Le watermarking digital pour images fixes

Travail de Bachelor réalisé en vue de l'obtention du Bachelor en

Informatique de Gestion HES

Par :

Alex VALLON

Conseiller au travail de Bachelor :

Peter Daehne, Professeur HES

Genève, 3 mai 2011

Haute École de Gestion de Genève (HEG-GE)

Filière Informatique de Gestion

Déclaration

Ce travail de Bachelor est réalisé dans le cadre de l'examen final de la Haute école de gestion de Genève, en vue de l'obtention du titre d'informaticien de gestion. L'étudiant accepte, le cas échéant, la clause de confidentialité. L'utilisation des conclusions et recommandations formulées dans le travail de Bachelor, sans préjuger de leur valeur, n'engage ni la responsabilité de l'auteur, ni celle du conseiller au travail de Bachelor, du juré et de la HEG.

« J'atteste avoir réalisé seul le présent travail, sans avoir utilisé des sources autres que celles citées dans la bibliographie. »

Fait à Genève, le 3 mai 2011

Alex VALLON

_____

Remerciements

Je souhaiterais remercier toutes les personnes m'ayant soutenu tout au long de mes études et de ce travail.

Je tiens à remercier particulièrement Monsieur Peter Daehne pour son soutien, sa disponibilité et ses conseils.

J'aimerais également remercier toutes les personnes qui ont contribué à mes sources.

Je remercie également Daniel Amor et Faustino Garcia, pour leur aide à l'évaluation des logiciels et à une phase de test.

Pour finir, je remercie ma famille.

Sommaire

Le début de ce travail présente brièvement le watermarking et ses différents champs d'applications, la suite du travail est axée sur le watermarking sur image fixe ; afin de bien comprendre celui-ci, deux formats d'image sont décrits.

Par la suite, le watermarking visible est présenté succinctement, car celui-ci est simple et n'apporte pas de grande valeur ajoutée aux images, puis le watermarking invisible est analysé plus profondément.

Une analyse multicritères est faite sur différents logiciels de watermarking pour sélectionner les quatre logiciels les plus susceptibles d'être utilisés. Une fois les quatre logiciels sélectionnés, des tests de robustesse sont réalisés, afin d'apprendre quelles modifications peuvent effacer le watermarking, dans le but d'élaborer une stratégie de mise en œuvre.

Liste des mots clefs : watermarking, empreinte digitale, étalement de spectre, fractale, patchwork, bits de poids faible, copyright, droit d'auteur, jpeg, bitmap.

Table des matières

Liste des Tableaux

Liste des Figures

Introduction

À l'époque où les appareils photographiques n'existaient pas, pour « immortaliser » un paysage, il fallait le peindre. Pour « recopier » cette peinture à l'identique, cela demandait du temps et du savoir-faire.

L'invention de l'appareil photo avec support négatif[1] a permis, suivant un procédé chimique, la production de photographies en nombre illimité de tirages. À l'époque pour « copier » une photo, il fallait soit posséder le négatif soit capturer l'image au moyen d'un appareil photo ; mais cette dernière méthode occasionne des pertes de qualité. Plus tard, la photocopieuse fut inventée et permit une « copie » de la photo avec une perte minime, pour ce faire, il faut pouvoir manipuler la photo en question.

Finalement, avec l'ère de l'informatique est apparu le scanner qui permet de numériser les images (mais comme pour la photocopieuse, il faut manipuler la photo) et l'appareil photo numérique (APN). Le scanner et l'APN génèrent des fichiers numériques, ce qui par la même occasion facilite la copie identique et instantanée du fichier et donc de la photographie.

La copie étant devenue beaucoup plus simple qu'au temps des tableaux, la nécessité de protéger les images, en termes de droit d'auteur, est devenue une grande préoccupation ces dernières années. Partant de ce problème, nous allons au cours de ce rapport analyser les différents moyens existants de protection d'images numériques, c'est-à-dire, les différentes façons de faire du « digital watermarking ».

1 Feuille sensible qui réagit à la lumière, le noir devient blanc, et inversement. Grâce à un procédé chimique, l'image se forme avec les bonnes couleurs.

1. Qu’est-ce que le watermarking ?

Le « watermarking », « tatouage numérique » ou encore « empreinte numérique » est l'art d'insérer de l'information dans une image ou dans n'importe quel autre document numérique, à des fins de copyright ou d’ajout d’information.

1.1 Types de Watermarking

1.1.1 Image

1.1.1.1 Applications

Les champs d’application du watermarking sur image servent à des fins de notoriété voire publicitaire, au contrôle de la véracité de photos, à la protection de la propriété intellectuelle et, récemment, le watermarking peut servir de « pont » entre une image imprimée et un site web.

1.1.1.2 Concepts

Il existe plusieurs concepts de watermarking, le filigrane, la modification de bits de poids faible, l’étalement de spectre, la technique du Patchwork, les fractales et l’algorithme de Koch et Zhao.

1.1.2 Audio

1.1.2.1 Applications

Deux champs d’application sont beaucoup étudiés pour le watermarking audio : la mesure de l’audience (TV, radio) et la protection de la propriété intellectuelle.

1.1.2.2 Concepts

Les techniques propres au watermarking audio sont le watermarking par phase, le watermarking par écho et le watermarking par étalement de spectre.

Ces trois techniques n’entrainent pas une modification du son perceptible pour l’humain, le signal rajouté est inaudible.

1.1.3 Vidéo

1.1.3.1 Applications

Les champs d’applications du watermarking pour la vidéo sont la publicité et la protection de la propriété intellectuelle.

1.1.3.2 Concepts

Pour le watermarking sur vidéo, il existe plusieurs concepts tels que la modification de vecteurs de mouvement, la compression fractale, la transformée de coefficients, la modulation d'indice de quantification et l'étalement de spectre.

Dans ce rapport, nous nous concentrerons sur les images fixes comme support pour informations.

Il existe deux types de watermarking que nous aborderons plus tard :

- Le watermarking visible.
- Le watermarking invisible.

2. Historique

Le terme « watermarking » vient d'un procédé utilisé en 1282 qui servait à ajouter un filigrane visible dans du papier pour l'identification (marque de production, papier de qualité). Aujourd'hui, le filigrane est utilisé pour garantir l'authenticité de documents officiels (billets de banque, ordonnance médicale). Les filigranes doivent être difficilement imitables, afin d'empêcher la contrefaçon, et ne doivent pas altérer le document.

Le watermarking digital (tatouage numérique) est une pratique récente, le premier article parlant d'une technique de watermarking date du début des années 90. Mais le terme « digital watermarking » apparaît en 1992 dans l'ouvrage « Electronic Water Mark »[2].

2 A.Z. Tirkel et al. « Electronic Water Mark ». 1992. p.666-673

3. Formats d'images

3.1 Introduction

Il est important de bien connaître le format d'une image numérique afin de mieux comprendre comment fonctionnent certaines techniques de watermarking. C'est pourquoi nous allons examiner deux formats d'images.

3.2 Windows bitmap (BMP)

3.2.1 Introduction

Nous allons tout d'abord décrire le format « Windows bitmap» sur 24 bits, car c'est l'un des formats les plus simples et il n'est pas propriétaire. Il a été développé par Microsoft et IBM.

3.2.2 Structure du bitmap

Nous pouvons décomposer le bitmap 24 bits en 3 zones :

- L'en-tête du fichier.
- L'en-tête de l'image.
- Les données relatives à l'image (le corps de l'image).

Dans notre cas, seule la structure du corps de l'image nous intéresse, car c'est dans cette partie du fichier que sera effectué le watermarking.

Les versions bitmap inférieures à 24 bits contiennent une palette pour définir les couleurs, il est possible de faire du watermarking grâce à la palette en suivant les mêmes techniques. Cependant, le watermarking sur ces palettes ne va pas être analysé, car il n'a aucune chance de résister à une conversion de type.

3.2.2.1 L'en-tête du fichier (BITMAPHEADER)

C'est ici qu'est indiqué les informations sur le type de fichier, sa taille et où commencent les informations de l'image.

Offset#	Taille	Description
0x0000	2 octets	Le nombre magique correspondant à l'utilisation du fichier BMP : BM - Windows 3.1x, 95, NT, etc…
0x0002	4 octets	La taille du fichier en octets
0x0006	2 octets	Réservés pour l'identifiant de l'application qui a créé le fichier
0x0008	2 octets	Réservés pour l'identifiant de l'application qui a créé le fichier

0x000A	4 octets	L'offset (l'adresse de départ) du contenu du BMP

Tableau 1 : Bitmapheader

3.2.2.2 L'en-tête de l'image (BITMAPINFOHEADER)

Dans l'en-tête de l'image se trouvent les informations concernant les dimensions et les couleurs de l'image.

Offset #	Size	Description
0x00Eh	4 octets	La taille de l'en-tête elle-même.
0x012h	4 octets	La largeur de l'image en pixels.
0x016h	4 octets	La hauteur de l'image en pixels.
0x01Ah	2 octets	Le nombre de plans de couleurs utilisées (toujours à 1).
0x01Ch	2 octets	Le nombre de bits par pixel (la profondeur de la couleur). Dans notre cas 24.
0x01Eh	4 octets	La méthode de compression (dans notre cas aucune → 0)
0x022h	4 octets	La taille de l'image en octets (utile pour la compression).
0x026h	4 octets	La résolution horizontale de l'image (pixel par mètre).
0x02Ah	4 octets	La résolution verticale de l'image (pixel par mètre).
0x02Eh	4 octets	Le nombre de couleurs dans la palette (dans notre cas 0).
0x032h	4 octets	Le nombre de couleurs importantes (généralement à 0).

Tableau 2 : Bitmapinfoheader

3.2.2.3 Les données relatives à l'image (le corps de l'image)

Cette dernière zone contient les données liées à l'image. Dans notre cas (image Windows bitmap 24 bits), la couleur des pixels de l'image va être définie par une suite de 3 octets. Le premier octet définit le niveau de bleu, le deuxième octet définit le niveau de vert et le troisième octet définit le niveau de rouge.

L'image va être construite au moyen de lignes, qui sont elles-mêmes constituées de pixels. Le premier pixel défini concerne celui qui est placé tout en bas à gauche de l'image. Les lignes doivent obligatoirement être constituées d'un nombre total d'octets qui doit être un multiple de quatre.

3.3 *Joint Photographic Experts Group (JPEG)*

3.3.1 Introduction

Pour le deuxième format, nous allons décrire le format « JPEG » ou plutôt la « norme JPEG ». JPEG est une norme qui définit l'algorithme et le format de décodage. Ce format utilise une compression avec perte (il existe un format sans perte, mais celui-ci n'est que très peu utilisé). C'est l'un des formats les plus utilisés sur Internet de par sa petite taille.

3.3.2 Compression d'un JPEG

3.3.2.1 Introduction

L'algorithme de compression JPEG se compose de différentes étapes. (Les étapes entrainant une perte sont représentées sur fond gris)

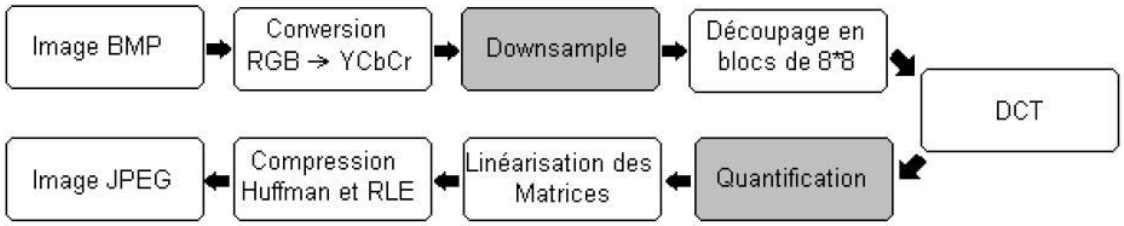


Figure 1 : La compression JPEG[3]

3.3.2.2 Conversion RGB à YCbCr

L'œil humain étant plus sensible à la luminance (intensité lumineuse, clarté) qu'à la chrominance (la couleur), pour compresser une image, le format JPEG va « jouer » sur les valeurs de la couleur même et non pas sur la clarté de l'image. De cette façon, la différence de qualité de l'image ne sera que très peu visible (cela dépend du taux de compression).

