Filigranage d'images digitales

Autor(en): **Deguillaume, Frédéric / Voloshynovski, Sviatoslav / Pereira, Shelby**
Objekttyp: **Article**

Zeitschrift: **Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association Suisse des Electriciens, de l'Association des Entreprises électriques suisses**

Band (Jahr): **92 (2001)**

Heft 9

PDF erstellt am: **08.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-855698

Filigranage d'images digitales

Les technologies numériques se sont considérablement répandues et imposées en tant que vecteurs des données, documents et œuvres de notre vie quotidienne, se substituant de plus en plus aux supports analogiques traditionnels. Les avantages techniques des supports digitaux sont innombrables; les outils tels

que les ordinateurs, les imprimantes, et les moyens de communication numérique à haut débit sont devenus bon marchés et largement accessibles. La popularité de l'Internet a clairement démontré le formidable potentiel économique du marché du multimédia digital, et les utilisateurs investissent largement dans l'audio, l'image et la vidéo numériques.

Malheureusement ces avancées technologiques offrent aussi une opportunité sans précédent pour le piratage d'œuvres protégées par un droit d'auteur (copyright); en effet, les données numériques peuvent être très aisément et rapidement recopiées à l'infini de manière exacte, donc sans perte de qualité, à un coût dérisoire. Aussi une solution proposée à ce problème est d'insérer un filigrane digital

Frédéric Deguillaume, Sviatoslav Voloshynovskiy, Shelby Pereira, Maribel Madueno, Thierry Pun

(tatouage, ou watermark) invisible et robuste dans le document à protéger, sorte d'équivalent des filigranes papier d'autrefois, afin de détecter et de suivre les violations de copyright [1–6]. Le filigranage digital est devenu un domaine de recherche très actif, et qui suscite le plus grand intérêt parmi les artistes, les éditeurs, etc. – d'une manière générale parmi ce que l'on peut appeler les fournisseurs de contenu.

Différentes applications du filigranage digital

Un filigrane digital est une marque invisible insérée dans le document, et qui contient une information [5, 6]. Ce qui est important est que cette information n'est pas placée dans une entête, mais dans les données elles-mêmes au moyen de la modification de certaines de leurs composantes. En fait le principe de cacher une information dans des données hôtes concerne de nombreux domaines d'applications, dont les principaux sont:

- *la sténographie:* Le premier – et sans doute le plus ancien – d'entre eux est la «stéganographie» (du grec steganos, communication secrète) où l'information insérée correspond à un message que l'on veut communiquer secrètement à un correspondant, sous couvert d'une communication d'apparence anodine; dans ce cas la quantité d'information cachée est en général importante.
- *la vérification d'intégrité:* L'information insérée permet la détection de toute modification du document.
- l'*authentification:* Elle consiste à vérifier que le document protégé est bien celui que l'on pense ou provient bien de l'expéditeur déclaré; elle peut concerner les applications légales ou administratives, comme les pièces à conviction lors des procès, ou les cartes d'identité infalsifiables.

D'autres applications ne sont pas liées à la sécurité: par exemple à des fins commerciales, un document peut contenir un lien vers un site Internet à titre de publicité, et sa présentation à une caméra entraîner automatiquement la connexion à ce site (internet-bridge); les aveugles et les malvoyants peuvent bénéficier d'images contenant une brève description, qui serait lue par synthèse vocale à l'aide d'un logiciel adapté.

Le copyright

Dans le cas du filigranage appliqué à la protection du copyright, une infrastructure de sécurité est nécessaire afin que la protection soit efficace. Cette infrastructure est non seulement d'ordre technique, mais aussi d'ordre légal. Très brièvement, un ayant-droit (copyright holder ou CH) enregistre préalablement son œuvre auprès d'un centre d'enregistrement des copyrights agréé (copyright center, CC), qui retourne à ce dernier un certificat de copyright crypté contenant les informations nécessaires à l'identification du copyright déposé ainsi qu'une date de dépôt infalsifiable (timestamp). Le filigrane inséré dans le document est alors un pointeur qui permet de retrouver l'information associée au copyright dans la base de données du CC. Si un client veut se procurer ou acheter le document protégé, il doit en demander l'autorisation au CH et au CC. Le système, ainsi que les échanges entre les différents acteurs, sont basés sur des techniques de cryptographie assymétrique (c'est-à-dire utilisant des paires «clé publiques – clés privées»), qui garantissent entre autres la confidentialité de la clé secrète utilisée pour l'insertion du filigrane. Ainsi le décodage d'un copyright dans un document qui a été préalablement enregistré auprès du CC peut constituer une preuve en cas de litige.

Les techniques de filigranage digital utilisées sont très différentes selon le type de données à marquer; dans cet article nous nous intéresserons au filigranage robuste des images, appliqué à la protection du copyright.

Principe du filigranage digital

Dans le cas de la protection du copyright, l'information insérée (message) contient généralement le propriétaire du document, son ayant-droit, ou un client auquel le document a été vendu; il peut aussi s'agir d'un pointeur vers une base de données contenant ces informations. L'altération des données marquées lors de l'insertion du filigrane doit être imperceptible à l'être humain, mais aussi robuste que possible, c'est-à-dire impossible à enlever ou à invalider sans dégrader la qualité du document au point de le rendre sans valeur. D'une façon générale, les trois critères principaux d'un bon filigrane destiné à la protection du copyright sont:

- *l'imperceptibilité:* la marque doit être invisible, inaudible dans le cas de l'audio, etc. afin de ne pas réduire la valeur du document
- *la robustesse:* il ne doit pas être possible de la supprimer ou de l'invalider sans y être autorisé

– *la capacité:* la quantité d'information dans le message doit être suffisante

Le message est généralement crypté à l'aide d'une clé gardée secrète, cette clé étant requise pour son extraction et son décodage, c'est-à-dire pour la vérification d'un document suspect. Les techniques les plus récentes permettent l'extraction du message sans avoir recours au document original (oblivious watermarking).

Le processus d'insertion et de vérification d'un filigrane digital dans une image est illustré par la figure 1. La première étape est l'insertion du filigrane, ou filigranage, à l'aide d'une clé secrète. La deuxième est la distribution de l'image marquée qui peut alors subir diverses altérations ou attaques. La dernière étape est l'extraction du message en utilisant la même clé secrète.

Le filigranage

Premièrement le filigrane est inséré dans l'image originale x que l'on veut protéger, donnant l'image filigranée y. Le message m est représenté en binaire, c'est-à-dire par n bits $m_i \in \{0, 1\}$, $i = 1 \ldots n$. m est ensuite crypté et encodé à l'aide d'une clé secrète K, donnant le code c. Le cryptage, utilisant un algorithme de cryptographie symétrique connu, assure la confidentialité du message, alors que son encodage définit la manière dont il est représenté. L'encodage inclut typiquement un code de détection ou de correction des erreurs (error correction code, ECC), des bits de référence ainsi que la disposition des bits dans les blocs. Généralement, c est représenté par n_c symboles $c_j \in \{-1, 0, 1\}$, $j = 1 \ldots n_c$. Dans un filigranage additif (ce qui est le plus souvent utilisé), les symboles -1 et 1 correspondent aux bits initiaux $\{0, 1\}$ et sont respectivement soustraits ou ajoutés aux données à marquer, souvent après modulation par un facteur; les symboles à 0 correspondent aux composantes qui ne seront pas modifiées. Afin d'assurer l'invisibilité, c est modulée par un modèle visuel, c'est-à-dire par une fonction de masquage visuel $M(x)$ calculée à partir de l'image originale sur les bases des propriétés du système visuel humain (human visual system, HVS). $M(x)$ permet d'augmenter l'énergie du filigrane tout en assurant son invisibilité, par exemple en augmentant son intensité dans les composantes de l'image les plus «masquantes» telles que les contours, et en la diminuant dans les composantes plus «vulnérables» telles que les zones relativement constantes. Le résultat est le filigrane w qui est inséré dans l'image pour donner l'image filigranée y.

