

pratique, il ne reste pas longtemps secret. On suppose ici que chaque clé est propre à un ayant droit, clé qui permet de l'identifier. Parallèlement, on met au point un système de gestion des clés, reposant sur un « tiers de confiance ». Ce dernier est une entité sécurisée et angélique qui ne triche ni ne ment jamais : c'est elle qui va gérer les clés et opérer les vérifications. Cette opération délicate ne peut être confiée, ni à l'ayant droit présumé du document, car il pourrait mentir, ni à quelqu'un d'autre, car il faut la clé pour opérer cette vérification, et si celle-ci est révélée au grand jour, les marques qu'elle a produites deviennent très vulnérables.

Revenons aux techniques d'incrustation proprement dites. Le tatouage est engendré par des techniques de traitement du signal. Nous envisagerons ici le tatouage des images fixes (les contraintes du tatouage de la vidéo sont légèrement différentes : une image vidéo étant de moins bonne qualité, il est plus facile d'y camoufler une marque, mais, d'un autre côté, l'algorithme de tatouage doit être très rapide).

L'évolution des algorithmes de tatouage proposés depuis cinq ans est très nette : on est passé de solutions simples, naïves et peu résistantes à des techniques complexes et plus robustes. Ces dernières reposent sur la modification des coefficients de la transformée de Fourier (bidimensionnelle) de l'image (voir la figure 3). Ces approches engendrent des filigranes de bonne résistance. La détection du filigrane repose en général sur la présence ou non d'une structure particulière dans l'image ; on cache par exemple un signal présentant des propriétés de corrélation très spécifiques (voir la figure 4). La conception d'un algorithme de tatouage/vérification commence donc par le choix de la structure de modification de l'image ; ce choix est contraint par la spécificité de l'utilisation (degré d'invisibilité, robustesse, rapidité d'exécution, mémoire utilisée).

Le tatouage impose un certain nombre de compromis entre la quantité d'information cachée, l'invisibilité et la robustesse de la marque. Il faut également tenir compte, lors de la concep-

tion de l'algorithme de vérification, des risques de non-détection (l'ayant droit présumé est réellement le propriétaire du document, mais l'algorithme n'arrive pas à le prouver) et de fausse alarme (on identifie une personne comme étant l'ayant droit du document, alors que c'est faux). Il convient aussi de définir si la présence de l'image originale est nécessaire à la vérification.

Les techniques d'incrustation se répartissent en deux catégories : les « spatiales » qui modifient directement les pixels (un pixel est un élément d'image), et les « fréquentielles » qui changent les coefficients des transformées de Fourier. Les algorithmes présentés ci-après donnent un panorama des techniques employées et des concepts qui entrent en jeu. Ces algorithmes opèrent uniquement sur la luminance (intensité lumineuse par unité de surface) des pixels (voir la figure 2).