Le système de codage RGB n'est donc pas approprié pour réussir à « jouer » sur la valeur de la chrominance puisque les valeurs de la clarté de l'image sont imbriquées avec ceux de la couleur. Tandis qu'avec le système de codage YCbCr, la clarté et séparée de la chrominance. C'est pourquoi l'algorithme JPEG va convertir les valeurs RGB en YCbCr. L'algorithme de conversion est le suivant :

- Y= (0.299*R) + (0.587*G) + (0.114*B)
- Cb=(-0.1687*R) – (0.3313*G) + (0.5*B) + 128
- Cr= (0.5*R) – (0.41874*G) – (0.0813*B) + 128

3 http://r0ro.free.fr/tipe/docs/TIPE.pdf

Suite à cette étape, il n'y a pas de pertes d'information.

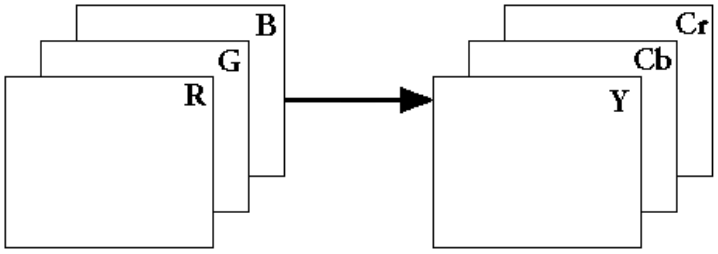


Figure 2 : Passage RGB à YCbCr

3.3.2.3 « Downsample » (Sous-échantillonnage)

Cette étape va engendrer une perte de qualité puisqu'elle consiste à (pour les informations de chrominance) sous-échantillonner l'image ; concrètement, le JPEG va garder la moyenne de quatre pixels. Dans ce cas-là, le sous-échantillonnage est appelé 2h2v (2:2 horizontalement et verticalement). La luminance ne subit pas de sous-échantillonnage.

Sur une photo ou une image quelconque, ne garder en mémoire que la moyenne de chrominance de quatre pixels, au lieu des informations entières des quatre pixels, n'est pas dérangeant ; puisque l'œil ne distingue pas les petites voire moyennes différences de couleur au sein d'un carré de deux sur deux pixels.

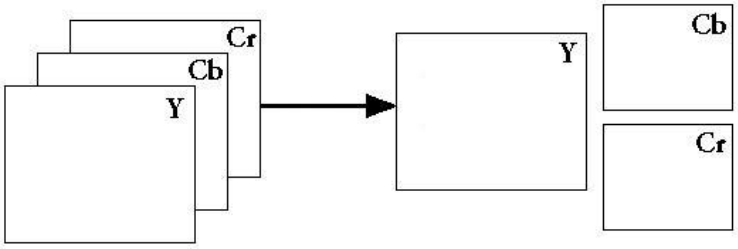


Figure 3 : Sous-échantillonnage

3.3.2.4 Discrete Cosine Transform (DCT)

Cette étape va être appliquée sur des blocs de huit pixels par huit et sur chaque « plan » (Y, Cb et Cr). L'image est pour ainsi dire « découpée » en blocs.

L'étape consiste à convertir les blocs, qui sont des matrices de pixels, par une « carte » de fréquences et d'amplitudes. La DCT décompose un bloc en 64 signaux (fréquences spatiales).

La DCT permet de séparer les basses fréquences des hautes fréquences de l'image ; les premières vont se retrouver en haut à gauche de la « carte » et les secondes en bas à droite. L'œil humain est plus sensible aux basses fréquences.

La DCT utilise l'algorithme suivant :

$$\mathrm{DCT}(i,j) = \frac{2}{N} C(i) C(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \mathrm{pixel}(x,y) \cos\left[\frac{(2x+1)i\pi}{2N}\right] \cos\left[\frac{(2y+1)j\pi}{2N}\right]$$

Figure 4 : Transformée DCT directe[4]

C'est un algorithme complexe et dur à comprendre, mais sa maîtrise n'est pas indispensable pour la compréhension du format JPEG.

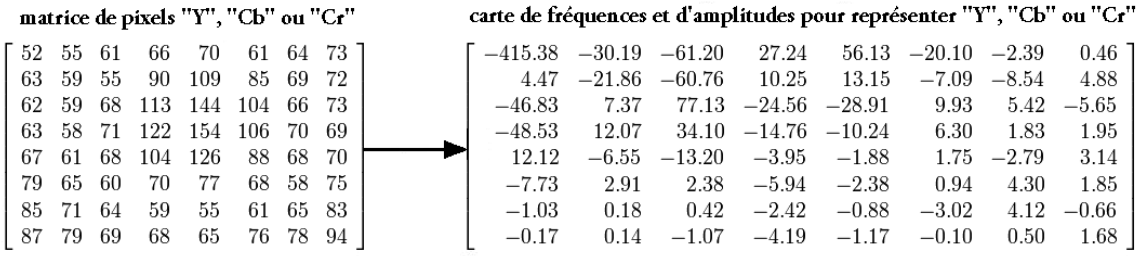


Figure 5 : Transformation DCT

3.3.2.5 Quantification

La quantification est l'étape qui va entraîner le plus de pertes de qualité d'image, mais qui permet une meilleure compression.

L'étape consiste à atténuer les fréquences, en particulier les hautes fréquences qui sont en bas à droite de nos « cartes » et auxquelles l'œil humain est peu sensible. Les « cartes » vont être divisées par des matrices de quantification. Plus la quantification est importante, plus la qualité de l'image est mauvaise.

La recommandation T.81 de l'ITU propose deux tables de quantification, une pour la luminance (« Y ») et une pour les chrominances (« Cr » et « Cb »). Il est toutefois possible de créer ses propres tables de quantification.

Luminance quantization table

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Chrominance quantization table

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

Figure 6 : Tables de quantification

4 http://fr.wikipedia.org/wiki/JPEG

carte de fréquences et d'amplitudes pour représenter "Y"

$$\begin{bmatrix} -415.38 & -30.19 & -61.20 & 27.24 & 56.13 & -20.10 & -2.39 & 0.46 \\ 4.47 & -21.86 & -60.76 & 10.25 & 13.15 & -7.09 & -8.54 & 4.88 \\ -46.83 & 7.37 & 77.13 & -24.56 & -28.91 & 9.93 & 5.42 & -5.65 \\ -48.53 & 12.07 & 34.10 & -14.76 & -10.24 & 6.30 & 1.83 & 1.95 \\ 12.12 & -6.55 & -13.20 & -3.95 & -1.88 & 1.75 & -2.79 & 3.14 \\ -7.73 & 2.91 & 2.38 & -5.94 & -2.38 & 0.94 & 4.30 & 1.85 \\ -1.03 & 0.18 & 0.42 & -2.42 & -0.88 & -3.02 & 4.12 & -0.66 \\ -0.17 & 0.14 & -1.07 & -4.19 & -1.17 & -0.10 & 0.50 & 1.68 \end{bmatrix}$$

Luminance quantization table

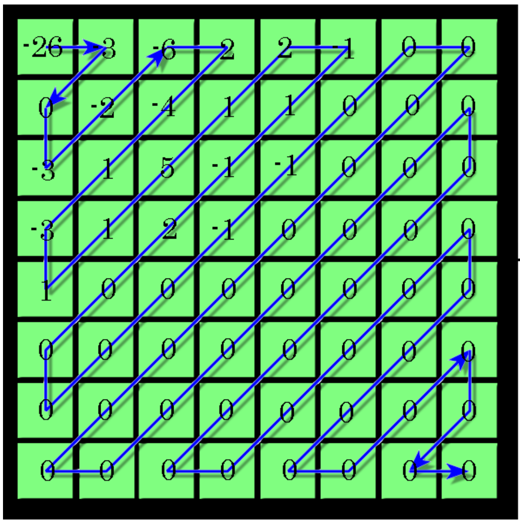
$$\begin{bmatrix} 16 & 11 & 10 & 16 & 24 & 40 & 51 & 61 \\ 12 & 12 & 14 & 19 & 26 & 58 & 60 & 55 \\ 14 & 13 & 16 & 24 & 40 & 57 & 69 & 56 \\ 14 & 17 & 22 & 29 & 51 & 87 & 80 & 62 \\ 18 & 22 & 37 & 56 & 68 & 109 & 103 & 77 \\ 24 & 35 & 55 & 64 & 81 & 104 & 113 & 92 \\ 49 & 64 & 78 & 87 & 103 & 121 & 120 & 101 \\ 72 & 92 & 95 & 98 & 112 & 100 & 103 & 99 \end{bmatrix}$$

$$\rightarrow \begin{bmatrix} -26 & -3 & -6 & 2 & 2 & -1 & 0 & 0 \\ 0 & -2 & -4 & 1 & 1 & 0 & 0 & 0 \\ -3 & 1 & 5 & -1 & -1 & 0 & 0 & 0 \\ -3 & 1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Figure 7 : Quantification

3.3.2.6 Run Length Coding (RLE) et Compression Huffman

Le résultat de la quantification donne une matrice contenant beaucoup de zéros. La matrice va être lue en zigzag (linéarisation de la matrice) afin de rapprocher les valeurs identiques et de ramener le maximum de zéros vers la fin de la séquence. Une majorité de zéros se retrouvent donc à la fin de la séquence, l'algorithme RLE va pouvoir les compresser. Au lieu de coder une séquence de nombres, le codage RLE va coder en paires (skip, value), « skip » est le nombre de zéros précédant la « value » (valeur d'un nombre non nulle) et un « End Of Bloc » va signaler que la fin de la séquence se terminera que par des zéros.



→ (-26 -3 0 -3 -2 -6 2 -4 1 -3 1 1 5 1 2 -1 1 -1 2 0 0 0 0 0 -1 -1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0)

Figure 8 : Lecture en zigzag

RLE : (0 ;-26) (0 ;-3) (1 ;-3) (0 ;-2) (0 ;-6) (0 ;2) (0 ;-4) (0 ;1) (0 ;-3) (0 ;1) (0 ;1) (0 ;5) (0 ;1) (0 ;2) (0 ;-1) (0 ;1) (0 ;2) (5 ;-1) (0 ;-1) EOB.

Puis l'algorithme de Huffman sera appliqué à cette séquence.

3.3.3 Décompression d'un JPEG

La décompression consiste à exécuter les étapes de la compression en sens inverse. Les pertes d'information étant déjà occasionnées par la compression, l'image d'origine ne pourra pas être reproduite avec la même qualité d'image.

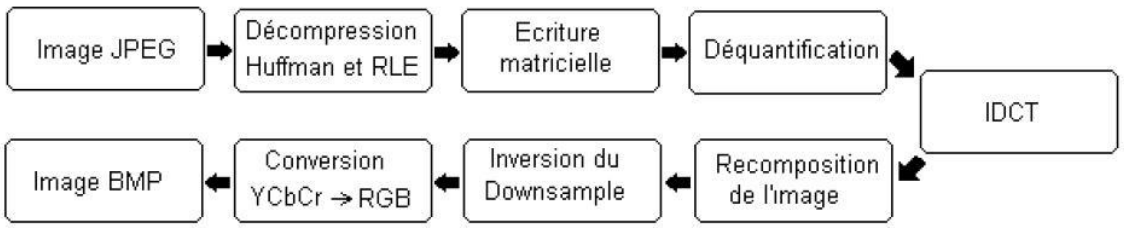


Figure 9 : La décompression JPEG[5]

3.3.3.1 Décompression Huffman et Run Length Coding (RLE)

L'algorithme d'Huffman est appliqué en premier sur les informations de l'image, puis le RLE est appliqué en sens inverse ; au lieu de former des paires, il va les désassembler.