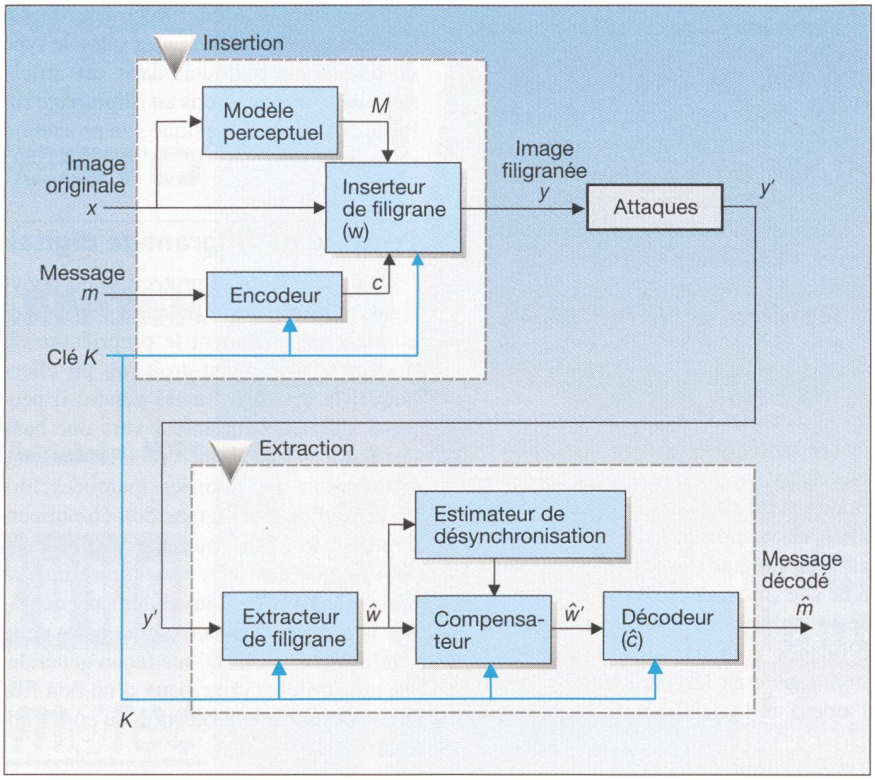

Fig. 1 Principe du filigranage digital. *Insertion:* un message m est encodé et crypté avec la clé secrète K, donnant le message codé c; le message codé produit un filigrane w qui est inséré dans l'image originale x, donnant l'image filigranée y. Un modèle visuel M calculé à partir de x module w lors de son insertion afin d'assurer son invisibilité. *Attaques:* l'image filigranée y subie des attaques, résultant en une version altérée y'. *Extraction:* de y' est extraite une estimation $\hat{w}$ du filigrane. La désynchronisation (distorsions géométriques) éventuellement subie est déterminée, et le filigrane est compensé en conséquence donnant $\hat{w}'$. Le message est décodé, résultant en un code estimé $\hat{c}$, puis un message estimé $\hat{m}$. Le processus nécessite l'utilisation de la même clé K que lors de l'insertion.

Les attaques

L'image filigranée et distribuée peut subir diverses attaques, qui sont constituées par toutes les altérations qu'elle peut subir, intentionnelles ou non, et qui ont pour conséquence d'affaiblir le filigrane inséré ou d'en rendre la détection difficile. Les attaques considérées sont soit une dégradation ou un filtrage de l'image tendant à affaiblir le filigrane, soit des distorsions géométriques qui le désynchronisent. Par exemple l'impression sur papier est une attaque (généralement non intentionnelle) qui correspond à une conversion analogique. Dans ce cas l'image doit être renumérisée sur un scanner afin de pouvoir en lire le filigrane, et ce processus combine généralement une dégradation de la qualité (due surtout à la trame d'impression) et une rotation de la feuille qui est posée non alignée sur le scanner. Les attaques sont discutées dans un prochain paragraphe. Le résultat est l'image filigranée et éventuellement altérée y'.

L'extraction

L'image y' est vérifiée afin de savoir si elle contient un copyright. D'abord le filigrane est estimé à partir de y', ce qui peut se faire par une approche stochastique, en considérant le filigrane comme un bruit ajouté à l'image. On obtient une estimation du filigrane $\hat{w}$. Ensuite un estimateur de désynchronisation calcule les éventuelles distorsions géométriques subies par l'image à partir de $\hat{w}$ et corrige le signal produisant une estimation compensée $\hat{w}'$. Les techniques pouvant être utilisées pour la détermination des transformations géométriques sont données dans le paragraphe suivant. L'information est ensuite extraite de $\hat{w}'$, donnant le code estimé $\hat{c}$ qui est corrigé à l'aide de l'ECC puis décrypté, donnant une estimation du message d'origine. Le décodage et le décryptage de $\hat{c}$ requièrent la même clé secrète K que celle qui a été utilisée pour le filigranage.

Méthodes de filigranage

De manière générale, on peut considérer deux catégories de techniques de filigranage: le filigranage dans le domaine spatial, où l'information est insérée directement dans l'image, et le filigranage dans le domaine transformé où l'informa-

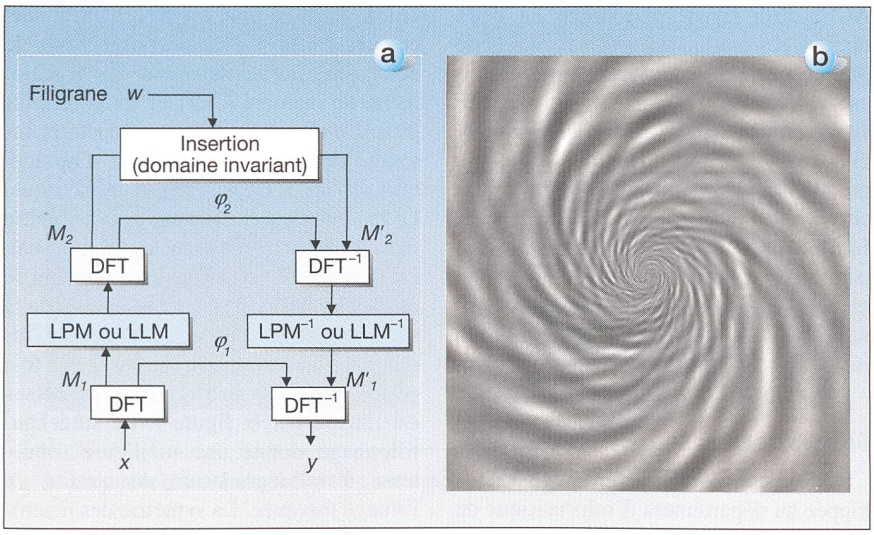

Fig. 2 Filigranage invariant basé sur la transformée de Fourier-Mellin (TFM). *a:* La TFM comprend deux transformées de Fourier (DFT) et une conversion en log-polar map (LPM), ou en log-log map (LLM); les notations DFT^{-1}, LPM^{-1} et LLM^{-1} représentent les inverses respectives de ces transformations. Seules les magnitudes des DFT successives (M_1, M_2) participent au processus, les phases (φ_1, φ_2) étant conservées sans modification. La magnitude M_2 de la TFM forme le domaine invariant où le filigrane peut être inséré; l'invariance est en rotation et changement d'échelle pour la version LPM, ou en changement d'échelle et de proportion pour la version LLM. *b:* Un filigrane (amplifié) dans le domaine TFM, version LPM

tion est placée dans une transformée mathématique de l'image telle que la transformée de Fourier. D'autre part, les méthodes actuelles de filigranage résistent essentiellement aux distorsions géométriques telles que les rotations, les changements d'échelle et de proportions, les transformations affines générales, et plus rarement les déformations locales aléatoires. Actuellement la résistance aux transformations géométriques est assurée principalement par trois méthodes: premièrement les filigranes insérés dans un domaine invariant aux distorsions; deuxièmement les filigranes accompagnés par des données de synchronisation appelées template; et enfin les filigranes auto-référencés.

