CH 694 233 A5

(19) CONFÉDÉRATION SUISSE
INSTITUT FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE

(11) CH 694 233 A5

(51) Int. Cl.[7]: G 07 D 007/00

Brevet d'invention délivré pour la Suisse et le Liechtenstein
Traité sur les brevets, du 22 décembre 1978, entre la Suisse et le Liechtenstein

(12) FASCICULE DU BREVET A5

(21) Numéro de la demande: 01832/00

(22) Date de dépôt: 20.09.2000

(24) Brevet délivré le: 30.09.2004

(45) Fascicule du brevet publié le: 30.09.2004

(73) Titulaire(s):
AlpVision SA, Rue du Clos 12
1800 Vevey (CH)

(72) Inventeur(s):
Martin Kutter, chemin des Combes 17a
1802 Corseaux (CH)
Frédéric Jordan, Les Rosalys 121
1619 Les Paccots (CH)
Roland Meylan, avenue de Senalèche 23B
1009 Pully (CH)

(74) Mandataire:
Leman Consulting S.A., 62, route de Clémenty
1260 Nyon (CH)

(54) Procédé d'application et de reconnaissance d'un filigrane numérique surimprimé.

(57) Cette invention décrit une technique de filigrane numérique permettant de cacher des informations invisibles par surimpression en utilisant une technique dite de modulation d'amplitude asymétrique. Cette technique peut être appliquée à tout type de matériau imprimé comme du papier, des emballages ou toute autre surface. Des informations visibles peuvent également être imprimées pardessus le filigrane. Un document papier comportant ce filigrane permet de garantir son authenticité car une copie supprime la signature.

Description

L'accès conditionnel aux données numériques sur moyen de stockage comme les CD-ROM ou les disquettes est un problème important et comprend en particulier le problème de la protection contre le piratage. De nombreuses approches ont déjà été proposées, elles sont basées sur des solutions logicielles ou matérielles. Par exemple, dans le cas des disquettes, une solution matérielle consiste à percer le disque de minuscules trous. Une copie de la disquette est détectée par l'absence de ces trous.

Le cryptage à clés secrètes ou clés publiques fournit une solution logicielle pour crypter des données numériques. Les applications des technologies de cryptage sont par exemple la protection des données personnelles, la vérification de l'intégrité des données ou l'authentification de la source des données.

Une autre technique logicielle dans le domaine de la sécurité est connue sous le nom de filigrane numérique ou tatouage numérique. Il s'agit de techniques permettant de cacher des informations de manière robuste et imperceptible dans des données multimédia telles que la musique, la vidéo, la télévision, les images, les documents, etc. L'information qui est cachée s'appelle la signature. Cette signature peut être par exemple un numéro ou un nom et l'on parle alors d'image signée, de vidéo signée, etc.

«Cacher» comporte un sens bien spécifique dans ce contexte: par exemple dans le cas d'une image, on changera légèrement la couleur de certains pixels, et dans le cas d'une musique on modifiera un peu le son de temps à autre.

«Imperceptible» veut simplement dire que les modifications introduites sont telles que l'on ne peut pas distinguer les données originales des données signées. Par exemple, une image signée doit avoir exactement la même apparence qu'une image normale, une musique signée doit sembler tout à fait normale, de même pour une vidéo ou n'importe quelle autre donnée multimédia. Tout le problème consiste à faire en sorte qu'un ordinateur soit capable de détecter cette information cachée alors qu'elle échappe à nos sens. Il existe aussi des applications ou un filigrane visible est acceptable voire même souhaitable. Cela permet notamment d'augmenter encore la robustesse et de permettre un contrôle visuel de la présence d'un filigrane. Le principe qui demeure est que le filigrane ne doit pas être dérangeant visuellement.

La «robustesse» d'un filigrane signifie que l'on doit pouvoir retrouver la signature après n'importe quelle manipulation de données multimédia signées. Prenons par exemple le cas d'une image signée: on doit pouvoir la comprimer, l'imprimer, la scanner, ou la tourner sans jamais perdre la signature. Il faut cependant noter que dans certaines applications il est parfois souhaitable de limiter la robustesse, cela permet alors de détecter des modifications apportées au média protégé. En effet, une altération ou une copie du média se traduira alors par un échec de la lecture du filigrane numérique.