3.3.3.2 Déquantification

Cette étape va être appliquée à des matrices. Les informations sont donc remises en matrices par le moyen de l'écriture en zigzag.

Puis les matrices vont être, cette fois-ci, multipliées par les matrices de quantification.

3.3.3.3 Inverse Discrete Cosine Transform (IDCT)

L'étape consiste à convertir (avec la formule IDTC) les blocs qui sont, à cette étape, des « cartes » de fréquences et d'amplitudes, par des matrices de pixels.

$$\mathrm{pixel}(x,y) = \frac{2}{N}\sum_{i=0}^{N-1}\sum_{j=0}^{N-1} C(i)C(j)\,\mathrm{DCT}(i,j)\cos\left[\frac{(2x+1)i\pi}{2N}\right]\cos\left[\frac{(2y+1)j\pi}{2N}\right]$$

Figure 10 : Transformée IDCT directe[6]

3.3.3.4 Inversion du « Downsample »

Cette étape consiste à (pour les informations de chrominance) suréchantillonner l'image, concrètement, le JPEG va recomposer quatre pixels avec la moyenne qu'il avait enregistrée.

---

5 http://r0ro.free.fr/tipe/docs/TIPE.pdf

6 http://fr.wikipedia.org/wiki/JPEG

3.3.3.5 Conversion YCbCr à RGB

Pour l'affichage le JPEG va reconvertir les valeurs YCbCr en RGB. L'algorithme de conversion est le suivant :

- $R = Y + 1{,}402 * (Cr - 128)$
- $G = Y - 0{,}34414 * (Cb - 128) - 0{,}71414 * (Cr - 128)$
- $B = Y + 1{,}772 * (Cb - 128)$

Après cette étape, l'information sur les pixels de l'image est transformée en données affichables par un écran.

4. Le watermarking visible

4.1 Introduction

En informatique, certaines idées sont calquées sur la vie « réelle ». Le watermarking n'échappe pas à cette « règle ». Le watermarking peut être comparé aux antivols que nous pouvons voir sur les habits. Il en existe plusieurs sortes. Les visibles, qui sont là pour dissuader les voleurs et les invisibles qui sont cachés dans le produit pour essayer de prendre le voleur en faute.

Si toutefois nous voulons enlever un antivol visible, il existe plusieurs façons. Une de ces de façon est de déchirer l'habit autour de l'antivol. C'est pareil pour une image, une façon d'enlever la marque est de découper autour. Dans les deux cas, cela laisse un trou indésirable.

4.2 Technique

4.2.1 Le filigrane

Le watermarking visible, communément appelé filigrane, a deux principales utilisations différentes. La première étant d'insérer la « signature » de l'artiste, d'une entreprise ou d'un site web à des fins de notoriété ou publicitaires. Cette signature ne dégrade l'image qu'à l'endroit où elle est ajoutée et est facilement effaçable à l'aide d'un logiciel de retouche d'image. Cette technique n'est pas très appropriée pour protéger une photo, car plus la signature est grande moins le sujet de l'image sera visible, mais plus elle est petite plus il sera facile de l'enlever.

La deuxième a pour but de montrer un « échantillon » d'une image et d'empêcher son utilisation telle quelle. Cette façon de faire « dégrade » volontairement et en grande partie l'image de telle manière à ce qu'il devient très difficile de supprimer la marque.

Finalement les deux utilisations peuvent être mises en œuvre simultanément.

4.3 Pratique

4.3.1 Introduction

Certains éditeurs d'images offrent la possibilité d'ajouter automatiquement un filigrane sur l'image en guise de watermark (marque). Nous allons voir qu'il est assez facile dans la plupart des cas d'insérer un filigrane.

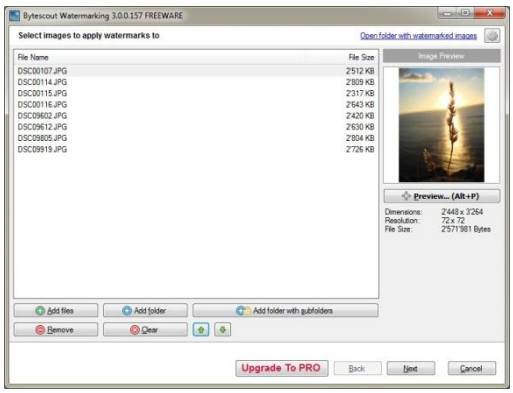
4.3.2 « Watermarking » par Bytescout, version 2.5

4.3.2.1 Présentation

La société « ByteScout » propose des logiciels pour les utilisateurs amateurs et professionnels ainsi que des outils de développement pour les développeurs de logiciels (ActiveX, .NET SDK).

Bytescout propose une version gratuite, mais bridée de leur logiciel « Watermarking ». Ce programme permet d'ajouter de manière automatique un filigrane personnalisé à des images préalablement sélectionnées. C'est un logiciel dont l'utilisation est vraiment instinctive. Il suffit de choisir l'image, les images ou un dossier contentant les images que vous voulez marquer puis de régler quelques paramètres concernant le filigrane souhaité et le logiciel fera une copie de vos images avec la marque.

4.3.2.2 Test



4.3.2.3 Résultats

4.3.3 Autres éditeurs d'image testés

4.3.3.1 FastStone Image Viewer

FastStone Image Viewer est un éditeur, navigateur et convertisseur d'images. Il a plusieurs fonctionnalités (visionnement d'image, comparaison, suppression des yeux rouges, mailing, redimensionnement, recadrage, retouche et ajustements des couleurs). Bien que ce soit un outil puissant, l'ajout de filigranes n'est pas sa fonctionnalité prioritaire, en effet, l'outil est bien caché dans les options.

4.3.3.2 PhotoScape

PhotoScape est un logiciel qui permet de retoucher des photos avec des outils. Dans ce logiciel l'ajout de filigranes n'est pas mentionné en tant que tel ; il est possible d'ajouter du texte ou des images qui serviront de filigranes.

4.3.3.3 Adobe Photoshop Lightroom

Lightroom 3.3 est un logiciel développé par Adobe Systems, créé pour assister les photographes professionnels en postproduction. Il permet de gérer les flux de productions photographiques de l'importation des données depuis un périphérique jusqu'à la publication. L'ajout de filigranes est une option lors de l'exportation (de l'enregistrement) de photos, il est possible de sauvegarder plusieurs signatures différentes.

5. Le watermarking invisible

5.1 Introduction

Le watermarking invisible est le fait d'ajouter une marque dans une image, son atout majeur sur le watermarking « visible » est qu'il ne détériore pas l'image et qu'il est plus difficilement détectable. Par conséquent, il devrait être moins évident de l'enlever. Comment supprimer volontairement quelque chose quand on ignore son existence ?

5.1.1 Watermarking invisible ou stéganographie ?

Le watermarking « invisible » peut être considéré comme de la stéganographie. La stéganographie est l'art de dissimuler un message dans n'importe quel support (image, audio, etc…). Le principe du watermarking invisible est de cacher puis récupérer une marque dans une image. La seule différence avec la stéganographie se trouve dans l'objectif ; la stéganographie a pour but de transmettre un message, une information qui avec le temps deviendra obsolète. Tandis que le watermarking a pour but de laisser une « empreinte » sur le fichier.

5.1.2 Approche

Le watermarking peut être comparé au schéma de communication de la figure 11. Les deux modèles transmettent des données d'un émetteur à un récepteur ; le message est la marque qui va être encodée puis ajoutée dans une image, le canal (channel) représente l'image marquée, le bruit (noise) représente les modifications possibles sur l'image. Le décodeur va récupérer la marque.

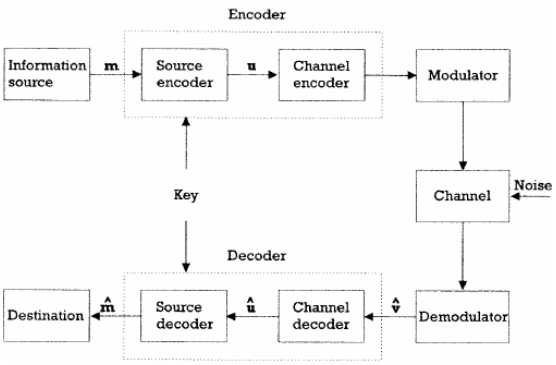


Figure 11 : Schéma de communication basique pour une transmission sécurisée.[7]

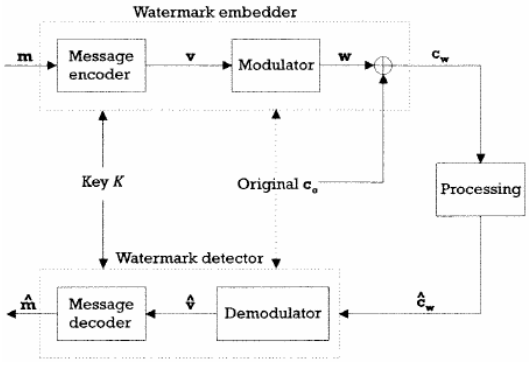


Figure 12 : Modèle basique de watermarking.

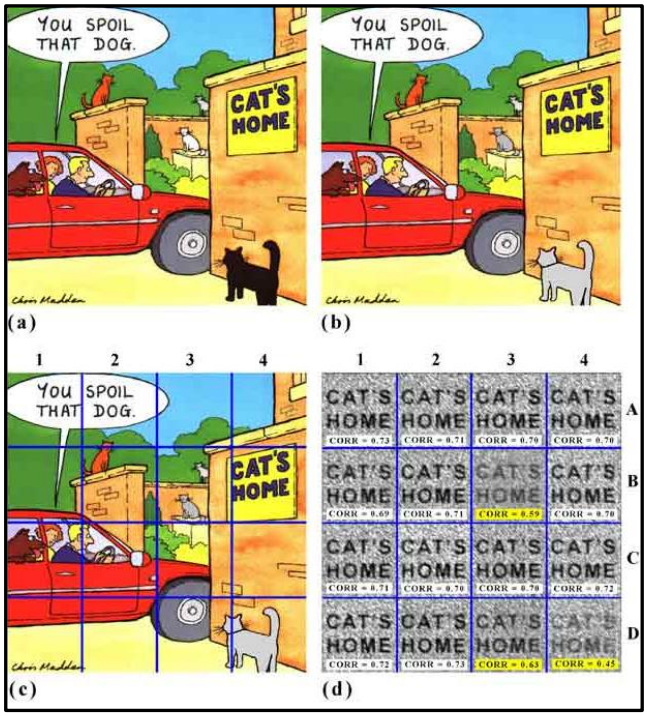
7 ARNOLD, Michael et al. « Techniques and applications of digital watermarking and content protection ». 2003.

5.1.3 Objectifs

5.1.3.1 Contrôler la véracité des photos

La modification de photo peut, dans certains cas, ne pas poser de problèmes (par exemple, pour les photos artistiques), mais dans certains cas, il est important de pouvoir vérifier si la photo est modifiée ou non.

Le principe est de marquer la photo dans le but de pouvoir contrôler sa véracité. Une watermark conçue à cet effet doit être « fragile », le moindre changement de la photo doit effacer la watermark.



La figure 13a représente une œuvre originale watermarquée, la figure 13b représente l'image après modification ; la figure 13d représente la marque qui provient de l'image modifiée, il est possible de voir qu'à certains endroits, la marque a été altérée.

Figure 13 : Watermarking fragile[8]

Ce procéder pourrait être utilisé par les satellites pour assurer la véracité des clichés pris, afin d'éviter toutes manipulations, ou par les médias qui souhaiteraient contrôler l'authenticité de photos[9].