Domaine spatial et domaine transformé

Le filigranage dans le domaine spatial

Cette approche consiste en la modification directe des pixels de l'image. Afin d'assurer l'invisibilité de la marque, cette modification doit rester limitée. Une des toutes premières approches utilisée consiste à insérer les bits du message dans les bits de poids faible de chaque pixel (least significant bits, LSB). Une autre approche, appelée patchwork, est la modification des propriétés statistiques de petites régions de l'images, comme la moyenne ou l'écart-type, le message étant représentée par exemple par la différence des ces propriétés entre deux régions adjacentes. On peut aussi inclure dans cette catégorie les techniques consistant à encoder le message dans l'histogramme de l'image, en modifiant les valeurs des pixels en conséquence. Ou bien le filigrane w peut être tout simplement ajouté aux pixels de l'image, avec une faible intensité bien sûr, selon les principes énoncés dans le paragraphe précédent.

L'inconvénient des méthodes appliquées au domaine spatial ci-dessus est qu'elles sont en général peu robustes. C'est en particulier le cas de l'approche LSB, qui ne résiste à aucune altération, même la plus mineure.

Le filigranage dans le domaine transformé

Une autre approche est d'insérer l'information après avoir calculé une transformée de l'image à marquer. L'avantage de cette approche est la possibilité de mieux décorréler les composantes de l'image, en particulier celles qui résistent le mieux aux altérations, ainsi que celles dont la modification ont peu d'impact visuel. Le domaine transformé présente en effet une meilleure correspondance avec le HVS, et il y est alors plus aisé d'isoler les composantes qui ont peu d'impact visuel. Le filigrane est alors plus robuste, tout en restant invisible. La transformée la plus utilisée est celle de Fourier dans sa version discrète (discrete Fourier transform, DFT), qui décompose l'image en toutes ses composantes fréquentielles. En observant que la majeure partie de l'énergie d'une image se trouve concentrée dans les basses fréquences spatiales, et que les signaux ajoutés dans les fréquences moyennes ou élevées sont peu visibles, le filigrane sera essentiellement ajouté dans les fréquences moyennes. De manière analogue, la transformée cosinus discrète (discrete cosine transform, DCT) qui est utilisée par les standards de compression MPEG et JPEG peut être employée. Mentionnons aussi qu'il existe des méthodes basées sur une décomposition fractale de l'image, qui exploitent les similitudes à différentes échelles pour encoder l'information. Cependant une transformée de plus en plus utilisée aujourd'hui pour le filigranage, et que nous proposons, est la transformée par ondelettes discrète (discrete wavelets transform, DWT) [7, 8]. Comme nous allons le voir dans les paragraphes suivants, la DWT permet de séparer différentes résolutions d'image, en meilleur accord avec le HVS, tout en conservant une certaine possibilité de localisation spatiale dans l'image (ce que la DFT ne permet pas). En outre, les algorithmes basés sur les ondelettes peuvent aisément s'intégrer dans les standards de compression futurs, tels que JPEG 2000, qui sont aussi basés sur cette transformée.

Résistance aux transformations géométriques

Insertion d'un filigrane

Une des premières approches utilisées consiste à insérer le filigrane dans un domaine transformé complètement invariant à (certaines) distorsions géométriques. Par exemple il est bien connu que la magnitude de la DFT est invariante aux translations, donc un filigrane placé dans ce domaine sera aussi invariant aux translations. De même, une transformée de Fourier-Mellin (TFM), qui combine la magnitude de deux DFT successives et une conversion dans une espace logarithmique et polaire (e^{μ}, θ) appelé log-polar map (LPM), est invariant aux translations, aux rotations (d'angle θ), et aux changements d'échelle (proportionellement à e^{μ}) [9]. En utilisant la TFM en combinant les deux DFT avec un espace logarithmique (e^{μ_x}, e^{μ_y}) appelé log-log map (LLM), on est invariant aux translations, aux changements d'échelle ou de proportions (proportionnellement à e^{μ_x}, e^{μ_y}, le long de chaque axe). La figure 2a représente le processus de filigranage avec la TFM, et la figure 2b montre l'apparence d'un filigrane dans le domaine de la TFM (version LPM). Malheureusement la TFM n'est pas invariante à une rotation combinée avec un changement de proportions, ni aux transformations affines en général, et d'autre part introduit une perte de qualité importante dans l'image filigranée en raison des interpolations successives.

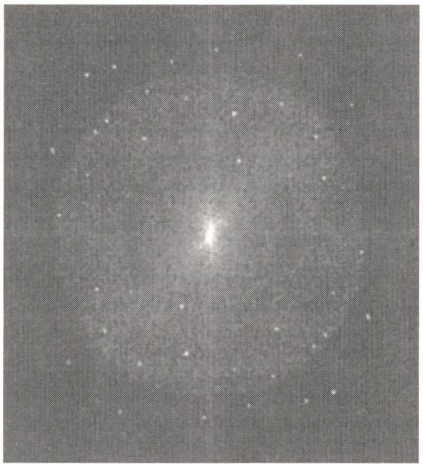

Fig. 3 Filigrane (amplifié) avec template, dans la magnitude de la transformée de Fourier. La tâche centrale (basses fréquences) concentre la majeure partie de l'énergie de l'image, le disque correspond au filigrane (fréquences moyennes), et les points sont les points du template.

Insertion d'un template

Une deuxième approche largement utilisée est l'insertion d'un template en plus du filigrane, ce dernier n'étant pas invariant. Le template consiste généralement en un certain nombre de points de référence insérés dans la magnitude de la DFT de l'image [10]. Lors de l'extraction, la comparaison des pics extraits de la DFT de l'image, avec les positions de référence connues, permet la détermination des distortions subies et la resynchronisation du filigrane. En principe toute transformation affine générale peut être déterminée par cette approche [11]. La figure 3 est un exemple de filigrane dans la DFT accompagnée d'un template. Cependant le premier inconvénient de cette approche est la nécessité d'une recherche exhaustive coûteuse en performances entre les points de référence et les points extraits, même si des contraintes sont appliquées afin de se limiter aux distorsions acceptables. Le second inconvénient est le manque de robustesse du template, qui contient une énergie bien plus faible que le filigrane afin d'éviter trop d'artefacts visibles.

