



Le tatouage des images numériques

CAROLINE FONTAINE

Le tatouage des images, qui protège les créateurs, est indécélable par l'observateur : l'image de droite, tatouée, semble identique à la figure de gauche. Le tatouage est une signature qui prouve l'origine de la copie. Il n'est efficace que s'il résiste aux divers traitements de l'image, compression, ajout de bruit, changement de contraste, etc.



Le développement des réseaux de communication et des supports numériques comme le Compact Disc, le CD-ROM, le Digital Versatile Disc... entraîne une diffusion massive de documents stockés à l'aide de formats numériques, tels JPEG, MPEG, MP3. Ces techniques, qui permettent d'emmagasiner une grande quantité d'information en peu de place, facilitent aussi l'utilisation illégale des documents : il est en effet extrêmement aisé de récupérer un document sur Internet, ou sur un CD-ROM, et de le copier un grand nombre de fois avant de diffuser ces duplications. Non seulement la copie est facile, mais elle est parfaite : alors qu'un document analogique se détériore lorsqu'on le duplique, la copie numérique a exactement les mêmes qualités que l'original. Ces manipulations, si elles débouchent sur la commercialisation des copies, ou sur toute utilisation autre que privée, sont illégales tant que les droits d'auteur n'ont pas été versés à l'ayant droit du document.

L'objectif est d'associer à un document le nom du ou des ayant(s) droit associé(s) (il peut y avoir plusieurs ayants droit : le créateur, le producteur et le diffuseur, par exemple).

LA NÉCESSITÉ DE NOUVELLES TECHNIQUES

La recherche sur la protection des images a principalement débuté vers 1993, et aujourd'hui plus d'une centaine d'articles sont annuellement consacrés à ce sujet. Les premières techniques, comme le contrôle d'accès (destiné à autoriser ou

à refuser l'accès au document) ou la cryptographie (chiffrer ou signer le document) se sont révélées insuffisantes ou d'un emploi difficile. En effet, les dispositifs de cryptographie protègent l'image lors d'une transaction, mais pas au-delà : le destinataire retrouve après déchiffrement (ou vérification de la signature) la même version de l'image que celle qui précédait l'envoi, donc sans protection. Une technique complémentaire a alors été envisagée : le tatouage, dérivé de la stéganographie.

La stéganographie est l'art de cacher une information, une signature, dans un message que n'importe qui va pouvoir observer. Ce message peut être de diverses natures : texte, image, son. Une manière très simple est, par exemple, d'écrire un texte et de considérer le premier mot de chaque ligne : le texte «acrostiche» semble innocent dans sa globalité, mais la phrase constituée des premiers mots de chaque ligne peut avoir un sens tout différent. On peut aussi, dans un message électronique, placer des espaces en fin de ligne, le nombre d'espaces déterminant le «caractère» caché dans cette ligne ; on peut aussi inscrire l'information dans certaines composantes de l'image. Ainsi, toute personne non avertie ne s'apercevra pas qu'une information importante est transmise par l'intermédiaire d'un document d'apparence innocente.

L'idée est de cacher dans le document une information propre à son ayant droit sous la forme d'une marque qui ne pourra être enlevée sans une altération importante de ce document (rendant alors son

utilisation impossible). Cette marque, dénommée filigrane, devra rester imperceptible et faire suffisamment corps avec le document pour rester présente malgré les manipulations que ce dernier risque de subir. Les transformations pouvant altérer la marque sont des rotations, des changements d'échelle, des symétries, des découpages, des changements de format, l'application de filtres, l'ajout de bruit etc. La marque peut aussi être dégradée lors d'une impression/renumérisation par scanner.