Pour le cas d'un photographe, le dilemme est de savoir à quel moment poser la marque. À première vue, le choix le plus judicieux serait d'insérer la marque lors de la

8 New Invisible Watermark to Prevent Fake Photos : http://www.livescience.com/3869-invisible-watermark-prevent-fake-photos.html

9 New Invisible Watermark to Prevent Fake Photos : http://www.livescience.com/3869-invisible-watermark-prevent-fake-photos.html

capture de la photo (laisser l'APN gérer le watermarking), pas si judicieux que ça, car premièrement cela augmenterait le délai d'enregistrement de la photo et deuxièmement toutes photos n'ont, apparemment, pas lieu d'être marquées.

Un second choix serait de laisser le photographe marquer la photo, mais cela ne l'empêcherait pas de modifier le contenu avant l'application du watermarking.

Il existe aujourd'hui une autre option pour vérifier l'authenticité d'une photo ; TUNGSTENE : Tungstène est un logiciel permettant de détecter les modifications apportées par un logiciel de retouche d'image (Photoshop). Il a notamment été utilisé lors d'un procès pour prouver qu'une photo, à charge contre un accusé, avait été modifiée.

Exemple de modification de photo :

Figure 14 : Suppression d'une personne sur une photo[10]

Détection de modifications par Tungstène :

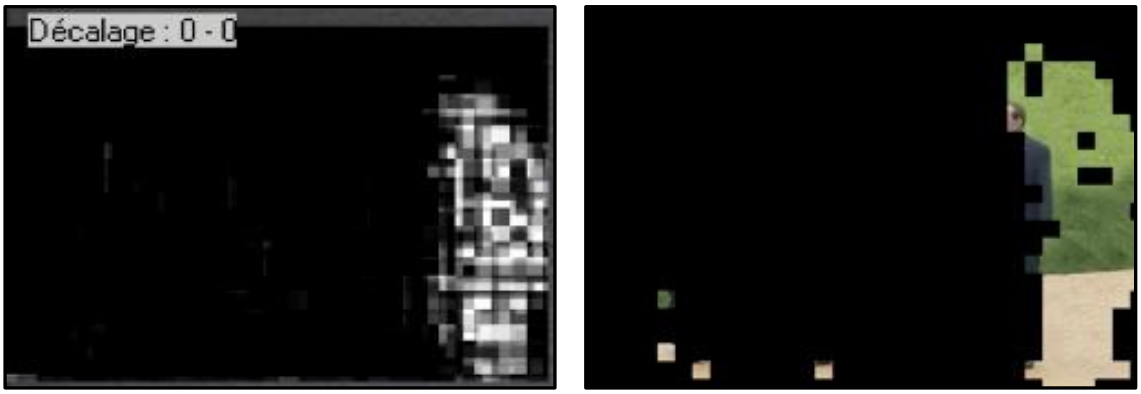


Figure 15 : Zones de détection de modification de la photo[11]

10 http://www.exomakina.com/eXo_maKina/Cobalt.html

11 http://www.exomakina.com/eXo_maKina/Cobalt.html

Exemple d'authentification de photo par Tungstène :

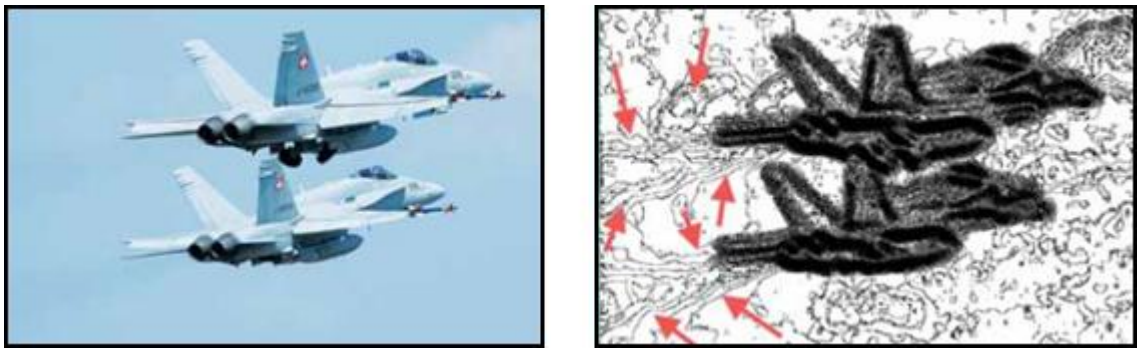


Figure 16 : Détection de l'authenticité d'une photo[12]

5.1.3.2 La protection de la propriété intellectuelle

Internet peut être utilisé comme une grande vitrine ouverte sur le monde, les photographes professionnels y exposent leurs œuvres dans le but de les vendre et de trouver de nouveaux clients. Le problème réside dans le fait qu'il faut réussir à intéresser les clients potentiels en leur montrant des photos de qualité tout en évitant de se les faire « voler ».

Essayer d'empêcher la copie de la photo est une mauvaise stratégie, puisqu'une œuvre diffusée a le droit d'être utilisée à des fins privées (voir annexe 1 : art 19. Al 1). C'est la rediffusion de l'œuvre qui est illégale ; donc c'est à ce moment-là qu'il faut prouver que l'œuvre nous appartient bel est bien, c'est là qu'entre en jeu le watermarking.

5.1.3.3 Conteneur d'informations

Comme le code QR (voir annexe 2), le watermarking peut servir de conteneur d'informations, dans la plupart des cas, l'information introduite dans l'image est un lien URL. À l'aide d'une application adéquate, l'information peut être lue et le lien URL peut être directement utilisé.

5.2 Techniques

5.2.1 Introduction

Les techniques de watermarking de ce chapitre sont analysées dans leur version de base autant que possible, il existe aujourd'hui des versions améliorées pour la plupart de ces techniques.

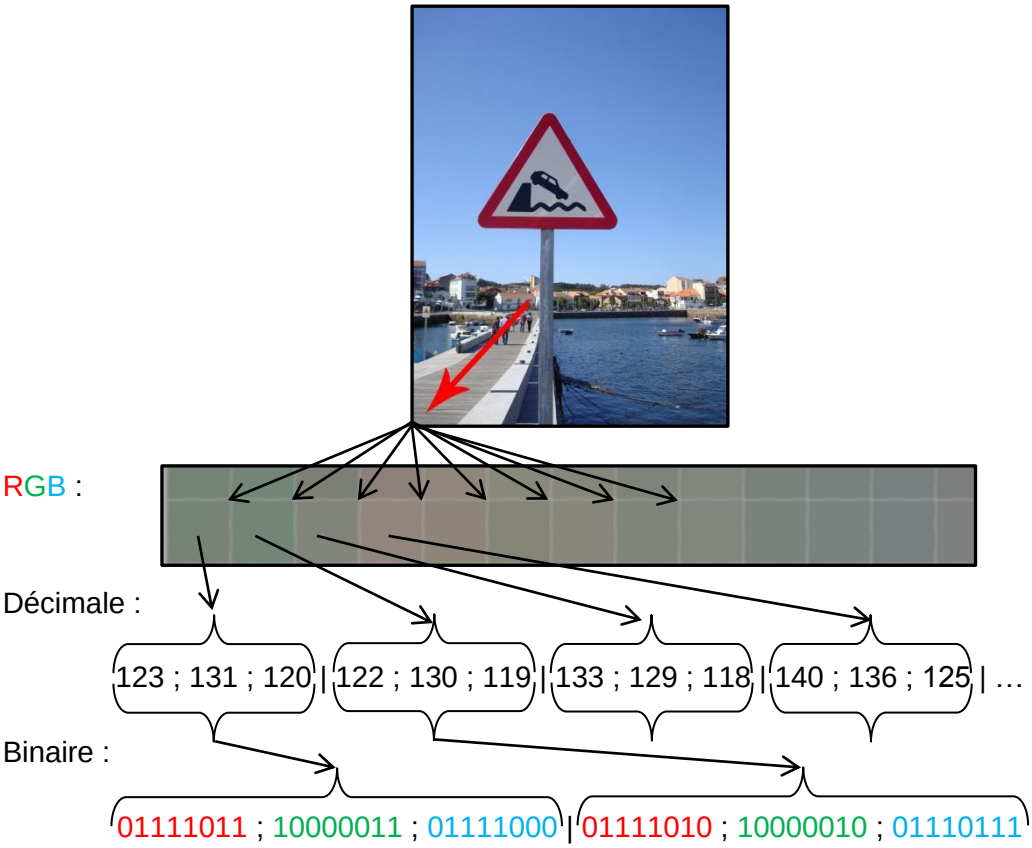
12 http://www.exomakina.com/eXo_maKina/Tungstene.html

Pour marquer une photo, il est envisageable de combiner plusieurs techniques.

5.2.2 Modification des bits de poids faible

Une première technique consiste à modifier les bits de poids faibles des octets qui servent à définirent la couleur des pixels sachant que l'œil humain ne verra pas la différence de couleur. Cette technique est peu robuste (elle est très sensible à la moindre manipulation de l'image) et est détectable à l'aide d'une analyse statistique des bits de poids faibles et donc, cette technique n'est pas entièrement « invisible ».

Exemple : Dans cet exemple, je vais marquer l'image avec mon nom : « VALLON » → valeur de la table ascii en décimal « 86 65 76 76 79 78 » → valeur en binaire « 01010110 | 01000001 | 01001100 | 01001100 | 01001111 | 01001110 »



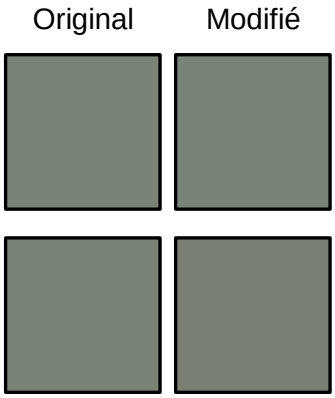
Commencement de l'insertion de « VALLON » (01010110 | 0100…):

01111001 ; 10000001 ; 01111001 | 01111010 ; 10000001 ; 01110100

Valeurs décimales après modification :

121 ; 131 ; 121 | 122 ; 129 ; 116

Comparaison entre les pixels :



La différence de couleur n'est pas perceptible à l'œil nu.

5.2.3 Watermarking par étalement de spectre

La technique du watermarking par étalement de spectre a été présentée par Cox et al.[13]. Elle consiste à extraire une séquence de données depuis les basses fréquences de l'image (l'image subit une transformation DCT) puis la marque est ajoutée à cette séquence ; la séquence modifiée est réinsérée dans l'image.

Pour vérifier si une photo est marquée, il faut posséder la photo originale, la marque originale et la photo potentiellement marquée ; transformer les deux photos dans le domaine des fréquences (DCT) puis soustraire leur valeur afin d'obtenir une séquence qui sera comparée à la marque originale.

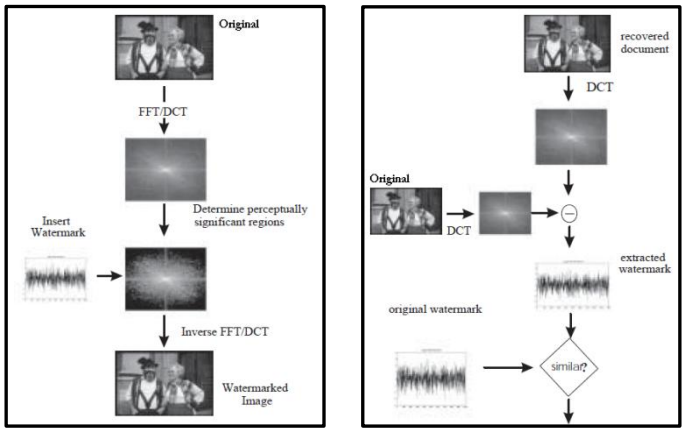


Figure 17 : Étapes d'insertion et de détection de watermarking[14]

13 Ingemar J. Cox, Joe Kilian, F. Thomson Leighton, and Talal Shamoon « Secure Spread Spectrum Watermarking for Multimedia »

14 Ingemar J. Cox et al. « Secure Spread Spectrum Watermarking for Multimedia »

5.2.4 Technique du "patchwork"

La technique du « patchwork » a été présentée par Bender et al.[15]. C'est une technique qui permet seulement de poser une marque et non un message.