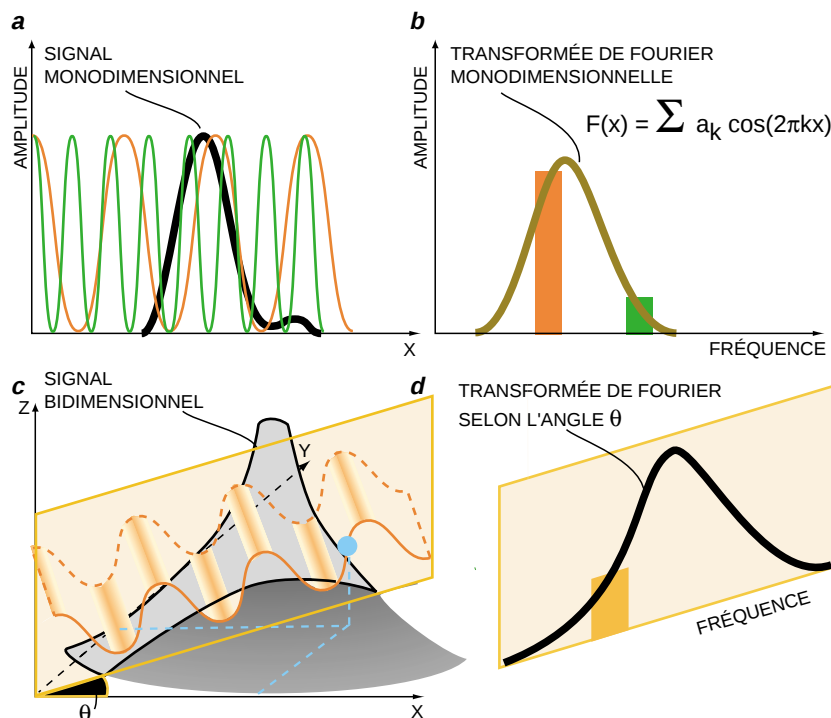
### LA PROGRESSION DES TECHNIQUES

La première technique proposée est simple : une clé secrète détermine, dans une zone de l'image, l'emplacement de pixels. La luminance de chacun d'entre eux est codée par une valeur comprise entre 0 (en binaire 00000000), et 255 (en binaire 11111111). Le bit de poids faible de l'écriture binaire, le dernier, est celui qui a le moins d'influence sur la valeur de la luminance. Statistiquement ces bits de poids faible ont une probabilité 1/2 de valoir 0, et 1/2 de valoir 1. On cache l'information en introduisant un biais dans cette proportion : pour ce faire, on impose la valeur 1 aux bits de faible poids de certains pixels, choisis selon la clé. Cette modification sera imperceptible pour l'œil car la luminance de ces pixels aura varié d'au plus 1. On vérifie alors, sur l'image modifiée, la présence ou non d'un tatouage, en analysant les bits de poids faible correspondant aux pixels associés à la clé : si ces bits sont égaux à 1, alors l'image a été tatouée avec la clé (et elle appartient à l'ayant droit associé à cette dernière) sinon, elle n'a pas été tatouée avec cette clé (et n'appartient pas à cet ayant droit).

Malheureusement, les bits de poids faible des octets sont modifiés quand on applique la moindre transformation à l'image, en particulier lors d'une compression avec JPEG.

En 1995, W. Bender et ses collègues de l'Institut de technologie du Massachusetts ont proposé un algorithme dénommé *Patchwork*, qui repose sur la différence de luminance observée entre deux ensembles de pixels. Il est fondé sur l'analyse statistique suivante : si l'on considère deux grands ensembles A et B de

### 3. LA TRANSFORMÉE DE FOURIER



La transformée de Fourier monodimensionnelle consiste à décomposer un signal ne dépendant que d'un seul paramètre en une superposition de fonctions sinusoïdales de différentes fréquences (a). À chacune de ces fréquences correspond un coefficient ( $a_k$ ) de la transformée, dont la valeur mesure la contribution de cette fonction sinusoïdale (b). De la même manière, on considère la transformée de Fourier d'un signal bidimensionnel, dépendant de deux paramètres (c). Dans une direction  $\theta$ , on décompose le signal selon des ondulations de différentes fréquences. Les contributions des différentes fréquences sont les coefficients de la transformée de Fourier dans cette direction.

pixels répartis dans une image, alors la moyenne des différences de luminance entre les pixels de A et ceux de B est très proche de 0. Dans ce tatouage, on choisit des ensembles A et B (suivant une clé secrète), puis on modifie leur luminance : on augmente celle des pixels de A d'une quantité  $c$ , et l'on diminue celle des pixels de B de la même quantité  $c$ .

Pour vérifier la provenance de l'image, on détermine les ensembles A et B à l'aide de la clé, puis on mesure la moyenne des différences de luminance des pixels. On obtient une moyenne proche de  $2c$  si l'image a été tatouée avec la clé, une moyenne proche de 0 sinon. Ce type de filigrane résiste mieux que le précédent à certaines manipulations de l'image, mais, hélas, il n'est toujours pas satisfaisant face à une compression JPEG (remarquons cependant que les modifications des propriétés statistiques d'ensembles de pixels, ou de coefficients, sont souvent utilisées et peuvent donner des filigranes résistants).

## LA COMPRESSION

Revenons sur le principe de la compression JPEG : les trois composantes de luminance et de chrominance sont traitées séparément et de la même manière. Une composante de l'image numérisée est découpée en blocs contigus de taille  $8 \times 8$ , soit 64 pixels (si l'image n'a pas une taille adéquate, elle est complétée par des octets nuls) et l'on applique une transformée de Fourier bidimensionnelle (voir la figure 3) : on obtient ainsi 64 coefficients de Fourier qui correspondent à 64 paires d'orientation et de fréquence différentes. On modifie ensuite les coefficients correspondant aux hautes fréquences, modification d'autant plus importante que l'on accepte une diminution de la résolution. On effectue ensuite la transformation de Fourier inverse pour retrouver un bloc image de  $8 \times 8$  pixels.

Les octets de luminance ont été changés et leur bit de poids faible, sensible à la moindre variation, a pris une valeur aléatoire : c'est pour cette raison que toute technique de tatouage reposant sur la valeur des bits de poids faible est mise en défaut par une compression JPEG.

Afin d'être sûrs de créer un filigrane résistant à la compression JPEG, E. Koch et J. Zhao, travaillant au *Franhofer Institute for Computer Graphics*, à Darmstadt, ont décidé, en 1995, de mettre au point un algorithme de tatouage qui tient compte de l'algorithme de compression JPEG. On ne peut cacher l'information dans les coefficients de Fourier de haute fréquence car ceux-ci sont modifiés lors de la compression ; on ne peut, non plus, changer les coefficients de basse fréquence qui se

## 4. AUTOCORRÉLATION DES SUITES

Une technique de tatouage consiste à disposer dans l'image une suite de bits de façon qu'elle soit clairement identifiable. Pour cela il importe que la fonction d'autocorrélation, que nous allons examiner, soit de valeur élevée, et que les fonctions de corrélation avec des suites décalées soient faibles. Examinons deux suites où chaque terme est égal à +1 ou -1 : la corrélation de ces deux suites est égale au nombre de fois où deux chiffres de même rang coïncident, moins le nombre de fois où ils diffèrent, c'est-à-dire à la somme des produits des termes de même rang.