C'est précisément cette propriété qui est mise en œuvre dans le présent brevet. Un exemple typique d'application consiste à empêcher la contrefaçon de papiers de valeurs comme les billets de banque.

De nombreuses publications ont été faites sur les différentes techniques permettant de cacher un tatouage dans une image, dans une vidéo ou un signal audio. En ce qui concerne les images, ces dernières peuvent se classer en fonction de la technique utilisée pour le marquage: certaines opèrent des modifications directement dans le domaine spatial [1], d'autres opèrent ces modifications dans un domaine transformé (par exemple le domaine fréquentiel) voire des domaines intermédiaires comme les ondelettes (voir [2]).

Ces techniques peuvent également être utilisées pour le marquage de vidéo, moyennant certaines adaptations. D'autres techniques spécifiquement dédiées au marquage de vidéo sont aussi possibles en définissant de nouveaux domaines transformés comme les sous-bandes 3D ou les vecteurs de mouvements (par exemple, cf. [3] et [4]).

L'invention concerne un procédé permettant de cacher un filigrane numérique en utilisant une technique de surimpression. Les méthodes de tatouage habituelles, qui sont entièrement calculées dans le domaine digital, cachent toujours le filigrane en augmentant ou en diminuant l'intensité des couleurs de certains points.

La technique de surimpression consiste à cacher un filigrane en l'imprimant par-dessus les couleurs propres du matériau et donc sans tenir compte des variations locales des couleurs à la surface de ce matériau. Cette approche impose que les valeurs des composantes de couleur du matériau signé ne peuvent qu'être assombries puisque de l'encre supplémentaire est ajoutée. Mathématiquement, cela correspond donc à une modulation asymétrique de la couleur des points.

La difficulté consiste à retrouver le filigrane asymétrique. D'une manière générale, la majorité des techniques de tatouage peuvent extraire l'information de l'image signée sans utiliser l'image originale. Certaines techniques réalisent d'abord une prédiction de ce qu'était l'image originale à partir de l'image signée et peuvent ensuite en déduire quelle est la signature. Cette technique est encore applicable dans le cas présent mais l'asymétrie de la modulation conduit à un taux d'erreur important qui peut cependant être compensé par une augmentation de la redondance et de l'amplitude de la modulation.

Dans le cas où le matériau possède une couleur initiale uniforme et connue, il est possible de supprimer cette prédiction. C'est en particulier le cas d'une feuille de papier blanc. Cela permet d'augmenter la fiabilité de la détection et donc de diminuer l'intensité, donc la visibilité du filigrane jusqu'à l'extrême limite de sensibilité d'un scanner optique. En conséquence, cela rend très difficile la duplication du matériau signé, par exemple par photocopie: en effet, les pertes propres à tout système de reproduction affaiblissent en général cette signature au-dessous du seuil de détectabilité. Une application consiste à inclure un tel filigrane sur des papiers dont on souhaite éviter la copie, comme des billets de banque par exemple.

Finalement, des informations lisibles peuvent à nouveau être sur-imprimées sur le matériau signé

lui-même. Ces informations peuvent être liées au filigrane. Par exemple, les chiffres clés d'un contrat peuvent ainsi être cachés dans le filigrane du papier et permettre ainsi d'en garantir l'intégrité.

L'invention sera mieux comprise grâce à la description détaillée qui va suivre et qui se réfère aux dessins annexés qui sont donnés à titre d'exemple nullement limitatif, à savoir:

Fig. 1: Procédé de signature d'un matériau en trois étapes.

Fig. 2: Procédé de lecture d'une image uniforme signée en trois étapes.

Fig. 3: Procédé de lecture d'une image non-uniforme signée en trois étapes.

La fig. 1 illustre le procédé de création d'une signature. A partir de la signature 101 et de la clé 102, un filigrane est calculé (110), cette image 103 est ensuite seuillée (120) pour donner une image 104 qui est ensuite ajoutée à l'image du matériau 105 lors de l'opération d'impression (130) pour obtenir l'image finale 106.