Insertion d'un filigrane auto-référencé

Enfin la troisième approche utilisée, la plus récente, qui est aussi celle proposée dans cet article, est d'insérer un filigrane auto-référencé qui permet sa resynchronisation par lui-même, sans nécessiter un template supplémentaire [3, 8]. Un tel filigrane est répétitif, et donc périodique, et peut être inséré soit dans le domaine spatial, soit dans le domaine transformé de l'image. L'approche utilisée ici est basée sur le fait que la fonction d'autocorrélation (autocorrelation function, ACF) d'un signal périodique en deux dimensions produit une grille régulière de pics (i.e. des maxima locaux), et dont les espacements correspondent aux périodes selon chaque direction de périodicité. Grâce à son ACF, le filigrane lui-même produit un template permettant la resynchronisation de toutes les distortions affines. Comme nous allons le voir dans les paragraphes suivants, cette approche est bien plus robuste comparée à celles utilisant un template, et d'autre part évite les recherches exhaustives.

Filigranage par ondelettes

La technique de filigranage développée au département d'informatique de l'Université de Genève consiste en l'insertion d'un filigrane auto-référencé périodique, utilisant l'auto-corrélation (ACF), dans la transformée par ondelettes (DWT) de l'image [8]. Le message m, de 64 bits typiquement, est encodé par un code correcteur d'erreurs (ECC) et crypté à l'aide de la clé secrète K, puis répété afin d'obtenir un filigrane périodique. Le filigrane est modulé en fonction du HVS et ajouté à la DWT de l'image originale. La figure 5 montre un image avant et après son filigranage par notre méthode; aucune différence n'est visible entre les deux.

Un filigrane robuste aux transformations affines

Afin de produire un filigrane périodique, m est encodé, crypté, et est alloué dans un bloc carré de petite taille. Lors du processus d'encodage, des bits de référence sont aussi ajoutés dans le bloc, qui permettront la resynchronisation en translation. Puis, ce bloc est suréchantillonné, ce qui signifie que chaque point est répété deux fois, horizontalement et verticalement, de manière à former un point plus gros. Le résultat est encore répété et retourné deux fois dans chaque direction, afin d'obtenir un macrobloc symétrique. Le macrobloc a finalement un côté quatre fois plus grand que celui du bloc initial. La périodicité est obtenue en répétant le macrobloc afin de couvrir la totalité de la surface de l'image, ceci donnant au filigrane w une structure régulière, à la fois périodique et symétrique. Ce processus est illustré par la figure 4. Le suréchantillonnage donne une meilleure robustesse à la dégradation de qualité de l'image marquée. La symétrie des macroblocs assure premièrement une résistance intrinsèque aux retournements et/ou aux rotations à angle droit de l'image, et deuxièmement diminue l'impact visuel qu'aurait une périodicité trop marquée.

Lors de la détection, le filigrane est d'abord estimé à partir de l'image filigranée y, donnant $\hat{w}$, à l'aide d'une approche stochastique qui considère le filigrane comme un bruit additif Gaussien. Un filtre de Wiener/Lee est utilisé pour cette étape,

$$\hat{x} = \bar{y} + \frac{\sigma_x^2}{\sigma_w^2 + \sigma_x^2} \cdot (y - \bar{y}) \qquad (1)$$

où $\bar{y}$ est la moyenne locale de y (utilisée comme approximation $\bar{x}$, la moyenne local de x), σ_x^2 est la variance globale de l'image originale x, et σ_w^2 est la variance globale de w; les variances sont estimées à partir de y et $\bar{y}$. On obtient $\hat{x}$, une estimation de l'image originale, qui est en

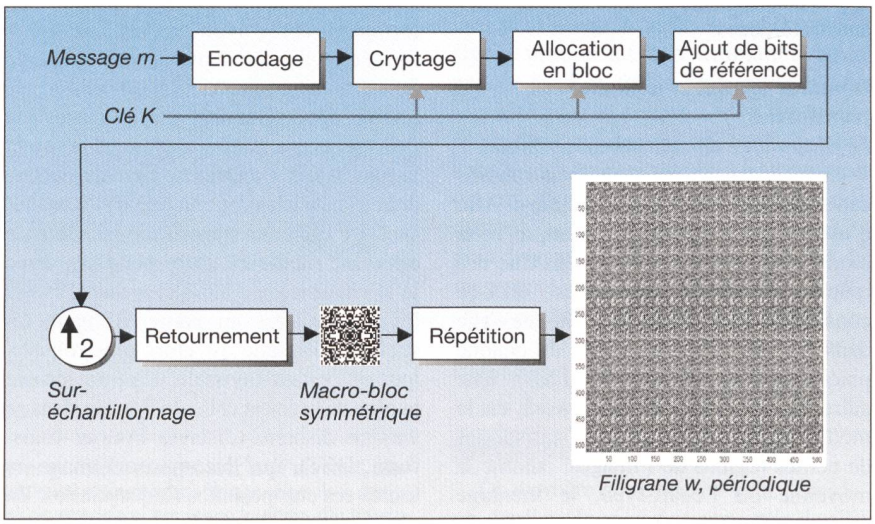

Fig. 4 Génération d'un filigrane auto-référencé. Le message m est encodé donnant c, crypté, et alloué dans un bloc 2D de petite taille; des bits de référence sont aussi ajoutés dans le bloc. L'encodage, le cryptage, l'allocation en bloc et les bits de références dépendent tous de la clé K. Le bloc est ensuite suréchantillonné deux fois, répété avec retournement dans chaque direction, donnant un macrobloc de symétrie centrale. Le macrobloc est enfin répété de manière à couvrir l'image à filigraner, ce qui lui donne une structure périodique.

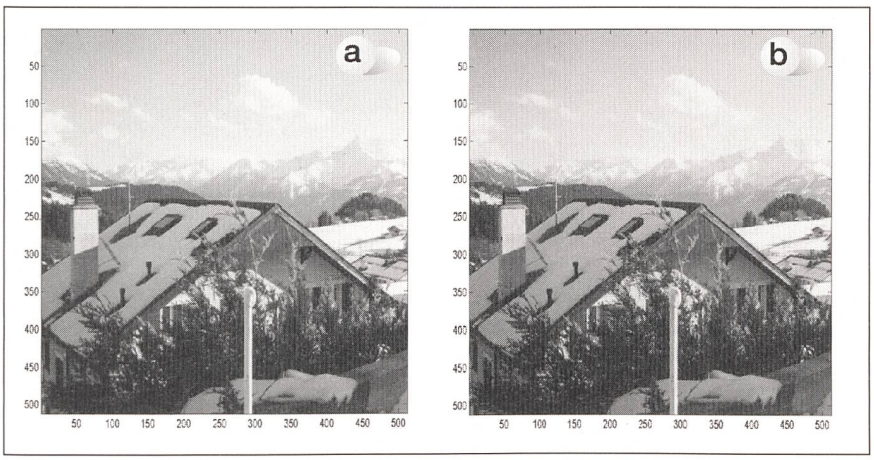

Fig. 5 *a:* Image originale. *b:* Image filigranée par l'approche développée à l'Université de Genève

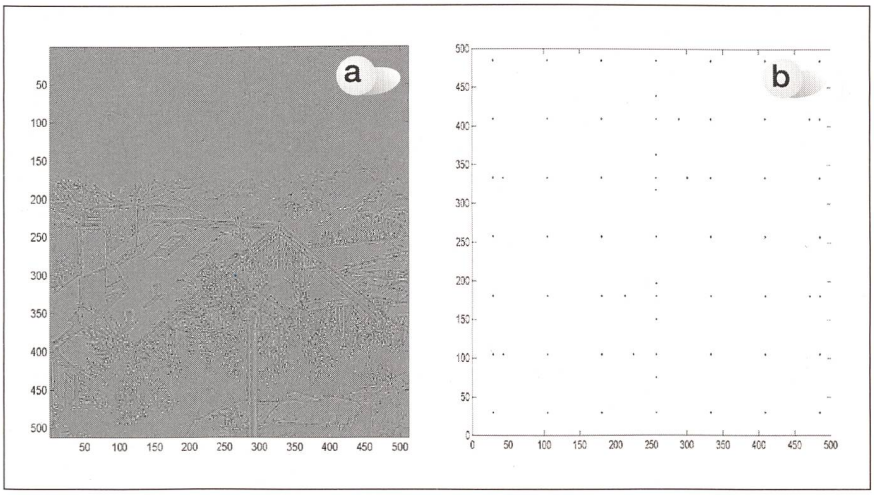

Fig. 6 *a:* Estimation du filigrane à partir de l'image filigranée basée sur une modélisation stochastique. *b:* calcul des points de la fonction d'auto-corrélation (ACF); leur disposition correspond à la période du filigrane, hormis quelques points supplémentaires produits par du bruit.