Elle consiste dans un premier temps à définir deux sous-ensembles distincts. Dans le premier sous-ensemble, les pixels vont être éclaircis d'une certaine valeur, puis dans l'autre sous-ensemble, ils vont être assombris.

Quand l'image n'est pas marquée, la différence de luminosité entre deux blocs (A et B) choisis pseudoaléatoirement est, dans la majorité des cas, proche de zéro. Pour « a » la luminosité du bloc « A », « b » la luminosité du bloc « B » et « S » la différence de luminosité on obtient : $S = a - b \approx 0$.

Quand l'image est marquée, la différence de luminosité entre les deux blocs est proche de : valeur d'éclaircissement + valeur d'assombrissement. Dans le cas où nous avons éclairci et assombri les blocs par la même valeur « q », on obtient : $S = a - b = 2 * q$.

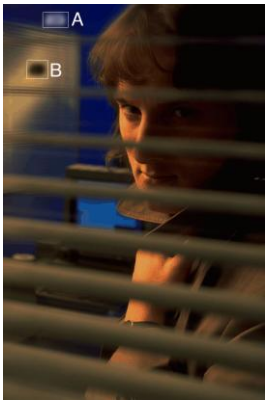


Figure 18 : Patchwork exagéré[16]

5.2.5 Watermarking fractal

Le watermarking fractal va utiliser le principe de la compression fractale, qui consiste à créer des fonctions itérées (IFS) basées sur l'autosimilarité. C'est-à-dire, des blocs de l'image (blocs de destination) vont être définis par d'autres blocs (blocs sources), généralement plus grands, leurs ressemblant.

Le watermarking fractal consiste à ajouter une similarité dans l'image afin de pouvoir contrôler le code fractal. Pour cela, il faut sélectionner des blocs sources qui ne sont

15 W. Bender, D. Gruhl, N. Morimoto ,A. Lu « Techniques for data Hiding »

16 W. Bender, D. Gruhl, N. Morimoto ,A. Lu « Techniques for data Hiding »

pas similaires les uns des autres. Puis, il faut sélectionner et modifier les blocs de destination qui se rapprochent le plus de :

$$\hat{R} = R_{hp} + \delta * S * \frac{D_{lp}}{max(D_{lp})}$$

Figure 19 : Calcul de bloc de destination[17]

Où, « R » indique le bloc de destination, « D » signifie le bloc source, « hp » signifie les hautes fréquences, « lp » les basses fréquences, « δ » est égal à : -1 si le bit à insérer est 0 et 1 dans le cas contraire, « S » l'intensité de la signature.

Pour retrouver la marque, il faut connaître l'emplacement des blocs sources et des blocs de destinations.

5.2.6 Algorithme de Koch et Zhao (et Burgett)

Cette technique de watermarking consiste à cacher la marque dans les fréquences moyennes de l'image. La technique est calquée sur une partie du schéma de la compression JPEG. Pour cela, l'algorithme de Koch et Zhao va diviser l'image en blocs de huit pixels par huit, puis des blocs vont être sélectionnés pseudoaléatoirement. Chaque bloc choisi subit une conversion DCT. Dans chaque bloc, une paire de nombres se trouvant dans les moyennes fréquences est choisie, puis, si besoin il y a, leur valeur est modifiée afin que leur différence « plus grand que » ou « plus petit que » indique l'information devant être cachée. Exemple : A > B = 0 ; A < B = 1.

17 Patrick Bas, Jean-Marc Chassery, Franck Davoine « Tatouage d'images par modification du code fractal »

5.3 Analyse multicritères

5.3.1 Introduction

Afin de sélectionner quelques logiciels, sur lesquels seront effectués des tests de robustesse, une analyse multicritères sera appliquée sur les logiciels trouvés sur Internet, dans le but de savoir quels programmes sont le plus susceptibles d'être utilisés.

5.3.2 Critères obligatoires

Les critères auxquels devront répondre les logiciels pour l'analyse multicritères sont dits « obligatoires » :

- Le logiciel est gratuit ou propose une version démonstrative.
- Le logiciel permet de marquer une image au format « jpeg » ou « bmp » en y insérant soit du texte soit une autre image.

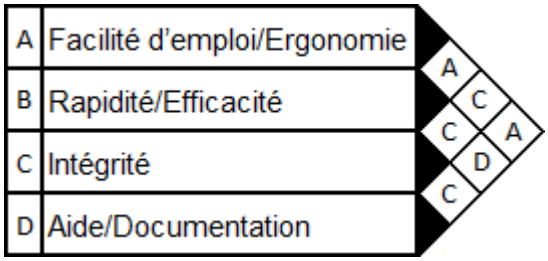
5.3.3 Critères facultatifs

La liste des critères facultatifs est faite à partir d'un « brainstorming ».

- Facilité d'emploi/Ergonomie : Le logiciel est facile à utiliser (utilisation intuitive).
- Rapidité/Efficacité : le logiciel ne consomme que les ressources nécessaires.
- Intégrité : Le logiciel est protégé des erreurs de manipulation.
- Aide/Documentation : Le logiciel propose une aide, une marche à suivre pour son utilisation.

5.3.4 Matrice de préférence

La matrice de préférence permet de comparer les critères facultatifs entre eux afin de faire ressortir leur importance, s'il en ressort qu'un critère n'a pas d'importance, il pourra ne pas être pris en compte pour la suite. Avec l'aide de cette matrice, nous pourrons créer une pondération.



5.3.4.1 Pondération

Suite à la matrice de préférence, il en ressort la pondération suivante :

- Facilité d'emploi/Ergonomie : 2/6 = 33.33%
- Rapidité/Efficacité : 0/6 = 0%
- Intégrité : 3/6 = 50%
- Aide/Documentation : 1/6 = 16.67%

5.3.5 Logiciels testés

Ne trouvant pas beaucoup de logiciels axés sur le watermarking invisible, certains logiciels testés ici sont plutôt conçus pour faire de la stéganographie.

- Icemark 1.4
- Cameleon 1.0
- Invisible secret 4
- Eikonamark 4.8
- Hide Secret Passwords in Picture Encryptor
- StegoMagic 1.0
- Jpeg Hides (JPHS)
- TextInPicture 2.0
- Digimarc (Plugin dans Photoshop)

5.3.6 Résultat des tests

Trois personnes, dont moi, ont testé les logiciels et ont noté chaque critère facultatif. Ce qui a permis de créer le tableau des points.

5.3.6.1 Tableau des points

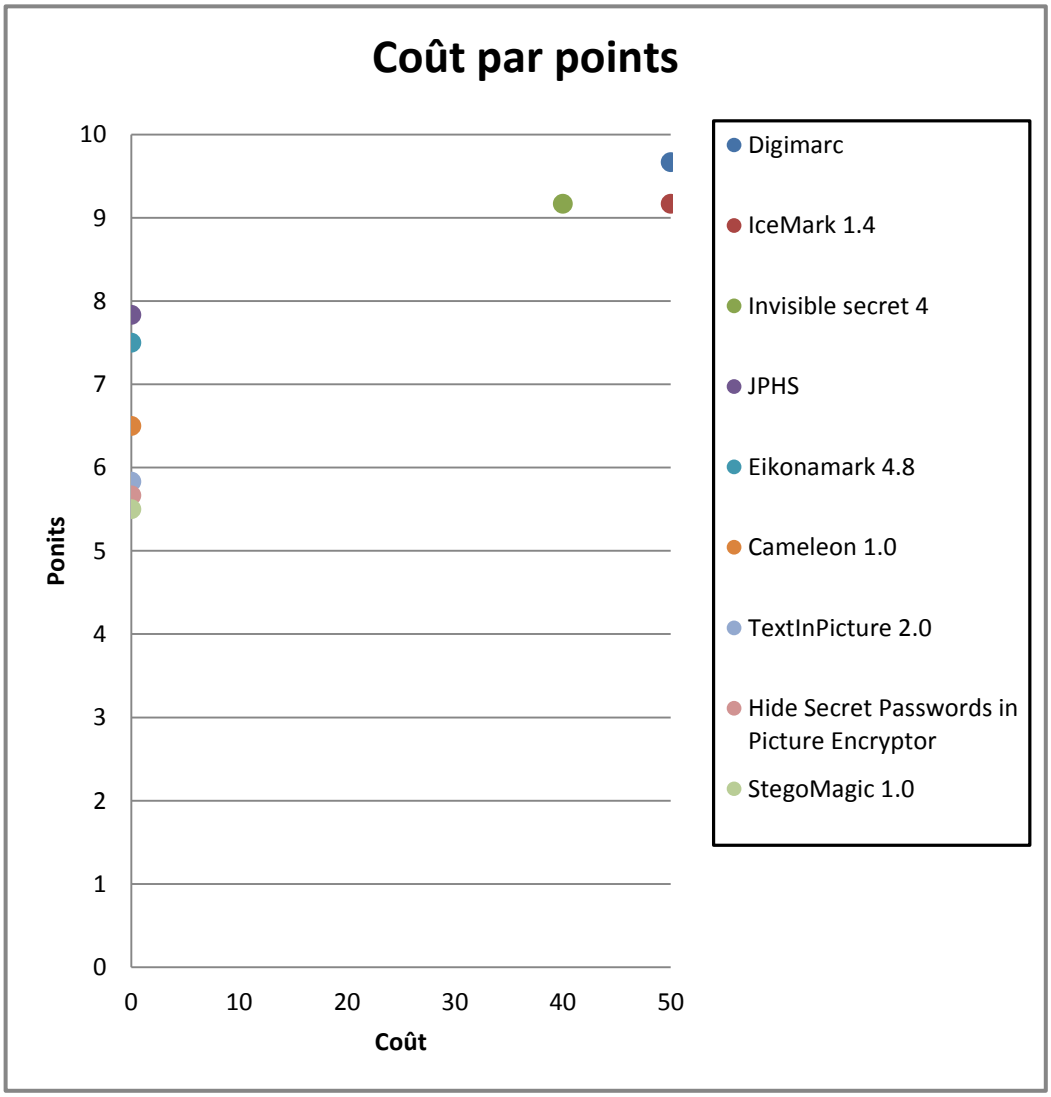
Critères facultatifs	Pondération	Digimarc			IceMark 1.4			Invisible secret 4			JPHS		
		Version d'essai	Gratuit		Version d'essai	Gratuit		Version d'essai	Gratuit		Version d'essai	Gratuit	
		✔			✔			✔				✔	
		Points obtenus		Note	Points obtenus		Note	Points obtenus		Note	Points obtenus		Note
Intégrité	50%			0	9		4.5	9		4.5	9		4.5
Facilité d'emploi/Ergonomie	33.33%			0	9		3	9		3	8		3
Aide/Documentation	16.67%			0.00	10		1.67	10		1.67	7		1.17
				0.0			9.2			9.2			8.3

Critères	Pondération	Eikonamark 4.8			Cameleon 1.0			TextInPicture 2.0			Hide Secret Passwords in Picture Encryptor		
		Version d'essai	Gratuit		Version d'essai	Gratuit		Version d'essai	Gratuit		Version d'essai	Gratuit	
			✔			✔			✔			✔	
		Points obtenus		Note	Points obtenus		Note	Points obtenus		Note	Points obtenus		Note
Intégrité	50%	9		4.5	5		2.5	5		2.5	5		2.5
Facilité d'emploi/Ergonomie	33.33%	9		3	7		2	6		2	6		2
Aide/Documentation	16.67%	0		0.00	10		1.67	8		1.33	7		1.17
				7.5			6.5			5.8			5.7

Critères	Pondération	StegoMagic 1.0		
		Version d'essai	Gratuit	
			✔	
		Points obtenus		Note
Intégrité	50%	4		2
Facilité d'emploi/Ergonomie	33.33%	7		2
Aide/Documentation	16.67%	7		1.17
				5.5

5.3.6.2 Coût par points

Avec le tableau des coûts par points, nous remarquons que les trois logiciels payants finissent en tête du classement. Ces résultats ne sont pas étonnants.



