(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 1 887 565 A1**

(12) **DEMANDE DE BREVET EUROPEEN**

(43) Date de publication:
13.02.2008 Bulletin 2008/07

(51) Int Cl.:
G10L 19/00 *(2006.01)*

(21) Numéro de dépôt: **07301153.8**

(22) Date de dépôt: **27.06.2007**

(84) Etats contractants désignés:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IS IT LI LT LU LV MC MT NL PL PT RO SE SI SK TR
Etats d'extension désignés:
AL BA HR MK YU

(30) Priorité: **11.07.2006 FR 0652919**

(71) Demandeur: **FRANCE TELECOM**
75015 Paris (FR)

(72) Inventeurs:
- **Develle, Olivier**
  21360, CUSSY-LA-COLONNE (FR)
- **Le Guyader, Alain**
  22300 LANNION (FR)
- **Gilloire, André**
  22300 LANNION (FR)

(54) **Procédé et dispositif de détection d'un identificateur de tatouage dans un signal audio**

(57) L'invention concerne un procédé et un dispositif de détection d'un identificateur de tatouage dans un signal audio. Le procédé de l'invention met en oeuvre une méthode de recouvrement par bloc pour effectuer un calcul de corrélation par une méthode de transformation rapide. Les valeurs de corrélation obtenues sont comparées à un seuil pour détecter le début d'un identificateur de tatouage.

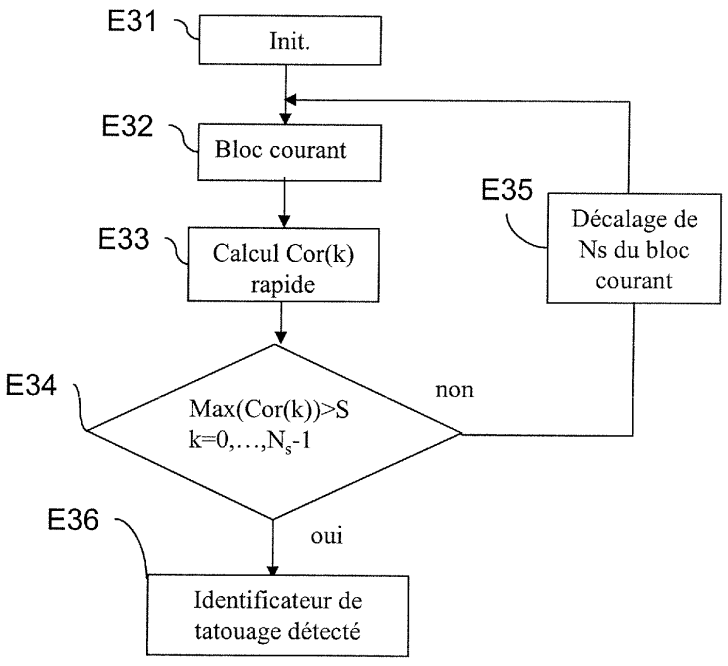

Fig.3

EP 1 887 565 A1

Description

[0001] L'invention se rapporte à un procédé et à un dispositif de détection d'un identificateur de tatouage ou de marque dans un signal audiovisuel et notamment un signal audio.

[0002] Le tatouage permet de transmettre une information additionnelle dans des données support de manière imperceptible. Pour des données audiovisuelles cela revient à établir un canal de communication de données dissimulé, en parallèle avec l'infrastructure classique de transport de l'information.

[0003] Un des principaux avantages du tatouage est que les données auxiliaires sont dissimulées et attachées au signal et par la même sont capables de supporter des changements de format et de fréquence d'échantillonnage donnant au tatouage une interopérabilité au niveau des terminaux et des réseaux, seules les extrémités au niveau de la détection devant être compatibles avec l'insertion.

[0004] Une trame du canal de communication dissimulé dans le signal porteur est par exemple constituée d'une marque de synchronisation que l'on peut également appeler identificateur de tatouage, suivie du message inséré dans le signal, le début du message étant indiqué par l'identificateur de tatouage.