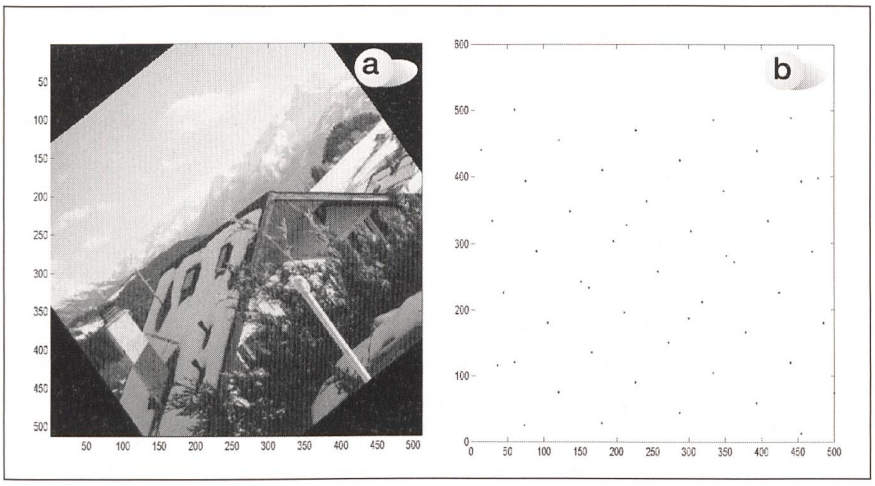

Fig. 7 *a:* Image filigranée ayant subi une rotation. *b:* Points de l'ACF correspondante

fait une image restaurée à partir de y. Le filigrane est alors estimé par $\hat{w}=y-\hat{x}$; il est illustrée par la figure 6a. Une ACF est ensuite calculée sur $\hat{w}$, donnant une série de pics, c'est-à-dire des maximas locaux, alignés selon les deux axes de périodicité de $\hat{w}$ et dont les espacements correspondent aux périodes selon les axes (figure 6b). Si l'image a subie une transformation affine, les directions des axes et les périodes sont modifiées, mais la structure reste régulière. D'autre part l'ACF peut être efficacement calculée à l'aide de la DFT.

C'est à ce stade que la périodicité du filigrane est utilisée pour la resynchronisation. Pour cela on assume que les distorsions géométriques subies sont des transformation affines générales. Les transformations affines comprennent les translations, les rotations, les changements d'échelle et de proportion, les cisaillements, les renversements horizontaux ou verticaux, ainsi que toute combinaison de ces distorsions. Une transformation affine peut être représentée par les quatre paramètres a, b, c, d pour la compostente linéaire, formant la matrice A cidessous, et par les deux paramètres v_x, v_y pour la composante translation formant le vecteur $\vec{v}$. En écrivant A et $\vec{v}$:

$$A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \vec{v}=\begin{pmatrix} v_x \\ v_y \end{pmatrix} \tag{2}$$

un point de coordonnées (x, y) est envoyé sur les nouvelles coordonnées (x', y') selon l'expression

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = A\begin{pmatrix} x \\ y \end{pmatrix} + \vec{v} \tag{3}$$

L'estimation de la matrice A se fait à partir des deux axes et des deux périodes des points de l'ACF, par référence avec les axes et périodes d'origine. La redondance et le caractère aligné des points permet une estimation robuste des axes, tout en évitant d'avoir recours à une recherche exhaustive. La figure 7 montre la structure de l'ACF lorsque l'image filigranée a subi une rotation. A ce stade il reste encore à estimer une translation éventuelle du filigrane, ce que l'ACF ne peut pas faire car elle est invariante aux translations. Pour cela, une intercorrélation entre les bits de référence insérés lors de la génération du bloc initial et le filigrane estimé et préalablement compensé par A^{-1} permet d'estimer le déplacement $\vec{v}$. Enfin l'inversion de l'équation (2) permet de calculer une estimation compensée $\hat{w}'$ du filigrane.

Le modèle visuel

Le modèle visuel utilisé dans notre approche utilise les deux plus importantes propriétés de masquage visuel du HVS: le masquage par les contours et les textures, et le masquage en fonction de la résolution et de la direction.

Masquage par les contours et les textures

L'œil est moins sensible à l'altération des régions qui changent vite, comme les contours des objets et les zones texturées

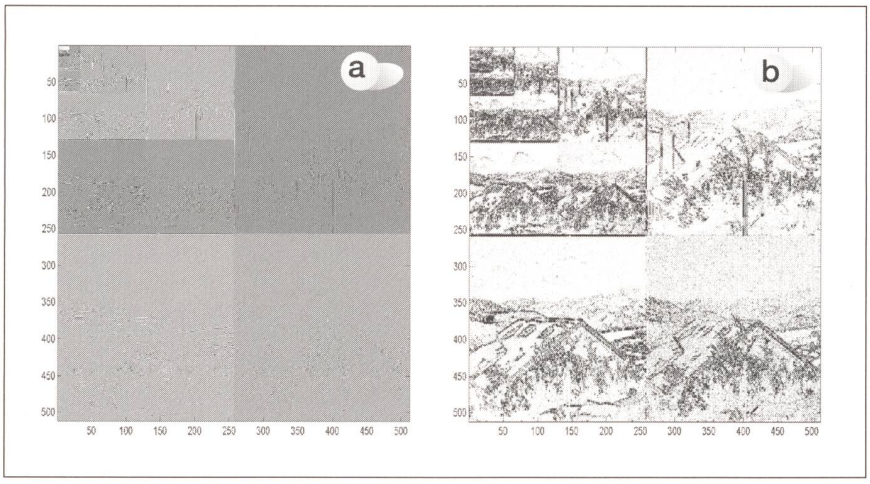

Fig. 8 *a:* Décomposition en ondelettes (DWT) de l'image originale, la décomposant en 5 bandes de résolution et 3 directions pour chacune de ces bandes; la petite image au coin supérieur gauche correspond à la résolution la plus basse. *b:* Fonction de visibilité du bruit (NVF) calculée séparément pour chaque composante de la DWT; remarquez que les contours et les textures, où toute altération est le mieux masquée, sont mis en évidence.