La fig. 2 illustre le précédé de lecture d'une image contenant une signature. L'image signée 202 obtenue par scanner est soustraite (220) de l'image originale 203 afin de restituer le filigrane 204, le bit constituant la signature est alors calculé (230) en utilisant la clé 205. Optionnellement, une étape supplémentaire de filtrage (210) de l'image signée 201 peut-être réalisée si des informations visibles ont été imprimées par dessus l'image uniforme signée.

La fig. 3 illustre le procédé de lecture d'une image contenant une signature et une image originale. L'image originale est prédite (310) à partir de l'image signée 301, l'image signée 302 est soustraite (320) de l'image prédite afin de restituer le filigrane 303, le bit constituant la signature 305 est alors calculé (330) en utilisant la clé 304.

Une réalisation de l'invention consiste à utiliser comme base un algorithme de filigrane numérique de type spatial à modulation d'amplitude, comme par exemple celui décrit dans [1]. Dans cette technique, une composante de couleur d'un ensemble de pixels c(k) est modifiée d'une valeur v qui dépend du signe du bit b={–1,1} à cacher ainsi que d'un générateur aléatoire a(k) donnant deux valeurs {–1,1}.

$$c(k)' = c(k) + v.b.a(k) \quad (1)$$

Dans l'équation (1), l'ensemble des points défini par v.b.a(k) constitue le filigrane (fig. 1, étape 1) qui est ajouté à l'image originale c(k) pour donner l'image signée c(k)'. C'est cette dernière qui est alors imprimée.

Dans le cas d'un filigrane en surimpression, ce n'est plus l'image c(k)' mais le filigrane lui-même v.b.a(k) qui est imprimé par dessus une image c(k). La composante c du support (bleu, luminance, etc.) a déjà une valeur initiale o(k) et ne peut qu'être augmentée lors de la surimpression. La formule suivante est alors appliquée:

$$\text{Si } b.a(k) > 0 \text{ alors } c(k)' = o(k) + v.b.a(k) \quad (2)$$
$$\text{sinon } c(k)' = o(k)$$

L'équation (2) est équivalente à seuiller les valeurs du filigrane en ne conservant que les valeurs positives (fig. 1, étape 2) puis à ajouter ces valeurs à l'image à signer (fig. 1, étape 3). Par comparaison avec la formule (1) correspondant à une modulation symétrique de l'amplitude selon le signe de b.a(k), cette technique est qualifiée de «modulation asymétrique d'amplitude». Si le générateur aléatoire a(k) génère le même nombre de valeurs positives et négatives, il en résulte que la moitié des pixels c(k) est modifiée. Si la valeur de v est choisie suffisamment faible et que la finesse d'impression est suffisamment haute (par exemple au-delà de 300 ppi), l'impression de ces points peut être faite de manière invisible.

La nouvelle valeur des points c(k)' peut être mesurée sur la feuille imprimée en utilisant un scanner optique. Deux cas se présentent alors selon que la couleur du matériau est uniforme et connue ou non.

Dans le premier cas, l'information b est alors aisément retrouvée dans la mesure où o(k)=Cste, v et a(k) sont tous connus par avance (fig. 2, étapes 2 et 3). La multiplicité des points modifiés crée une redondance permettant d'assurer la robustesse au bruit de la technique par corrélation statistique.

Cette méthode est généralisable à plusieurs bits b et permet alors de coder n'importe quelle information numérique comme un numéro ou une chaîne de caractères.

Dans le deuxième cas, un filtre de débruitage de type Wiener peut être utilisé pour réaliser une prédiction de o(k) (fig. 3, étape 1). Les étapes suivantes sont alors identiques au cas précédent (fig. 3, étape 2 et 3). L'erreur de prédiction étant notablement plus importante que dans le premier cas, le nombre de bits b codés de cette manière est systématiquement inférieur.

Dans la pratique il peut également être utile d'imprimer des informations visibles par-dessus le filigrane numérique. C'est le cas par exemple d'une feuille blanche de papier qui comporte un filigrane numérique et par dessus laquelle est imprimé un texte. Ceci est réalisable en choisissant des couleurs ou des intensités distinctes pour le filigrane et pour les informations visibles. Il est ensuite possible de filtrer l'image avant la détection du filigrane (fig. 2, étape 1) pour différencier le filigrane du texte imprimé. Une méthode consiste par exemple à utiliser la composante bleue pour le filigrane et à imprimer le texte du document en noir.