[0005] Après transmission du signal tatoué, à la lecture du media, la détection consiste d'abord à détecter l'identificateur de tatouage qui a été inséré en début de trame. Une fois cet identificateur repéré dans le contenu audio par exemple, la détection des bits du message peut commencer. Les séquences "identificateur de tatouage + message éventuel" sont insérées en continu dans le média, les débuts d'identificateur coïncidant avec les zones d'énergie suffisante propices à l'insertion. En réception la détection de chaque séquence se fait également en continu permettant ainsi de se resynchroniser en cas de coupure dans le média porteur (édition du signal, coupures par un pirate ou encore pertes de trames de la transmission).

[0006] Les identificateurs de tatouage ainsi que les messages sont formés à partir de séquences aléatoires gaussiennes issues d'un générateur de nombres aléatoires ou de séquences Pseudo-Aléatoires (Pseudo-Noise Séquences en Anglais ou séquences PN) générées par un registre à décalage dont les cellules sont bouclées de façon à produire une séquence de sortie de longueur maximale. Toute autre séquence aléatoire issue de la théorie des machines à états finis (séquences de Gold, codes de Baker, séquences de Walsh, ...) peut convenir à condition que sa fonction de corrélation soit proche d'une distribution de Dirac. Dans la suite de la description, nous parlerons de séquences aléatoires aussi bien pour désigner des séquences aléatoires que des séquences pseudo-aléatoires.

[0007] Une procédure classique de génération d'un signal tatoué est illustrée à la figure 1. Ainsi, le module 11 permet de générer une séquence aléatoire de longueur N à partir d'une valeur d'initialisation K fixée à l'avance. On obtient ainsi une séquence aléatoire w(n).

[0008] Dans le cas où on veut transmettre un bit d'information 0 ou 1, cette séquence est modulée par l'information à transmettre en la multipliant par 1 si le bit à transmettre est 1 et par -1 si le bit à transmettre est 0. Cette étape de génération est effectué dans le module 12 et génère une séquence modulée $\pm w(n)$.
Dans le cas où on veut juste insérer un identificateur de tatouage, la séquence aléatoire n'est pas modulée.

[0009] Un modèle psycho-acoustique 13 est pris en compte par le module 14 pour générer l'identificateur de tatouage ou le message $w_f(n)$ de façon à le rendre inaudible. Une étape d'ajustage par un gain est effectuée en 15. Cet identificateur de tatouage ou ce message est ensuite additionné en 16 au signal audio s(n) pour former le signal tatoué $s_w(n)$.

[0010] Ce signal est soit stocké sur un média pour lecture ultérieure par un lecteur soit transmis sur un réseau de transmission fixe, mobile ou de diffusion.
En réception l'identificateur de tatouage doit être détecté pour agir sur le signal reçu, par exemple en bloquant le lecteur en cas de détection de contenu piraté.

[0011] Une procédure classique de détection d'identificateur de tatouage est illustré en figure 2.

[0012] Le signal audio tatoué $s_w(n)$ est d'abord blanchi par filtrage inverse par le module 21 (correspondant à l'inverse de la prise en compte du modèle psycho-acoustique). L'opération de détection de la présence de l'identificateur de tatouage et du contenu de la trame elle-même est ensuite effectuée par calcul de corrélation par le module 22 entre le signal filtré $x_w(n)$ et la séquence aléatoire w(n) générée par le module 23 de la même façon que lors de l'insertion.

[0013] Cette détection détermine soit un repère de trame k_s lors de la détection du l'identificateur de tatouage, soit les bits de l'information insérée.

[0014] Ne connaissant pas l'instant de début de trame dans le signal porteur, le calcul de corrélation se fait de manière glissante. On parle alors d'intercorrélation glissante.

[0015] Cette méthode consiste à effectuer un calcul de corrélation entre les échantillons du signal tatoué et la séquence aléatoire pour chaque décalage d'un échantillon du signal tatoué, jusqu'à ce que le début de l'identificateur de tatouage soit révélé par le fait que le coefficient de corrélation *Cor(k)* dépasse un seuil *S.* Pour chaque instant d'échantillonnage k , le coefficient de corrélation est donné par:

$$Cor(k) = \sum_{n=0}^{N-1} x_w(n+k)\, w(n) \quad k = 0,...,k_s \qquad (1)$$

[0016] Une fois le début de trame détecté, un seul calcul de corrélation suffit pour détecter le message:

$$Cor_m = \sum_{n=0}^{N_m-1} x_w(n)\, w(n) \qquad (2)$$

sur N_m échantillons du signal porteur pour un bit de message. Le bit détecté sera 0 si la corrélation message Cor_m est négative, il sera de 1 dans le cas contraire.