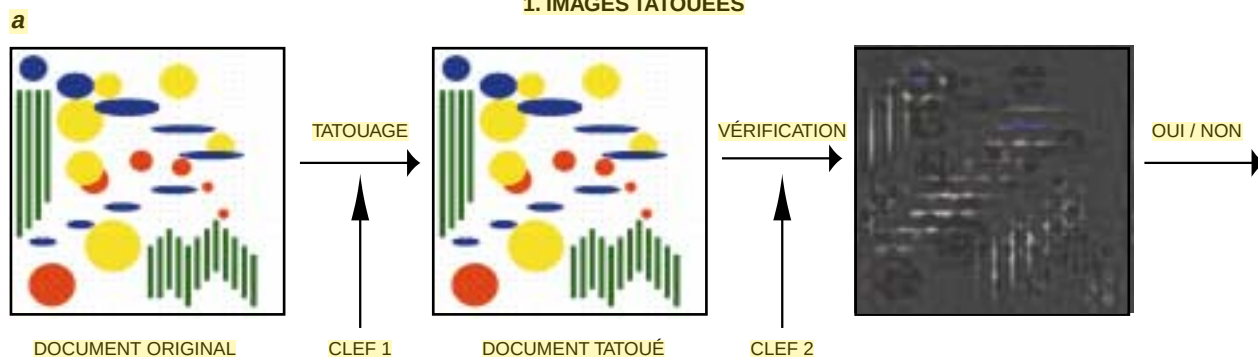
Ces manipulations peuvent avoir pour but la destruction de la marque, ou tout simplement une utilisation facilitée de l'image (compression JPEG ou changement d'échelle, par exemple). On doit reconnaître la marque même quand le contenu numérique de l'image a changé.

Un système de tatouage dépend du contexte de son utilisation ; les spécialistes prennent en considération les contraintes des ressources informatiques (temps d'exécution des programmes de tatouage et de vérification, mémoire disponible) et les impératifs de la sécurité (environnement ouvert, fermé, qui va avoir accès à quoi, qui va exécuter les programmes de tatouage, de vérification).

LE PRINCIPE DE VÉRIFICATION

L'algorithme de tatouage, supposé connu de tous, est paramétré par une clé qui reste secrète : il n'est pas raisonnable de faire reposer la sécurité du système sur l'idée que personne ne connaît l'algorithme, car on sait bien que, dans la

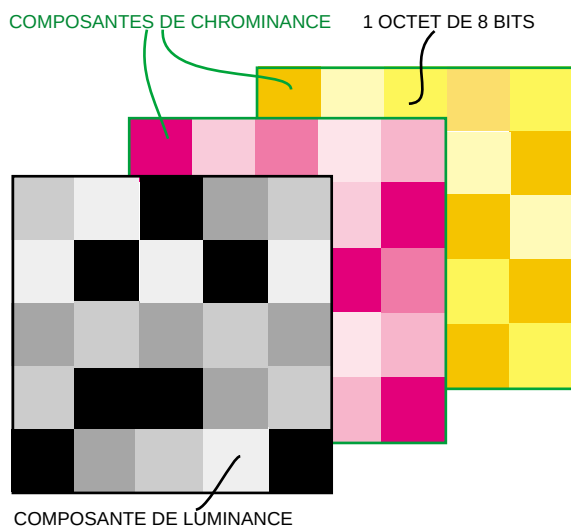
1. IMAGES TATOUÉES



Dans un système de tatouage (a), l'incrustation du filigrane est paramétrée par une clé ; l'algorithme de vérification dit si cette clé a bien servi à tatouer le document, et donc si la personne détentrice de la clé est propriétaire des droits du document. Exemple d'image tatouée (b) par l'algorithme mis au point à l'Université catholique de Louvain (Belgique)

avec, de gauche à droite, l'image originale, l'image tatouée, le tatouage "différence". Le tatouage, invisible à l'œil, exploite la nature de l'image : l'information cachée est insérée dans les zones où les variations d'intensité sont notables, car le changement sera moins perceptible, alors que dans les zones uniformes toute modification est patente.

2. LE STOCKAGE DES IMAGES NUMÉRIQUES



Il existe de nombreux formats de stockage des images numériques : bitmap, pixmap, gif, tiff, ppm... Une image est un tableau de pixels, ces derniers étant souvent codés sur trois octets (1 octet, égal à 8 bits, peut prendre 256 valeurs, de 0 à 255 ; le bit de poids faible de l'octet désigne celui qui code la parité du nombre représenté : 1 si le nombre est impair, 0 s'il est pair). Ces octets peuvent désigner les proportions de Rouge, Vert et Bleu, ou bien de manière équivalente une composante de luminance (intensité lumineuse) et deux composantes chromatiques (couleur). Certains formats, comme JPEG, correspondent à une version compressée de l'image. La compression minimise l'espace mémoire occupé dans le disque : la quantité d'information contenue dans l'image compressée est inférieure à celle de l'image initiale, et la quantité d'information perdue, paramétrée par l'utilisateur, détermine la qualité de l'image compressée. Cette compression peut altérer le tatouage et le rendre inopérant.