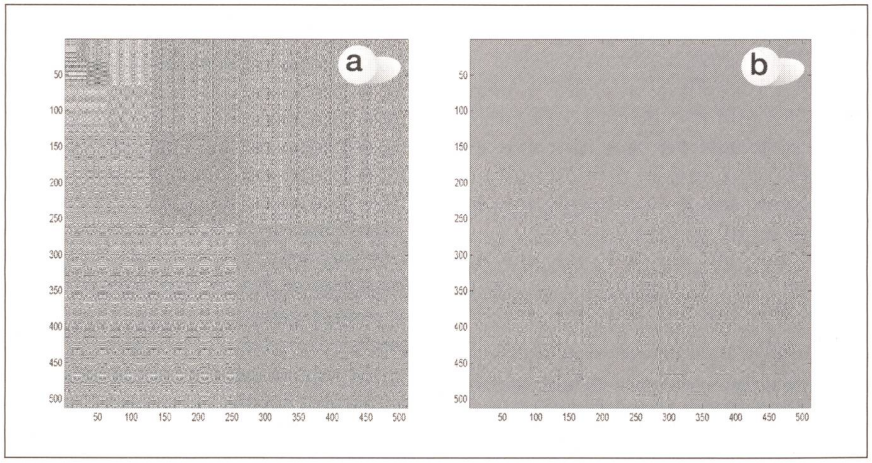

Fig. 9 *a:* La DWT du filigrane. *b:* Le filigrane tel qu'il a été inséré dans l'image, c'est-à-dire la différence amplifiée entre l'image filigranée et l'image originale; l'intensité est accrue au niveau des contours et des textures.

(p. ex. le feuillage d'un arbre). En revanche tout bruit ajouté dans les régions uniformes (p. ex. un ciel bleu) est immédiatement très visible. A partir de ce constat, il est possible de calculer une fonction de visibilité du bruit (noise visibility function, NVF), basé sur une modélisation stochastique de l'image et du bruit, dont la valeur sera faible pour les contours et les textures, et forte dans les régions uniformes. La modulation du filigrane par la NVF permet alors d'accroître l'intensité du filigrane dans les contours et les textures, et de la diminuer dans les régions uniformes.

Masquage selon la résolution et la direction

La sensibilité de l'œil au bruit varie selon sa résolution et selon sa direction. Grossièrement, les hautes ou basses résolutions ainsi que les directions diagonales correspondent à une sensibilité plus faible que les résolutions moyennes et les directions horizontales et verticales. La DWT permet de décomposer l'image en cinq bandes de résolution, et pour chaque bande en trois orientations: horizontale, verticale, et diagonale. L'intensité du filigrane est alors modulée en fonction de chaque bande de résolution et de chaque orientation, de manière à concentrer son énergie principalement dans les bandes et directions où il est le moins visibles.

Les deux types de masquage sont combinés de la manière suivante: d'abord la DWT permet d'obtenir la décomposition en résolutions de l'image. La figure 8a illustre la décomposition DWT de l'image originale. Ensuite la NVF est calculée séparément pour chaque bande et chaque direction de la DWT de l'image, comme illustré par la figure 8b. Le filigrane à insérer est également décomposé par la DWT en cinq bandes. Ensuite, pour chaque bande et direction différente, il est modulé par la NVF; il est multiplié par un facteur de pondération dépendant de la bande et de la direction; il est finalement ajouté à la DWT de l'image originale. L'image filigranée est alors reconstituée par la DWT inverse. La figure 9a montre la DWT du filigrane inséré, et la figure 9b le filigrane tel qu'il apparaît dans le domaine spatial et qui n'est autre que la différence amplifiée entre l'image marquée et l'image originale.

Résultats

La méthode développée est particulièrement robuste, d'une part aux dégradations grâce à l'approche stochastique utilisée pour l'estimation du filigrane, et d'autre part aux distorsions géométriques affines grâce à la structure périodique associée à l'ACF. La petite taille des blocs de base permet le décodage du message à partir d'une petite partie de l'image de l'ordre de 80×80 pixels, ou même 40×40 pixels en l'absence de distorsions géométriques. La méthode résiste à une compression avec pertes à de très fort taux de compression. Par exemple elle résiste à une compression JPEG avec un facteur de qualité (QF) de 40–50% environ, et même à un QF de 10% en l'absence de distorsion géométrique, ce qui correspond dans ce dernier cas à un taux de compression de 66 fois par rapport à la taille avant compression. La méthode présentée est aussi résistante à l'impression sur papier suivi d'une renumérisation sur un scanner, incluant les distorsions géométriques. Le filigrane est correctement décodé même si l'image imprimée à été gribouillée, froissée, déchirée, ou après plusieurs impressions/renumérisations successives. Il n'existe à ce jour aucun algorithme connu présentant ces performances. La figure 10 illustre ces expériences. Elles sont également décrites sur le site Web http://watermark.unige.ch.

Ce projet a été soutenu par divers programmes de recherche suisses et européens (Programme Prioritaire Suisse de Recherches en Structures d'Information et de Communication, projet européen Esprit-Omi-Jedi-Fire, projet européen Certimark). L'entreprise zurichoise Digital Copyright Technologies (DCT) à développé une infrastructure de sécurité et de produits commerciaux utilisant les techniques présentées dans cet article.

Attaques

Il existe beaucoup d'attaques contre les techniques de filigranage. Les attaques peuvent être dirigées soit contre le filigrane lui-même, soit contre le processus de détection du filigrane, soit contre les protocoles ou contre l'infrastructure de sécurité qui entoure le filigranage. Cependant ici deux catégories principales retiennent notre attention: les désynchronisations et les attaques basées sur le traitement du signal.

- Les *désynchronisations* correspondent aux distorsions géométriques que nous avons déjà vues; les déformations peuvent être globalement affines ou non, ou même peuvent varier localement. Elles ne détruisent pas le filigrane, mais rendent difficile la synchronisation du détecteur, d'où la nécessité de méthodes de compensation telle que celle que nous avons détaillée.
- Les *attaques basées sur le traitement du signal* en revanche tendent à affaiblir ou à brouiller le filigrane, en considérant ce dernier comme un bruit à enlever; les filtres simples des logiciels d'édition d'images, l'addition de bruit ainsi que les techniques plus élaborées du type restauration d'image appartiennent à cette catégorie.

Travailler sur les attaques n'est pas seulement l'apanage des pirates, mais permet aussi d'élaborer des méthodes afin d'éprouver la robustesse des algorithmes de filigranage développés. Les premières attaques connues et largement utilisées à cette fin sont essentiellement des attaques par filtrage simple, ou des attaques de désynchronisation comme le programme Stirmark de Fabien Petitcolas [12]. Voici une attaque que nous avons développé, basée sur le traitement du signal, qui associe une approche d'atténuation du bruit de type restauration d'image et une remodulation du filigrane résiduel dans les contours et les textures [13].

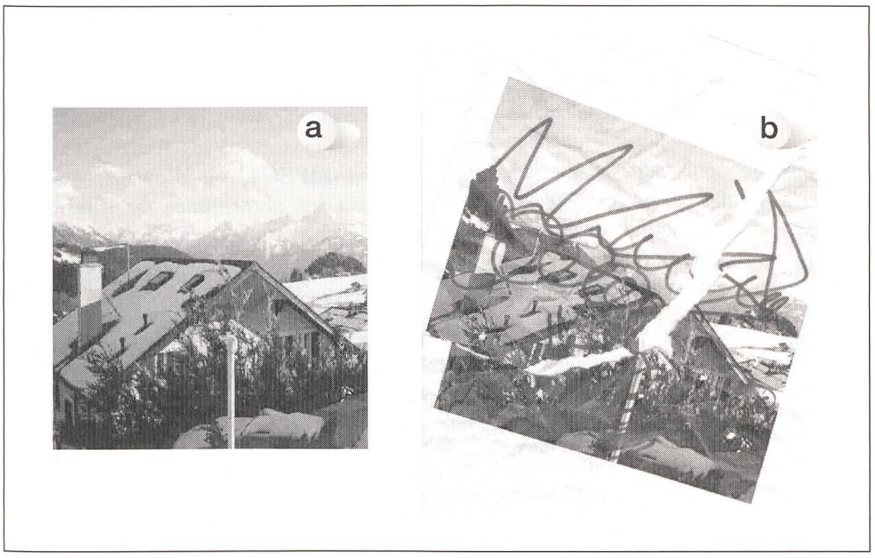

Fig. 10 Exemples d'attaques testées contre notre algorithme. *a:* Compression avec perte au format JPEG avec un facteur de qualité (QF) de 10%, soit 66 fois par rapport à la taille avant compression. *b:* Image scannée après avoir été imprimée et endommagée. Dans les deux cas, le message est décodé sans aucune erreur.