[0017] Il apparaît donc que pour détecter la position de l'identificateur de tatouage, c'est-à-dire l'instant où le message a été inséré il est nécessaire d'effectuer une intercorrélation pour chaque échantillon du signal porteur jusqu'à ce que l'identificateur soit trouvé. Pour des valeurs de *N* importantes, la recherche de l'identificateur est donc longue et complexe alors que la détection du bit émis se fait rapidement.

[0018] A titre d'exemple, pour une valeur de *N* égale à 4096 et une fréquence d'échantillonnage de 44100 Hz, le nombre de multiplications à effectuer par seconde sera de 18010^6 multiplications par seconde, ce qui est largement supérieur à la capacité des processeurs du commerce.

[0019] Il est donc important de réduire cette complexité de calcul pour la recherche de l'identificateur de tatouage dans le signal porteur notamment pour une mise en oeuvre dans des terminaux mobiles.

[0020] Par ailleurs, certaines techniques de calcul de corrélation rapides et efficaces sont décrites dans l'état de l'art.

[0021] Le document A. Alrutz, M. R. Schroëder "A fast Hadamard transform method for the évaluation of measurement using pseudo random test signals". Proceeding of the 11th conférence on acoustics, Paris, 1983, décrit une méthode qui permet de calculer efficacement les intercorrélations. Cette méthode s'applique dans le cas où on a inséré une séquence aléatoire de façon périodique.

[0022] La propriété qui est exploitée pour calculer la corrélation est l'application renouvelée et de façon cyclique de la séquence aléatoire.

[0023] Cette méthode ne s'applique donc pas au cas où on désire détecter le début d'une trame de tatouage qui représente l'identificateur de tatouage dans un système de tatouage audio.

[0024] En effet, un seul identificateur étant inséré à la fois, mais à plusieurs endroits du signal porteur, par exemple toutes les 10 à 50 secondes, et dans un endroit propice à la détection, l'application de la méthode d'Hadamard cité dans le présent document engendrerait dans le calcul du vecteur de corrélation, des termes de repliement parasites d'autant plus importants que le décalage entre le bloc d'analyse du signal tatoué et la séquence insérée est grand. Ces termes de repliement proviennent du produit du vecteur de signal tatoué par la diagonale inférieure de la matrice de la séquence aléatoire décalée circulairement. Les éléments de cette diagonale sont égaux à la séquence aléatoire repliée, pris dans un ordre miroir inverse d'où l'appellation "termes de repliement". Ces termes parasites, qui n'existent pas quand la séquence aléatoire est périodique comme utilisée dans le document d'Alrutz et Schroeder, diminueraient la valeur du pic de corrélation dans le cas d'une séquence aléatoire non périodique affectant ainsi la fiabilité de la détection de l'identificateur.

[0025] D'autres techniques d'insertion et de détection de tatouage qui améliorent la rapidité du calcul de corrélation lors de la détection existent. Dans la demande de brevet WO 2004/010376, le tatouage est inséré dans le domaine de Fourier, la marque fréquentielle est ajoutée au signal après un décalage lié de façon biunivoque avec l'identificateur inséré. Le signal tatoué dans le domaine temporel est obtenu par transformée de Fourier inverse. En détection chaque trame est passée dans le domaine fréquentiel par transformée de Fourier. Plusieurs trames de coefficients de Fourier sont accumulées, le résultat de l'accumulation étant corrélé avec la marque fréquentielle. Le maximum de la corrélation donne la valeur du décalage donc le contenu du message de la trame. Le maximum de corrélation est calculé par transformée de Fourier inverse du produit de la transformée de Fourier du signal accumulé par le conjugué de la transformée de Fourier de la marque fréquentielle. Cette méthode nécessite de nombreux passages d'un domaine fréquentiel à un domaine transformé du domaine fréquentiel et inversement, l'insertion s'effectuant dans le domaine fréquentiel.

[0026] La présente invention offre une solution qui ne présente pas ces inconvénients en proposant un procédé de détection d'un identificateur de tatouage qui minimise le nombre d'opérations à effectuer et la complexité des calculs tout en permettant une décision fiable.

