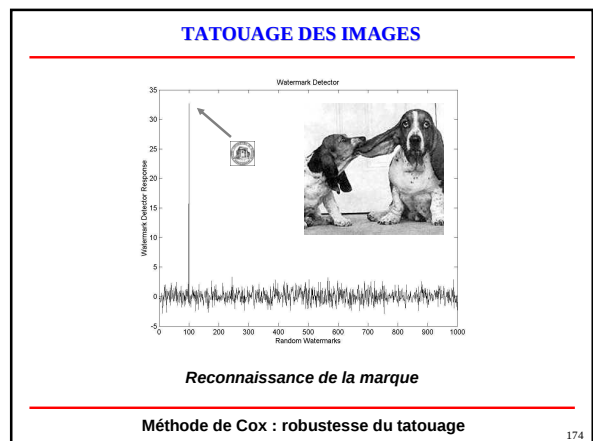
Image tatouée

Tatouage invisible d'une image

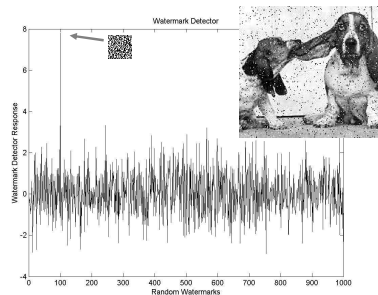
170



- ### TATOUAGE DES IMAGES
- Il existe deux types d'attaque d'un tatouage :**
- attaques destructives : utiliser des transformations sur l'image afin de détériorer ou supprimer le marquage.
 - compression JPEG
 - transformations géométriques (symétrie horizontale, rotation, changement d'échelle,...)
 - mosaïque : découper et recoller une image
 - attaque plus subtile de lavage de l'image sans l'endommager : suppression des hautes fréquences spatiales (détails) et conservation des basses fréquences (information significative).
- ➡ Utilisation de la transformée de Fourier
- Les attaques**
- 173



TATOUAGE DES IMAGES

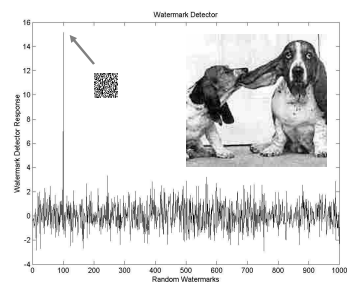


Bruitage de l'image

Méthode de Cox : robustesse du tatouage

177

TATOUAGE DES IMAGES



Compression JPEG

Méthode de Cox : robustesse du tatouage

178

TATOUAGE DES IMAGES

Plusieurs logiciels existent pour le tatouage d'images :

- ☐ Xidie (commercial) : BMP, JPEG
- ☐ InvisibleSecrets (shareware) : JPEG, PNG, BMP
- ☐ CryptArkan (shareware) : BMP
- ☐ SecureEngine4.0 (freeware) : BMP, JPEG
- ☐

Les logiciels

179

TATOUAGE DES IMAGES

Un logiciel d'évaluation de la robustesse du tatouage : Stirmark

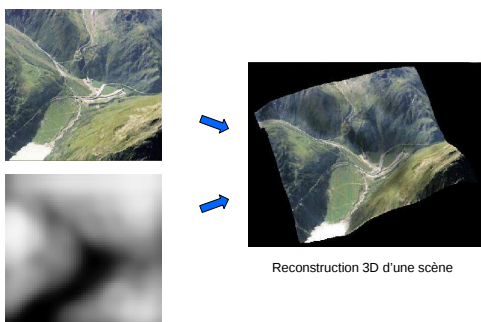
- ☐ objectif : évaluer les méthodes de tatouage actuelles
- ☐ création : 1997
- ☐ réalisation d'attaques du tatouage
- ☐ n'est pas destiné au piratage

<http://www.petitcolas.net/fabien/watermarking/stirmark/>

Les logiciels

180

TATOUAGE DES IMAGES



Reconstruction 3D d'une scène

sources : LIRMM UMR CNRS 5506

Applications : Tatouage des altitudes

181