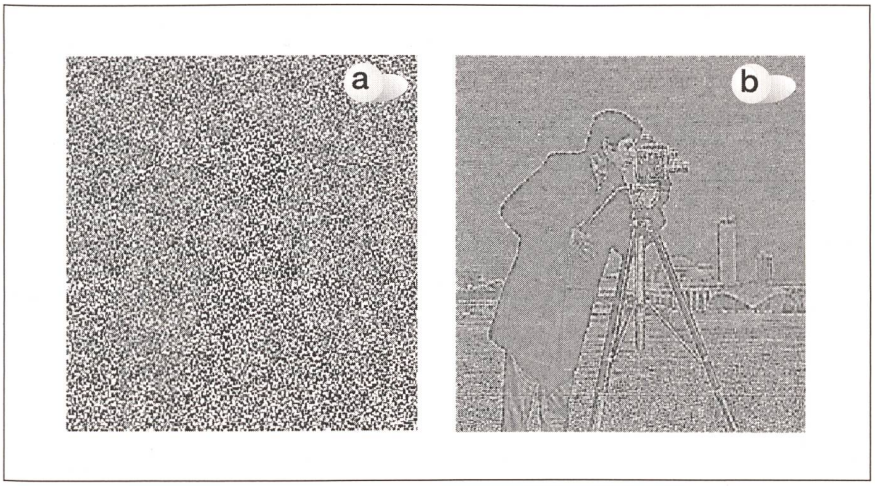

Fig. 11 *a:* Le filigrane avant l'attaque (différence entre l'image filigranée et l'image originale). *b:* Le filigrane après l'attaque (différence entre l'image attaquée et l'image originale); le filigrane restant dans les contours et les textures a été remodulé afin d'empêcher son décodage correct.

Abréviations

CH	Copyright holder
CC	Copyright center
ECC	Error correction code
HVS	Human visual system
LSB	Least significant bits
DFT	Discrete Fourier transform
DCT	Discrete cosine transform
DWT	Discrete wavelets transform
TFM	Transformé de Fourier-Mellin
LPM	Log-polar map
LLM	Log-log map
ACF	Autocorrelation function
NVF	Noise visibility function

Atténuation du bruit et remodulation

L'idée est de réduire la redondance du filigrane, assimilé à un bruit Gaussien, en utilisant des techniques de compression et/ou de suppression du bruit, puis de créer des propriétés statistiques peu favorables au décodage du filigrane. Ceci doit se faire, comme pour le filigranage, en tenant compte des propriétés du HVS afin d'éviter des artefacts visibles. Les étapes sont les suivantes:

Atténuation du bruit

On calcule une estimation de l'image originale $\hat{x}$ à partir de l'image marquée y par le filtre de Wiener/Lee de l'équation (1). $\hat{x}$ est donc une image restaurée, où le bruit est supprimé principalement dans les régions uniformes, mais où les contours et les textures sont préservés (si ce n'était pas le cas, la qualité de l'image serait dégradée).

Remodulation

On calcule une estimation du filigrane $\hat{w}=y-\hat{x}$. Puis on estime le signe du filigrane $s=sign(\hat{w})$. Finalement on remodule le filigrane résiduel dans $\hat{x}$, encore présent surtout dans les contours et les textures, en ajoutant un signal opposé au signe estimé s du filigrane ci-dessus et pondérée par la NVF introduite dans le paragraphe précédent.

La figure 11 montre clairement la suppression du filigrane dans les régions uniformes; comme la remodulation intervient essentiellement au niveau des contours et des textures, elle n'introduit

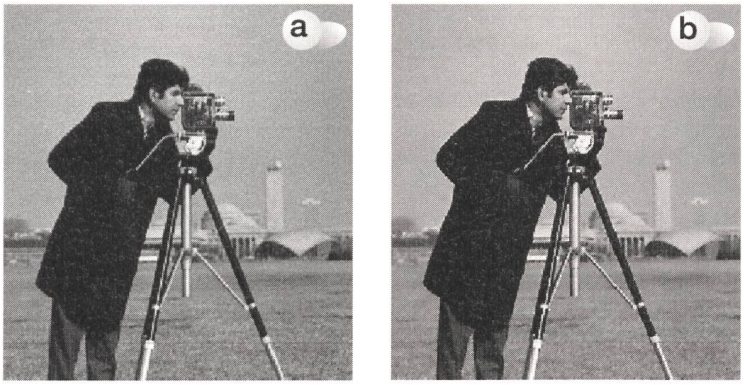

Fig. 12 *a:* **Une image filigranée; un bruit est visible, notamment dans le ciel.** *b:* **L'image attaquée par notre approche d'atténuation du bruit et remodulation; le bruit dans le ciel n'est plus visible, l'attaque a même amélioré la qualité de l'image.**

pas d'artefacts notable. Nous avons constaté que le processus améliore même la qualité de l'image, comme on peut le voir dans la figure 12. Aujourd'hui, encore peu d'algorithmes de filigranage résistent à ce type d'attaque.

Bancs de tests

Les techniques proposées pour le filigranage sont nombreuses, et pour chacune d'entre elles telle ou telle qualité est vantée par ses concepteurs. Travailler sur les attaques permet d'éprouver l'efficacité de ces méthodes. Malheureusement il est actuellement encore très difficile de comparer équitablement les différentes techniques entre elles. Il est donc nécessaire de définir des tests comparatifs (benchmarks) standardisés.

Le logiciel Stirmark [12] est une première proposition d'un tel benchmark. Il s'agit d'un logiciel appliquant une série d'attaques standards, composées de filtres simples (filtre passe-bas, quantification, addition de bruit Gaussien, etc.), et de distortions géométriques (transformations affines, distorsions locales aléatoires). La table I présente un sommaire des résultats obtenus par notre technique de filigranage par rapport à Stirmark version 3.1. Nous obtenons aujourd'hui un score proche de 1, supérieur à celui de tous les algorithmes connus actuellement.

Cependant les attaques de Stirmark ne sont pas représentatives des attaques qu'un pirate peut utiliser. C'est pourquoi le projet européen Certimark propose de créer de nouveaux benchmarks standardisés, incluant des attaques plus puissantes, basées sur des notions de traitement du signal comme celle qui est présentée dans le paragraphe ci-dessus. Ce projet devrait aider au développement de méthodes de filigranage particulièrement robustes. En offrant des protocoles de tests standardisés, il permettra également aux différentes classes d'utilisateurs de connaître les performances des méthodes de filigranage, par là-même de mieux choisir la plus appropriée (et d'accroître leur confiance dans cette technologie).