$$\begin{array}{cccccc} \text{Suite 1} & 1 & -1 & 1 & 1 & -1 \\ \text{Suite 2} & -1 & -1 & 1 & -1 & -1 \\ & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \text{Corrélation} & -1 & +1 & +1 & -1 & +1 = 3 - 2 = 1 \end{array}$$

L'autocorrélation d'une suite est mesurée par toutes les corrélations entre cette suite et ses versions décalées (permutations circulaires).

|                                     |    |    |    |    |    |                          |
|-------------------------------------|----|----|----|----|----|--------------------------|
| Suite initiale                      | 1  | -1 | 1  | 1  | -1 | Corrélation : 5 - 0 = 5  |
| Suite décalée de 1                  | -1 | 1  | -1 | 1  | 1  | Corrélation : 1 - 4 = -3 |
| Suite décalée de 2                  | 1  | -1 | 1  | -1 | 1  | Corrélation : 3 - 2 = 1  |
| Suite décalée de 3                  | 1  | 1  | -1 | 1  | -1 | Corrélation : 3 - 2 = 1  |
| Suite décalée de 4                  | -1 | 1  | 1  | -1 | 1  | Corrélation : 1 - 4 = -3 |
| Suite décalée de 5 = suite initiale |    |    |    |    |    |                          |

Une suite, dite M-séquence, présente une autocorrélation optimale (un pic très net, et les autres valeurs presque nulles) :

|                    |    |    |    |    |    |    |    |                          |
|--------------------|----|----|----|----|----|----|----|--------------------------|
| Suite initiale     | -1 | -1 | 1  | -1 | 1  | 1  | 1  | Corrélation : 7 - 0 = 7  |
| Suite décalée de 1 | 1  | -1 | -1 | 1  | -1 | 1  | 1  | Corrélation : 3 - 4 = -1 |
| Suite décalée de 2 | 1  | 1  | -1 | -1 | 1  | -1 | 1  | Corrélation : 3 - 4 = -1 |
| Suite décalée de 3 | 1  | 1  | 1  | -1 | -1 | 1  | -1 | Corrélation : 3 - 4 = -1 |
| Suite décalée de 4 | -1 | 1  | 1  | 1  | -1 | -1 | 1  | Corrélation : 3 - 4 = -1 |
| Suite décalée de 5 | 1  | -1 | 1  | 1  | 1  | -1 | -1 | Corrélation : 3 - 4 = -1 |
| Suite décalée de 6 | -1 | 1  | -1 | 1  | 1  | 1  | -1 | Corrélation : 3 - 4 = -1 |

De telles suites sont très utilisées en télécommunications. Ici, elles vont servir de structures de référence et seront garantes de la présence du tatouage.

traduisent sur l'image par des zones homogènes où toute modification est visible. Aussi les chercheurs changent-ils, selon une règle préétablie, les valeurs des coefficients de Fourier, pour des fréquences moyennes. Les blocs  $8 \times 8$  ainsi transformés sont déterminés par la clé secrète. Le filigrane enfoui dans l'image résiste alors bien à une compression JPEG ; il est néanmoins très vulnérable aux manipulations géométriques et à l'impression/renumérisation.

## LE PIC CACHÉ

Nous l'avons vu, l'objectif du tatouage est de transmettre une information à travers un support (l'image), bien que cette image subisse des transformations. Il est alors naturel d'utiliser des techniques qui ont fait leurs preuves dans les télécommunications. L'exemple le plus flagrant que nous allons examiner est celui de l'étalement de spectre. L'idée est de plaquer sur l'image un signal bidimensionnel ressemblant à une tôle ondulée ; la transformée de Fourier de ce signal a la forme d'un pic centré autour de la fréquence d'ondulation et décroît fortement autour

de ce pic. La clé est la structure de la tôle, c'est-à-dire sa fréquence spatiale et la direction d'ondulation.

Imaginons maintenant que vous désiriez prouver la provenance d'une image tatouée, en l'absence de l'image originale. Vous prenez la transformée de Fourier de l'image tatouée et vous en extrayez, grâce à la clé, le signal caché (voir la figure 5). Reste alors à vérifier si celui-ci contient bien la structure adéquate.

## LES M-SÉQUENCES

Un tatouage bien identifiable est obtenu à l'aide de suites binaires, appelées «M-séquences», qui présentent une très faible corrélation avec toutes leurs versions décalées ; à titre d'exemple (voir la figure 4), une version décalée à droite d'un cran de (1, -1, 1, -1, -1) est (-1, 1, -1, 1, -1).

L'analyse de la courbe de corrélation de ce pic permet de l'identifier même s'il a été déformé. La vérification est plus probante qu'une comparaison de la suite initiale de bits et de cette suite altérée. Cette technique a été employée, entre autres, par l'équipe «télé» de l'Université catholique de Louvain, qui a mis au point