5.4 Pratique

5.4.1 Manuelle

5.4.1.1 Introduction

Il est possible d'insérer manuellement un filigrane invisible sur une image, pour cela il va falloir jouer sur la teinte et la saturation des couleurs. À première vue, l'ajout manuel semble être une mauvaise idée puisque la détection d'une telle marque ne peut pas être effectuée automatiquement (à l'inverse d'une insertion automatique), mais il existe aujourd'hui des « moteurs de recherche d'images »[18] qui, à partir d'une image, vont rechercher sur Internet les images correspondantes. Ainsi, il est possible de retrouver vos photos publiées sur Internet (même si celles-ci ne sont pas marquées).

5.4.1.2 Watermarking manuel avec Photoshop

Il est possible d'insérer, dans une image, un texte qui sera camouflé (comme un caméléon), mais qui deviendra visible au moyen d'un certain procédé, par exemple : en réglant les paramètres de teinte, saturation et luminosité.

Une première technique consiste à ajouter du texte sur l'image, puis à choisir le mode de fusion « Couleur » pour fusionner le texte à l'image. Après cela il faut trouver une zone dans l'image qui camouflera le texte. (Pour des raisons de visionnement au format papier de ce document, un cadre rouge est ajouté autour du texte)

Figure 20 : Photo originale

Figure 21 : Ajout d'un texte sur photo

18 Moteurs de recherche d'images : « TinEye », « Gazopa »

Figure 22 : Texte mode de fusion couleur

Figure 23 : Texte emplacement camouflé

Si un zoom est effectué sur l'image finale à la zone d'insertion du texte, aucun texte, aucune modification de pixels n'est perceptible.

Figure 24 : Zoom photo originale

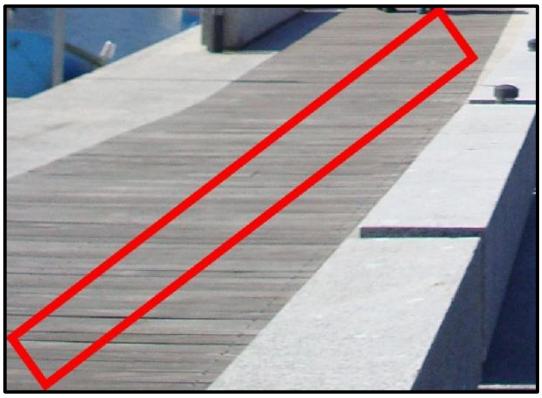


Figure 25 : Zoom photo modifiée

Pour retrouver le texte caché, il faut modifier les valeurs de saturation, teinte et luminosité.

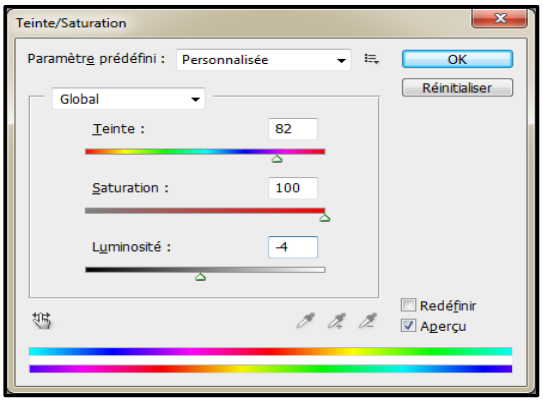


Figure 26 : Réglages de teinte et saturation

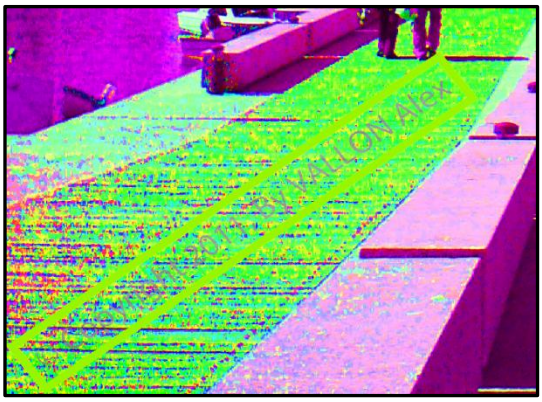


Figure 27 : Découverte du texte camouflé

L'avantage de cette technique est que la marque est vraiment invisible et ne dégrade pas l'image.

L'inconvénient de cette technique est qu'il faut placer le texte à la main (ce qui demande du temps) et selon la zone de fusion le texte peut être plus ou moins :

- visible.
- difficilement lisible après variation de la saturation.

Il faut trouver la zone la plus favorable à l'ajout du texte.

Exemple de mauvaise zone d'insertion (le texte est visible) :

Figure 28 : Texte emplacement visible

Une seconde technique du même genre est proposée par « Anti-Ripper Watermarking System by CypherXero » ; il propose une insertion automatique qui consiste à fusionner deux motifs (répétés à la taille de l'image) qu'il a créés (un échiquier et du texte) sur l'image au moyen d'une fusion par « différence ». Pour ce faire, il a créé deux motifs et deux actions Photoshop (« Encode » et « Decode ») ; les actions Photoshop fonctionnent comme des macros. En enclenchant l'action « Encode », l'image sera fusionnée avec ces deux motifs :

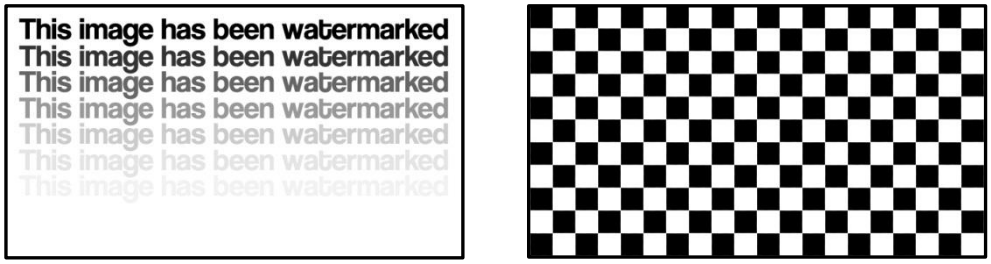


Figure 29 : Motifs utilisés pour le watermarking

La qualité de l'image est nettement dégradée, le quadrillage et le texte sont visibles lors d'un zoom.

Le **mode de fusion** défini dans la barre d'options détermine l'incidence d'un outil de peinture ou de retouche sur les pixels de l'image. Lorsque vous examinez l'effet d'un mode de fusion, pensez en termes de couleurs : • La couleur de base est la couleur d'origine de l'image. • La couleur de fusion est la couleur appliquée à l'aide de l'outil de peinture ou de retouche. • La couleur finale est la couleur résultant de la fusion.

Tableau 3 : Le mode de fusion[19]

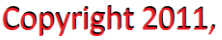
Couleur : Crée une couleur finale ayant la luminance de la couleur de base et la teinte et la saturation de la couleur de fusion. Ce mode préserve les niveaux de gris de l'image et est pratique pour colorer des images monochromes ou pour teinter des images en couleurs. **Différence** : Analyse les informations chromatiques de chaque couche et soustrait la couleur de base de la couleur de fusion, ou inversement, en fonction de la couleur la plus lumineuse. La fusion avec du blanc inverse les valeurs de la couleur de base ; la fusion avec du noir ne produit aucun effet.

Tableau 4 : Mode de fusion « couleur » et « différence »[20]

5.4.2 Automatique

5.4.2.1 Introduction

Certains programmes de watermarking proposent d'insérer du texte ou un ID dans l'image souhaitée, d'autre proposent d'y insérer une image. À première vue l'insertion d'un numéro d'identifiant n'a pas grand intérêt, sauf si celui-ci est utilisé comme lien vers un compte client ; comme le fait le plug-in de Digimarc.

Dans la phase de test, le texte « © Copyright 2011, By VALLON Alex » sera inséré en tant que marque ou l'image «  ».

5.4.2.2 Jpeg Hides (JPHS)

« JPHS for Windows - Freeware version BETA test rev 0.5 » est un programme gratuit créé par Allan LATHAN en 1999, il offre la possibilité de cacher un fichier dans une image au format JPG. C'est un logiciel de stéganographie.

---

19 http://help.adobe.com/fr_FR/Photoshop/11.0/WSfd1234e1c4b69f30ea53e41001031ab64-77eaa.html

20 http://help.adobe.com/fr_FR/Photoshop/11.0/WSfd1234e1c4b69f30ea53e41001031ab64-77e9a.html

5.4.2.3 NeoByte Solution : Invisible secret 4, version 4.7.0

Invisible secret est un logiciel de cryptographie et stéganographie, il propose notamment de cacher une image dans une autre image.

La licence du logiciel coûte environ 40$ (36CHF) pour le privé et pour les entreprises un pack de cinq licences coûte 150$ (134CHF). La version d'essai est limitée dans le temps, mais les modes de décryptage restent utilisables.

5.4.2.4 Icemark 1.4

Icemark est un logiciel permettant d'insérer une marque dans les images. Cette marque peut être du texte, des informations sur l'image (identifiant, usage restreint, ne pas copier, contenu adulte) ou une marque quelconque qui permet à Icemark de détecter si l'image est marquée.

La licence du logiciel coûte environ 50$ (48CHF) pour le privé et 950$ (910CHF) pour les entreprises. La version d'essai n'est pas limitée dans le temps, mais va imposer son filigrane sur les photos marquées.

5.4.2.5 Digimarc

Digimarc est un concepteur de technologies permettant l'identification de toutes formes de contenu, audio, vidéo, images et même certains objets.

Digimarc est un plug-in installé dans Photoshop. Sans abonnement à Digimarc, il est possible de marquer ses photos ; une marque invisible liée à un compte démonstratif est alors ajoutée à l'image. Trois différents types d'abonnement existent :

- Basic (50$ par an et 1000 images) : permet d'insérer une marque contenant des informations sur les droits d'utilisation et un lien dirigé sur un compte Digimarc ou dirigé sur une URL.
- Professionnal (100$ par an et 2000 images) : en plus de la possibilité de marquer le double d'images, un service de recherche est ajouté ; il va scanner des milliards d'images sur Internet et vous fournir un rapport sur vos images trouvées.
- Small Business (500$ par an et 5000 images) : il contient deux services de plus que l'abonnement « professionnal » :
    - La possibilité de diriger les recherches de Digimarc sur des sites spécifiques.
    - Une assistance téléphonique.

Figure 30 : Cycle de gestion de photos par Digimarc

5.5 Test de robustesse

Les tests de robustesse ont été réalisés afin de prendre connaissance de l'efficacité des logiciels et afin de savoir quelles transformations sont susceptibles d'effacer la marque.

	Jpeg Hides
Transformation	**JPG**
Rotation 90°/180°	✗
Conversion de format	✗
Ajout d'effets	✗
Contraste auto	✗
Ajout d'un cadre	✗
Publication sur Flickr	✗
Publication sur Facebook	✗

« Jpeg Hides » étant un logiciel de stéganographie, il n'est pas étonnant que la marque insérée dans le fichier ne soit pas résistante. En stéganographie, le support n'est pas censé subir des modifications ; il est supposé être transmis tel quel.