[0027] Le procédé selon l'invention offre la possibilité d'utiliser des algorithmes rapides de calcul de corrélation qui ne nécessitent pas d'insertion périodique de marques de synchronisation.

[0028] Le procédé selon l'invention peut être mis en oeuvre en temps réel sur des processeurs de faible capacité et dans le cas d'une réception en continu d'un signal tatoué.

[0029] A cet effet, l'invention propose un procédé de détection d'un identificateur de tatouage dans un signal audio, l'identificateur de tatouage ayant été inséré dans le signal audio à partir d'une séquence aléatoire d'une longueur de N échantillons, N étant multiple de Ns, obtenue par au moins une valeur d'initialisation. Le procédé est tel qu'il comporte les étapes suivantes:

- préparation d'un bloc courant de N échantillons à partir du signal tatoué;
- calcul de corrélation par une méthode de transformation rapide entre les échantillons du bloc courant et ceux de la séquence aléatoire obtenue à partir de la au moins une valeur d'initialisation;
- comparaison à un seuil prédéterminé des valeurs de corrélation issues du calcul de corrélation des Ns premiers échantillons;
- itération des étapes précédentes avec un bloc courant décalé par rapport au bloc précédent de Ns échantillons tant que le maximum des dites valeurs de corrélation n'est pas supérieure au seuil prédéterminé, le maximum des valeurs de corrélation supérieur au seuil prédéterminé indiquant le début de l'identificateur de tatouage

[0030] Ainsi, cette méthode de recouvrement par bloc, conjointement à la mise en oeuvre d'une méthode de transformation rapide, diminue le nombre de calcul de corrélation et la complexité de ce calcul par rapport au calcul de corrélation par fenêtre glissante effectué échantillon par échantillon.

[0031] De plus, une telle méthode permet d'effectuer une scrutation rapide du signal tatoué ne serait ce que pour détecter l'existence d'un tatouage.

[0032] Dans un mode particulier de réalisation l'identificateur de tatouage indique la position dans le signal audio d'un message inséré.

[0033] Ainsi, la détection de l'identificateur de tatouage permet de savoir où la détection du message inséré peut être effectuée.

[0034] L'étape de préparation de bloc courant comprend dans un mode préféré de réalisation, une étape de filtrage inverse du signal tatoué et une étape de filtrage de Wiener utilisant un filtre calculé à partir d'une fonction de corrélation d'une séquence d'apprentissage de l'identificateur de tatouage.

[0035] Ainsi, la prise en compte de certaines caractéristiques de la séquence utilisée pour insérer l'identificateur de tatouage permet d'améliorer la détection de l'identificateur de tatouage par l'accentuation des pics éventuels de détection.

[0036] Selon un mode de réalisation, la au moins une valeur d'initialisation est une clé (K_a) qui permet de générer la séquence aléatoire.

[0037] Dans un autre mode de réalisation, la séquence aléatoire est obtenue par deux valeurs d'initialisation, la première étant une première clé (K_a) permettant de générer une séquence aléatoire intermédiaire, la seconde étant une seconde clé (K_b) permettant de crypter la séquence aléatoire intermédiaire pour obtenir la séquence aléatoire.

[0038] L'utilisation d'une deuxième clé apporte donc une sécurité accrue.

[0039] Dans un premier mode de réalisation, la méthode de transformation rapide est une méthode du type d'Hadamard qui comporte les étapes suivantes:

- permutation des échantillons du bloc courant selon une première table de permutation;
- application de la transformée d'Hadamard aux échantillons ainsi permutés;
- permutation des échantillons du vecteur résultant de la transformée d'Hadamard selon une seconde table de permutation pour obtenir les valeurs de corrélations.

[0040] L'utilisation de la méthode d'Hadamard dans le procédé conforme à l'invention est particulièrement bien adaptée. Le procédé ainsi réalisé permet de s'affranchir des termes de repliement.

[0041] Avantageusement, le procédé comporte une étape préalable d'initialisation dans laquelle les première et seconde tables de permutation ainsi que la séquence aléatoire sont calculées et mémorisées.

[0042] Dans un mode particulier de réalisation, le calcul de la séquence aléatoire, de la première et de la seconde table de permutation est optimisé par un nombre minimum d'opérations binaires réalisées sur les bits d'un entier représentant dans chaque cas le registre à décalage de génération de la séquence ou de la table.