[1] M. Kutter, F. Jordan, F. Bossen, «Digital watermaking of color images using amplitude modulation», Journal of Electronic Imaging, vol. 7, n° 2, pp. 326–332, April 1998.

[2] Shelby Pereira, Sviatoslav Voloshynovskiy and Thierry Pun, Optimized wavelet domain watermark embedding strategy using linear programming, In Harold H. Szu and Martin Vetterli eds., Wavelet Applications VII (part of SPIE AeroSense 2000), Orlando, Florida USA, April 26-28 2000.

[3] Video watermarking using motion vectors (filed 01/97, issued 09/99, US5 960 081)

[4] Video watermarking in the compressed domain (filed 08/96, issued 03/97, EP 762 417A2.

Revendications

1. Procédé d'application d'un filigrane numérique sur un support, caractérisé en ce qu'il est basé sur une modulation asymétrique de l'amplitude d'au moins une composante couleur.

2. Procédé selon la revendication 1, caractérisé en ce que la modulation asymétrique du filigrane est déterminée sur la base d'une couleur uniforme du support.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que le support est du papier.

4. Procédé selon l'une des revendications précédentes, caractérisé en ce que des informations liées au filigrane sont appliquées sur le support d'une manière visible.

5. Proeédé selon la revendication 1, caractérisé en ce que la modulation asymétrique est appliquée sur une composante non visible de l'encre.

6. Procédé selon la revendication 1, caractérisé en ce que le support comporte au moins deux faces et qu'un filigrane différent est appliqué sur chacune des faces.

7. Procédé de reconnaissance d'un filigranes obtenu par le procécé selon l'une des revendications 1 à 6, caractérisé en ce qu'il consiste à:
– acquérir numériquement une image signée,
– filtrer ladite image signée par un filtre de débruitage,
– soustraire l'image filtrée à une image uniforme originale pour en extraire le filigrane,
– extraire sur le filigrane une information de signature.

8. Procédé selon la revendication 7, caractérisé en ce que le filigrane est lu au moyen d'un scanner.

9. Procédé de reconnaissance d'un filigrane obtenu par le procédé selon l'une des revendications 1 à 6, caractérisé en ce qu'il consiste à:
– acquérir numériquement une image signée,
– prédire l'image originale,
– soustraire l'image signée à l'image prédite pour en extraire filigrane,
– extraire sur le filigrane une information de signature.

10. Procédé selon la revendication 9, caractérisé eh ce que le filigrane est lu au moyen d'un scanner.

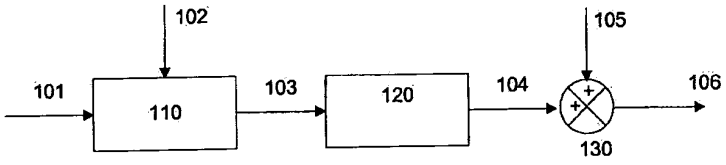

Fig. 1

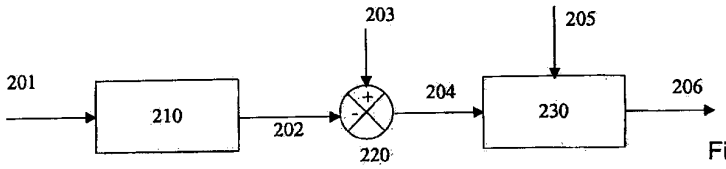

Fig. 2

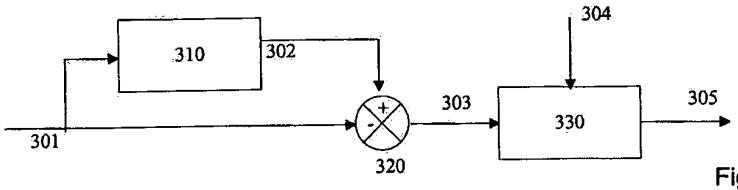

Fig. 3