	Invisible secret 4	
Transformation	**JPG**	**BMP**
Rotation 90°/180°	✗	✗
Conversion de format	✗	✗
Ajout d'effets	✗	✗
Contraste auto	✗	✗
Ajout d'un cadre	✗	✗
Publication sur Flickr	Impossible, erreur dans le fichier	Trop grand (30Mo)
Publication sur Facebook	✗	Format pas accepté

Les résultats du logiciel « Invisible secret 4 » ne sont pas surprenants sachant que c'est un programme de stéganographie.

	Icemark 1.4			
	texte		ID	
Transformation	**JPG**	**BMP**	**JPG**	**BMP**
Rotation 90°/180°	✗	✗	✗	✗
Conversion de format	✓	✓	✓	✓
Ajout d'effets	✓	✓	✓	✓
Contraste auto	✓	✓	✓	✓
Ajout d'un cadre	✗	✗	✗	✗
Publication sur Flickr	✗	Trop grand (30Mo)	✗	Trop grand (30Mo)
Publication sur Facebook	✗	Format pas accepté	✗	Format pas accepté

Nous remarquons dans le tableau ci-dessus que les images marquées avec « Icemark » ne résistent pas aux déformations géométriques. On aurait pu penser que cacher un « simple » numéro d'identification permettrait une meilleure résistance de la marque, mais ce n'est pas le cas ici.

	Plug-in Digimarc dans Photoshop	
Transformation	**JPG**	**BMP**
Rotation 90°/180°	✓	✓
Conversion de format	✓	✓
Ajout d'effets	✓	✓
Contraste auto	✓	✓
Ajout d'un cadre	✓	✓
Publication sur Flickr	✓	Trop grand (30Mo)
Publication sur Facebook	Seulement la photo sans traitement	Format pas accepté
Imprimer/scanner	✓	✓

Les résultats obtenus avec « Digimarc » sont tout simplement surprenants. La marque résiste à la plupart des modifications possibles et même en imprimant l'image, la marque reste incrustée.

5.6 Mise en œuvre

5.6.1 Introduction

Marquer ses photos dans le but de les protéger c'est bien, pouvoir les retrouver en cas d'utilisation abusive c'est mieux. Pour cela, il existe plusieurs stratégies.

5.6.2 Stratégies

Il existe plusieurs manières de retrouver vos photos diffusées abusivement sur Internet. Premièrement, vous pouvez tomber dessus par hasard ; il y a peu de chance que cela se produise, sauf si vous êtes passionné par un sujet, que vos photos apparaissent en première page lors de recherche Google et que vous consultez régulièrement tous les articles publiés sur Internet concernant le sujet. Deuxièmement, vous pouvez vous aider d'un moteur de recherche d'image inverse ; il est possible de s'aider d'un moteur de recherche d'image inverse pour retrouver ses photos, « TinEye » est vraiment performant, de plus, il existe un plug-in Firefox permettant d'ajouter « Search Image on TinEye » dans les options du clic droit. Enfin, vous pouvez laisser quelqu'un d'autre chercher vos photos pour vous ; par exemple, Digimarc propose plusieurs services après marquage de vos photos tel que l'envoi d'un rapport mensuel sur les images publiées sur Internet contenant la marque liée à votre compte.

5.6.3 Solutions proposées

5.6.3.1 Photographes professionnels ou entreprises

Pourquoi un client achèterait-il une image, si, après diffusion, celle-ci était gratuite pour tout le monde ?

Pour une entreprise dont le commerce tourne essentiellement autour de la photo ou de la création d'images, investir dans une solution de watermarking n'est pas une perte économique. Le watermarking ajoute une plus-value à l'image ; grâce à lui, il est possible de garantir aux clients que des moyens efficaces sont mis en œuvre pour empêcher l'utilisation abusive des photos vendues.

5.6.3.2 Photographes amateurs

Exposer ses œuvres, c'est toujours s'exposer à la copie, aux vols. Généralement quand on fait de la « création d'images » (photographie/dessin), c'est dans le but de les montrer, mais cela ne veut pas dire pour autant qu'on veuille en céder les droits d'utilisation.

Pour ceux qui ne veulent pas ou qui ne peuvent pas investir 50-100$ par an pour un système de watermarking, il reste plusieurs possibilités pour essayer de se protéger des vols de photos/images/dessins.

Premièrement, vous pouvez imposer un filigrane visible aux endroits clefs de vos images. Cela peut dissuader la plupart des gens à « prendre » vos images, mais cela gênera les visiteurs qui veulent juste admirer vos œuvres. Deuxièmement, à l'endroit de vos publications mentionnez que les droits de vos photos sont régis par la propriété intellectuelle et qu'il est illégal de rediffuser vos œuvres sans votre accord.

Une fois vos œuvres publiées, si vous avez le temps, utilisez un moteur de recherche d'images inverse (« TinEye » par exemple) pour retrouver vos images « empruntées » et avertissez par e-mail, le propriétaire et l'hébergeur du site que la diffusion de vos œuvres n'a pas été autorisée.

Conclusion

Pour conclure ce mémoire, je dirais que, comme pour un bien matériel, il n'existe aucun moyen efficace à cent pour cent qui puisse empêcher le vol d'un fichier numérique. Tout comme dans le cas d'un vol de bien matériel, il est conseillé de contrôler les points de revente, dans le cas d'un vol de fichier numérique, il est conseillé de contrôler les images diffusées sur d'autres sites web. Ces contrôles peuvent être réalisés à l'aide d'outils par soi-même ou par une entité tierce.

J'ajouterais, qu'il existe aujourd'hui des solutions payantes suffisamment efficaces pour réaliser du watermarking. Ces solutions ajoutent une plus-value aux images. Les solutions libres trouvées sur Internet semblent être plus des travaux de recherche que des logiciels élaborés dans le but d'une utilisation concrète. De plus, je ne pense pas qu'il puisse exister un logiciel « open source » efficace de watermarking, puisque si la méthode de marquage est connue, il devient plus facile d'enlever la marque ou de la modifier.

Il subsiste un autre problème qui est la connaissance sur le droit d'auteur ; bon nombre de visiteurs ne savent pas quels sont les droits sur les images qu'ils trouvent dans les sites web et par conséquent commettent parfois involontairement des actes illégaux.

Pour chacune des techniques de watermarking présentée, il existe différentes versions de mise en œuvre, ce qui m'a compliqué la tâche dans mes recherches et ce qui m'a poussé naturellement à analyser les versions de base (non améliorées). De plus, je ne m'attendais pas à rencontrer des formules mathématiques aussi complexes.

Avant le début de ce mémoire, j'avais entendu dire qu'un bon journaliste cherche toujours trois sources avant de valider une information ; le watermarking étant un domaine complexe et un nouveau domaine pour ma part, j'ai entamé ce mémoire dans cet état d'esprit. Pour chaque information trouvée, j'ai essayé de vérifier sur d'autres sites web si l'information était correcte ; j'ai ainsi pu constater que certains sites web ou documents contenaient des erreurs.

Ce travail m'a permis de constater que pour certains projets informatiques, il ne suffit pas d'avoir de bonnes connaissances en informatique, il faut aussi acquérir des connaissances dans un domaine auxiliaire. Je pense donc, qu'il est judicieux de se spécialiser dans un domaine complémentaire ou bien de se faire accompagner d'un expert ou d'une personne expérimentée.

Bibliographie

Informations globales

ARNOLD, Michael, SCHMUCKER, Martin, WOLTHUSEN, Stephen D. *Techniques and applications of digital watermarking and content protection*. 1er éd. Boston [etc.] : Artech House, 2003. 274 p. (Computer security series)

Tatouage numérique. In : *Wikipedia, the free encyclopedia* [en ligne]. http://fr.wikipedia.org/wiki/Tatouage_numérique (consulté le 02.03.2011)

Digital watermarking. In : *Wikipedia, the free encyclopedia* [en ligne]. http://en.wikipedia.org/wiki/Digital_watermarking (consulté le 02.03.2011)

Format Windows bitmap

COMMENTÇAMARCHE.NET. *Le format BMP* [en ligne]. http://www.commentcamarche.net/contents/video/format-bmp.php3 (consulté le 07.03.2011)

Windows bitmap. In : *Wikipedia, the free encyclopedia* [en ligne]. http://fr.wikipedia.org/wiki/Windows_bitmap (consulté le 07.03.2011)

KADDOUR, Chakib. Le format BMP [en ligne]. http://www.kaddour.com/annexeb/annexeb.htm (consulté le 08.03.2011)

Format JPEG

JPEG. In : *Wikipedia, the free encyclopedia* [en ligne]. http://fr.wikipedia.org/wiki/JPEG (consulté le 09.03.2011)

JPEG. In : *Wikipedia, the free encyclopedia* [en ligne]. http://en.wikipedia.org/wiki/JPEG (consulté le 09.03.2011)

MORLON, Jérôme. *Les techniques de compression: l'image JPEG* [en ligne]. http://www.journaldunet.com/developpeur/tutoriel/gra/010820gra_compression.shtml (consulté le 10.03.2011)

MAÎTRE, Henri. *La compression JPEG* [en ligne]. http://perso.telecom-paristech.fr/~maitre/BETI/test_JPEG/jpeg.html#modes JPEG (consulté le 11.03.2011)

Joint Photographic Experts Group. *La compression JPEG* [en ligne]. http://195.83.128.55/~src8b02/multimedia/sitenum/technique.html (consulté le 11.03.2011)

COURTELLEMONT, Pierre. *JPEG et la compression des images fixes* [en ligne]. http://perso.univ-lr.fr/pcourtel/espadon/site_web/Ch3/page3-4.htm (consulté le 11.03.2011)

AZÉ, Jérôme. *La norme JPEG* [en ligne]. http://www.lri.fr/~aze/enseignements/ifips/S3/docs/jpeg-crypto.pdf (consulté le 12.03.2011)

FLIEDEL, Romain. *La compression JPEG*. 2005. 08 p. T.I.P.E : http://r0ro.free.fr/tipe/docs/TIPE.pdf

Technique du "Patchwork"

BENDER, Walter et al. Techniques for data hiding. *IBM Systems Journal* [en ligne]. 1996, VOL 35, NOS 3&4, p. 313. http://cs.utsa.edu/~jortiz/CS4953/Papers/Techniques%20for%20Data%20Hiding-p.pdf (23.03.2011)

Watermarking par étalement de spectre

COX, Ingemar J et al. Secure Spread Spectrum Watermarking for Multimedia. *IEEE TRANSACTIONS ON IMAGE PROCESSING* [en ligne]. 1997, VOL 06, NO 12, p. 1673. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.118.9444&rep=rep1&type=pdf (11.04.2011)

Watermarking par compression fractal

BAS, Patrick, CHASSERY, Jean-Marc, DAVOINE, Franck. *TATOUAGE D'IMAGES PAR MODIFICATION DU CODE FRACTAL* [en ligne]. 1998. http://www.gipsa-lab.fr/~patrick.bas/mes_publis/bascoresa98.pdf (20.04.2011)

Logiciels

Icemark 1.4 : http://www.phibit.com/
Cameleon 1.0 : http://www.commentcamarche.net/download/telecharger-34055068-cameleon
Invisible secret 4 : http://www.invisiblesecrets.com/
Eikonamark : http://www.alphatecltd.com/watermarking/eikonamark/eikonamark.html
StegoMagic 1.0 : http://www.programmersheaven.com/download/38361/download.aspx
TextInPicture 2.0 : http://nacsoft.pagesperso-orange.fr/
Digimarc : http://www.digimarc.com/
Jpeg Hides (JPHS) : http://www.infosyssec.com/infosyssec/Steganography/programs.htm

Hide Secret Passwords in Picture Encryptor : http://www.clickok.org/steg/

Analyse multicritères

De BANOFF, Alexandre. Cours HEG module 655 : *Management*, année 2009-2010

BURDET, Xavier. Cours HEG module 6571 : *Assurance qualité : Facteur de la qualité du logiciel*, année 2009-2010

Autres

GIRARD, Cédric. *Photos volées : comment les retrouver avec TinEye* [en ligne]. 2008. http://blog.aube-nature.com/tineye-moteur-recherche-images-photos-volees/ (15.04.2011)

SCHIRBER, Michael. New Invisible Watermark to Prevent Fake Photos. *LiveScience* [en ligne]. 2005. http://www.livescience.com/3869-invisible-watermark-prevent-fake-photos.html (06.04.2011)

EXO MAKINA. *Photo-Interprétation avancée* [en ligne]. 2011. http://www.exomakina.fr/eXo_maKina/Tungstene.html (08.04.2011)

ADOBE PHOTOSHOP. *À propos des modes de fusion* [en ligne]. http://www.exomakina.fr/eXo_maKina/Tungstene.html (11.04.2011)

ADOBE PHOTOSHOP. *Liste des modes de fusion* [en ligne]. http://www.exomakina.fr/eXo_maKina/Tungstene.html (11.04.2011)

Annexe 1
Loi fédérale sur le droit d'auteur et les droits voisins [Extrait]

Source : http://www.admin.ch/ch/f/rs/c231_1.html

Titre 2 Droit d'auteur

Chapitre 1 L'œuvre

Art. 2 Définition

1 : Par œuvre, quelles qu'en soient la valeur ou la destination, on entend toute création de l'esprit, littéraire ou artistique, qui a un caractère individuel.