Attaque	Scores
Rehaussement du signal	1,00
Compression (JPEG/GIF)	0,99
Redimensionnement (changement d'échelle)	1,00
Recadrage (découpage d'une région)	0,99
Cisaillement	1,00
Rotation (auto-recadrage, auto-redimensionnement)	0,99
Suppression de lignes et/ou de colonnes	1,00
Retournement horizontal et/ou vertical	1,00
Déformations locales aléatoires	1,00
Score total	**0,997**

Table I Résultats obtenus par la technique présentée de filigranage en regard de Stirmark version 3.1, pour 6 images tests. Chaque ligne correspond à une série d'attaques standard, appartenant à la catégorie indiquée. Les scores sont notés de 0 (aucun filigrane décodé) à 1 (filigrane décodé pour toutes les attaques).

Conclusion

Le filigranage digital est un domaine récent et en constante évolution. La recherche a beaucoup avancé ces deux dernières années, notamment en ce qui concerne la robustesse et la visibilité des filigranes. Les approches sont de moins en moins empiriques, et celles qui sont basées sur une modélisation stochastique et/ou une décomposition par ondelettes offrent actuellement les meilleures performances connues. Des produits commerciaux de filigranage existent déjà, et bien que des progrès restent à faire, nous ne sommes plus très loin d'applications réellement robustes et sûres.

L'application du filigranage aux vidéos peut bénéficier des dernières techniques développées pour les images. Cependant le filigranage de vidéo constitue encore un challenge, car il ajoute des contraintes de traitement en temps réel d'un important flux de données. Par conséquent les standards actuels de la vidéo numérique tels que MPEG/MPEG2, et surtout les futurs standards comme MPEG4, ou d'autres, devront intégrer des algorithmes de filigranage efficaces, notamment qui évitent une décompression complète du flux vidéo.

Les applications du filigranage sont innombrables, qu'il s'agisse des données multimédia telles que le son et la musique, les images, la vidéo, mais aussi les objets tridimensionnels utilisés pour les images de synthèse, les textes, les bases de données, les logiciels, etc. Des objets matériels peuvent aussi être marqués, par exemple les passeports, les papiers valeurs (billets de banque), les puces électroniques, etc. Les enjeux économiques du filigranage sont considérables, que ce soit en matière de protection ou de sécurité des données, ou pour toutes autre application liée au commerce électronique.

Références

[1] *B. Macq, I. Pitas:* Special Issue on Watermarking. Signal Processing, vol. 66 n° 3, Mai 1998.

[2] *B. Macq:* Identification and Protection of Multimedia Information. Special Issue, Proceedings ot the IEEE, vol. 87 n° 7, juillet 1999.

[3] *M. Kutter:* Digital image watermarking: hiding information in images. Thèse de doctorat, EPFL, Lausanne, 1999.

[4] Digital Watermarking, Special Feature, IEEE Signal Processing Magazine, vol. 17 n° 5, septembre 2000.

[5] *S. Katzenbeisser, F. A. P. Petitcolas:* Information hiding: Techniques for Steganography and Digital Watermarking. Ed. Artech House, 2000.

[6] *V. Cappellini, M. Barni, F. Bartolini:* Information Theoretic Issues in Digital Watermarking. Special Issue, Signal Processing, 2001 (parution prochaine).

[7] *S. Mallat:* A theory for multiresolution signal decomposition: the wavelet representation. IEEE Trans. Pami, vol. 11, pp. 674–693, 1989.
[8] *S. Voloshynovskiy, F. Deguillaume, T. Pun:* Content adaptive watermarking based on a stochastic multiresolution modelling. Eusipco 2000, Tampere, Finlande, 2000.
[9] *J. K. Ó'Ruanaidh, T. Pun:* Rotation, scale and translation invariant spread spectrum digital image watermarking. Signal Processing, 66(3):303–317, 1998.
[10] *S. Pereira, J. K. Ó'Ruanaidh, F. Deguillaume, G. Csurka, T. Pun:* Template based recovery of Fourier-based watermarks using log-polar and log-log maps. Dans Int. Conference on Multimedia Computing and Systems, Special Session on Multimedia Data Security and Watermarking, 1999.
[11] *S. Pereira, T. Pun:* Fast robust template matching for affine resistant watermarks. Dans 3rd International Information Hiding Workshop, Dresde, 1999.
[12] *F. Petitcolas:* http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/. Stirmark 3.1(79), 1999.
[13] *S. Voloshynovskiy, S. Pereira, A. Herrigel, N. Baumgärtner, T. Pun:* A generalized watermark attack based on stochastic watermark estimation and perceptual remodulation. Editeurs Ping Wah Wong et Edward J. Delp, IS&T/Spie's 12th Annual Symposium, Electronic Imaging 2000: Security and Watermarking of Multimedia Content II, vol. 3971 des Spie Proceedings, San Jose, Californie, 2000.
[14] *S. Voloshynovskiy, S. Pereira, V. Iquise, T. Pun:* Attack modelling: towards a second generation benchmark. Signal Processing, Special Issue: Information Theoretic Issues in Digital Watermarking, 2001 (parution prochaine).

Digitale Wasserzeichen

Digitale Verfahren verdrängen die analogen Techniken zusehends. Neben vielen Vorzügen weisen sie aber auch Nachteile auf: Durch die vielfältigen, einfachen und praktisch kostenlosen Kopiermöglichkeiten lassen sich leicht Raubkopien erstellen, die sich von den Originalen kaum unterscheiden. Verletzungen der Autorenrechte (Copyrights) sind so nur sehr schwer nachzuweisen. Abhilfe schaffen digitale Wasserzeichen. Dazu wird zusätzliche Information in das zu schützende Original eingefügt. Diese Information wird dabei nicht in einem speziellen Sektor plaziert, sondern die Daten selber werden durch Algorithmen modifiziert. Die Qualität des Originals soll dabei nicht beeinträchtigt werden, und die Verfahren müssen so robust sein, dass das Wasserzeichen nicht durch Attacken modifiziert werden kann.

Adresse des auteurs

Université de Genève, Département d'informatique, 24, rue Général Dufour, 1211 Genève: Dr assistant *Frédéric Deguillaume* (frederic.deguillaume@cui.unige.ch); Dr *Shelby Pereira* (shelby.pereira@cui.unige.ch); *Maribel Madueno,* assistente de recherche; Prof. Dr *Thierry Pun* (thierry.pun@cui.unige.ch).; Prof. assistant *Sviatoslav Voloshynovskiy* (sviatoslav.voloshynovskiy@cui.unige.ch).

Die HYUNDAI Wirtschaftswunder.

Weniger Preis, mehr Ausstattung, neuer Turbodiesel, 3 Jahre Garantie.

H-1 2500 TDI Van mit 2.5 l Turbodiesel Intercooler für Fr. 25'990.–

H-1 2400 Combi Deluxe mit 4'600 oder 5'700 l Ladevolumen

H100 2400 Van Deluxe: 5'650 l Ladevolumen

H100 Camionnette mit 2.5 l Turbo-Diesel

Ich möchte ☐ einen Nutzfahrzeug-Prospekt ☐ eine Probefahrt

Vorname/Name

Strasse/Nr. PLZ/Ort

Senden an: HYUNDAI AUTO IMPORT AG, Steigstrasse 28, 8401 Winterthur, Tel. 052 208 26 33, Fax 052 208 26 29. Oder an Ihren HYUNDAI-Vertreter.

Nettopreise inkl. MWSt.

www.hyundai.ch

Alles dabei HYUNDAI

HYUNDAI-EFL-Leasing – Finanziert Ihr Fahrzeug diskret und schnell. Leasing oder Darlehen, Telefon 052 208 26 40
Koreas Nummer 1 – inkl. 3 Jahre Werkgarantie oder 100'000 km und HYUNDAI EuroService!