2g : Sont notamment des créations de l'esprit: les œuvres photographiques, cinématographiques et les autres œuvres visuelles ou audiovisuelles;

Chapitre 3 Étendue du droit d'auteur

Section 1 Relation entre l'auteur et son œuvre

Art. 9 Reconnaissance de la qualité d'auteur

1 : L'auteur a le droit exclusif sur son œuvre et le droit de faire reconnaître sa qualité d'auteur.

2 : Il a le droit exclusif de décider si, quand, de quelle manière et sous quel nom son œuvre sera divulguée.

Chapitre 5 Restrictions au droit d'auteur

Art. 19 Utilisation de l'œuvre à des fins privées

1 : L'usage privé d'une œuvre divulguée est autorisé. Par usage privé, on entend :

a) toute utilisation à des fins personnelles ou dans un cercle de personnes étroitement liées, tels des parents ou des amis;
b) toute utilisation d'œuvres par un maître et ses élèves à des fins pédagogiques;
c) la reproduction d'exemplaires d'œuvres au sein des entreprises, administrations publiques, institutions, commissions et organismes analogues, à des fins d'information interne ou de documentation.

3 : Ne sont pas autorisés en dehors du cercle de personnes étroitement liées au sens de l'al. 1, let. a :

a) la reproduction de la totalité ou de l'essentiel des exemplaires d'œuvres disponibles sur le marché;
b) la reproduction d'œuvres des beaux-arts;
c) la reproduction de partitions d'œuvres musicales;

d) l'enregistrement des interprétations, représentations ou exécutions d'une œuvre sur des phonogrammes, vidéogrammes ou autres supports de données.

4 : Le présent article ne s'applique pas aux logiciels.

Art. 20 Rémunération pour l'usage privé

1 : L'utilisation de l'œuvre à des fins personnelles au sens de l'art. 19, al. 1, let. a, ne donne pas droit à rémunération, sous réserve de l'al. 3.

Art. 62 Action en exécution d'une prestation

1 : La personne qui subit ou risque de subir une violation de son droit d'auteur ou d'un droit voisin peut demander au juge :

a) de l'interdire, si elle est imminente;
b) de la faire cesser, si elle dure encore;

Titre 5 Voies de droit

Chapitre 2 Dispositions pénales

Art. 67 Violation du droit d'auteur

1 : Sur plainte du lésé, est puni d'une peine privative de liberté d'un an au plus ou d'une peine pécuniaire quiconque, intentionnellement et sans droit:

a) utilise une œuvre sous une désignation fausse ou différente de celle décidée par l'auteur;
b) divulgue une œuvre;
c) modifie une œuvre;
d) utilise une œuvre pour créer une œuvre dérivée;
e) confectionne des exemplaires d'une œuvre par n'importe quel procédé;
f) propose au public, aliène ou, de quelque autre manière, met en circulation des exemplaires d'une œuvre;
g) récite, représente ou exécute une œuvre, directement ou par n'importe quel procédé ou la fait voir ou entendre en un lieu autre que celui où elle est présentée;
gbis) met une œuvre à disposition, par quelque moyen que ce soit, de manière que toute personne puisse y avoir accès d'un endroit et à un moment qu'elle peut choisir à sa convenance;
h) diffuse une œuvre par la radio, la télévision ou des moyens analogues, soit par voie hertzienne, soit par câble ou autres conducteurs ou la retransmet par des moyens techniques dont l'exploitation ne relève pas de l'organisme diffuseur d'origine;
i) fait voir ou entendre une œuvre mise à disposition, diffusée ou retransmise;
j) -
k) refuse de déclarer à l'autorité compétente la provenance et la quantité des objets en sa possession fabriqués ou mis en circulation illicitement et de désigner les destinataires et la quantité des objets qui ont été remis à des acheteurs commerciaux;
l) Loue un logiciel.

2 : Si l’auteur d’une infraction au sens de l’al. 1 agit par métier, il est poursuivi d’office. La peine est une peine privative de liberté de cinq ans au plus ou une peine pécuniaire. En cas de peine privative de liberté, une peine pécuniaire est également prononcée.

Annexe 2
Le Code QR

Source : http://fr.wikipedia.org/wiki/Code_QR (18.04.2011)

Le **code QR** (ou ***QR code*** en anglais) est un code-barres en deux dimensions (ou code à matrice) constitué de modules noirs disposés dans un carré à fond blanc. Le nom *QR* est l'acronyme de l'anglais *Quick Response*, car son contenu de données peut être décodé rapidement.

Destiné à être lu par un lecteur de code QR, un téléphone mobile, ou un smartphone, il a l'avantage de pouvoir stocker plus d'informations qu'un code à barres.

Un exemple de code QR

Histoire

Le code QR a été créé par l'entreprise japonaise Denso-Wave en 1994 pour le suivi des pièces de voiture dans les usines de Toyota.

En 1999, Denso-Wave a publié le code QR sous licence libre; cela a contribué à la diffusion du code au Japon. Ensuite, à la fin des années 2000, il est devenu l'un des codes bidimensionnels les plus populaires dans le monde, et les applications de lecture de codes QR sont souvent déjà installées par les fabricants dans les téléphones mobiles. Au Japon, cette pratique était déjà répandue en 2003.

En septembre 2005 a été lancé le projet Semapedia pour lier, via code QR, les lieux physiques aux pages relatives sur Wikipédia.

Normes et licences

En 1999, tout en conservant les droits du brevet, Denso-Wave a accordé l'utilisation du code QR avec une licence libre, défini et publié en tant que norme ISO.

- En octobre 1997 a été publié le standard AIM (Association for Automatic Identification and Mobility), renouvelé en 1999.
- En 1999 a été publié le standard japonais JIS X 0510.
- En juin 2000 a été publiée la norme ISO/IEC 18004.
- En novembre 2004, le *Micro QR code* a été approuvé par la norme JIS X 0510:2004.
- Le 1er septembre 2006, la norme ISO/IEC 18004:2006 a été renouvelée.

Du côté applicatif, il y a des variations entre les mises en œuvre. NTT DoCoMo a instauré de facto la norme pour l'encodage des URL, des informations de contact et

d'autres types de données. Le projet open source Zxing publie un guide des normes de codage de l'information dans les codes-barres.

Fonctionnement

Les codes QR peuvent mémoriser des adresses web, du texte, des numéros de téléphone, des SMS ou autres types de données lisibles par les smartphones et les téléphones mobiles équipés d'une application de lecture (lecteur de code QR ou *QR reader* en anglais).

L'avantage du code QR est sa facilité et rapidité d'utilisation et de création. Pour lire un code QR, il suffit de lancer l'application de lecture et viser le code dans le mobile. De nombreuses pages Web offrent ces applications pour mobiles, généralement sans frais. Le site de Semapedia contient une liste de lecteurs spécifiques pour chaque modèle de téléphone.

En ce qui concerne l'écriture, il y a plusieurs sites web qui permettent de générer librement les codes QR.

Spécification

Les codes QR peuvent stocker jusqu'à 7 089 caractères numériques, 4 296 caractères alphanumériques, bien au-delà de la capacité du code-barres (de 10 à 13 caractères).

Capacité de stockage de données

- Caractères numériques: max 7 089
- Caractères alphanumériques: max 4296
- Binaires (8-bits): max 2953 octets
- Kanji/Kana: max 1817 caractères

Correction d'erreur

Les codes QR utilisent le système Reed-Solomon pour la correction d'erreur: le code contient jusqu'à 30 % de redondance.

Capacité de corriger les erreurs

- Niveau L : environ 7% de redondance
- Niveau M : environ 15%
- Niveau Q : environ 25%
- Niveau H : environ 30%

Variantes

Exemple de *QR Micro*

- Le QR Micro (Micro QR code) est une version réduite du code QR normal, utilisé pour les applications qui nécessitent l'utilisation de petits espaces et une moindre quantité d'informations, comme par exemple l'ID de cartes de circuits imprimés ou des composants électroniques. Il existe différentes formes de QR Micro, la plus dense d'informations peut contenir jusqu'à 25 caractères alphanumériques.
- Grâce au système de correction d'erreur Reed-Solomon, les codes QR peuvent incorporer des images, telles que logos ou dessins, sans perdre les informations utiles à la lecture du code. Il suffit de transformer le code avec un logiciel de retouche d'image jusqu'à ce que le code continue de fonctionner.

Usage dans l'art

Fabrice de Nola, *Bottom up*, huile sur toile, 2006.

- Depuis 2006, l'artiste italien Fabrice de Nola utilise les codes QR dans des peintures à l'huile ou des photographies.
- En 2007, le groupe pop britannique Pet Shop Boys a utilisé un code QR pour télécharger le single Integral. Dans la vidéo, d'autres codes dirigent vers le site du groupe et des pages web au sujet de l'utilisation de la carte d'identité en Grande-Bretagne.
- En 2009, l'artiste japonais Takashi Murakami, en collaboration avec l'agence créative SET et Louis Vuitton, a créé un QR code avec l'image du motif LV et l'un des personnages de l'artiste.
- En 2010, le musicien hip hop américain DJ Spooky a exposé un code QR à la Biennale Experimenta de Melbourne. Le code dirige vers le site web Nauru Elégies, au sujet de l'île de Nauru au Pacifique.
- Dans la vidéo du single de Kylie Minogue, All The Lovers (2010), apparaît un code QR imprimé sur des objets. Le code n'est pas assez visible pour être lu directement à partir de la vidéo, mais un blogueur l'a reconstruit, révélant qu'il contient le mot anglais love (amour)
- En novembre 2010, le groupe français Valentine's Day a mis en place un code QR sur le verso de son album "Whatever You Want". Le code QR permettait le visionnage d'un clip unplugged du titre phare de l'album "Lady Bug.

- Le collectif Raspouteam au travers de son projet "Paris, Désordres publics, disposant des codes QR dans certaines rues de la ville de Paris et relatant les événements marquants propres à ces rues.

Usage dans l'interprétation

- Les musées et les offices du tourisme utilisent de plus en plus les QR codes pour que les possesseurs de smartphones puissent lire des informations complètes, via un lien vers une page du site web concerné, voire un lien QR vers un fichier son pour écouter le commentaire. C'est une sorte de guide, d'aide à l'accessibilité aussi: sans avoir besoin d'écrire le texte du lien Web sur le téléphone portable, on a accès à l'information.