[0043] La méthode de recouvrement de l'invention permet dans un second mode de réalisation d'utiliser une méthode de type de Fourier comme méthode de transformation rapide. Cette méthode comporte les étapes suivantes:

- application d'une transformée de Fourier au bloc courant;
- calcul d'un produit sur les échantillons résultant de la transformée du bloc courant et ceux du complexe conjuguée de la séquence aléatoire ayant subi une transformée de Fourier;
- application d'une transformée inverse de Fourier pour obtenir les valeurs de corrélation.

[0044] Avantageusement, le procédé comporte une étape d'initialisation dans laquelle la transformée de Fourier de la séquence aléatoire et son complexe conjugué sont calculés et mémorisés.

[0045] Pour améliorer la détection, le procédé comporte en outre une étape de correction des valeurs de corrélation par élimination de termes parasites.

[0046] Dans une variante de réalisation utilisant la méthode de type transformée de Fourier, le procédé comporte les étapes suivantes:

- segmentation en sous-séquences du bloc courant;
- segmentation en sous-séquences de la séquence aléatoire, la deuxième moitié de la sous-séquence aléatoire étant mise à zéro;
- application d'une transformée de Fourier aux sous-séquences du bloc courant et aux sous-séquences de la séquence aléatoire;
- calcul de corrélations partielles par le produit sur les échantillons résultant de la transformée des sous-séquences du bloc courant et ceux du complexe conjugué des sous-séquences de la séquence aléatoire;
- sommation des corrélations partielles calculées;
- application d'une transformée de Fourier inverse à la somme issue de l'étape de sommation pour obtenir les valeurs de corrélation.

[0047] Cette variante permet de s'affranchir de l'utilisation d'une transformée de Fourier de grande taille lorsque l'identificateur de tatouage a une taille importante.

[0048] Dans une seconde variante, le procédé comporte les étapes suivantes:

- segmentation en sous-séquences du bloc courant;
- segmentation en sous-séquences de la séquence aléatoire, la première moitié de la sous-séquence aléatoire étant mise à zéro;
- application d'une transformée de Fourier aux sous-séquences du bloc courant et aux sous-séquences de la séquence aléatoire;
- calcul de corrélations partielles par le produit sur le complexe conjugué des échantillons résultant de la transformée des sous-séquences du bloc courant et ceux des échantillons résultant de la transformée des sous-séquences de la séquence aléatoire;
- sommation des corrélations partielles calculées;
- application d'une transformée de Fourier inverse à la somme issue de l'étape de sommation pour obtenir les valeurs de corrélation.

[0049] L'invention vise également un dispositif de détection d'un identificateur de tatouage dans un signal audio, l'identificateur de tatouage ayant été inséré dans le signal audio à partir d'une séquence aléatoire d'une longueur de N échantillons, N étant multiple de Ns, obtenue par au moins une valeur d'initialisation. Le dispositif est tel qu'il comporte:

- des moyens de préparation d'un bloc courant de N échantillons à partir du signal tatoué;
- des moyens de calcul de corrélation par une méthode de transformation rapide entre les échantillons du bloc courant et ceux de la séquence aléatoire obtenue à partir de la au moins une valeur d'initialisation;
- des moyens de comparaison à un seuil prédéterminé des valeurs de corrélation issues du calcul de corrélation des Ns premiers échantillons;
- des moyens d'obtention d'un nouveau bloc courant par décalage de Ns échantillons par rapport au bloc précédent mis en oeuvre tant qu'une des dites valeurs de corrélation n'est pas supérieure au seuil prédéterminé.

[0050] Le dispositif ainsi décrit est apte à mettre en oeuvre le procédé selon l'invention.

[0051] L'invention vise enfin un programme d'ordinateur comprenant des instructions de code pour la mise en oeuvre des étapes du procédé selon l'invention, lorsque ledit programme est exécuté par un processeur.

[0052] Le dispositif et le programme d'ordinateur présentent les mêmes avantages que le procédé qu'ils mettent en oeuvre.

[0053] D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante, donnée uniquement à titre d'exemple non limitatif, et faite en référence aux dessins annexés, sur lesquels:

- la figure 1 représente un schéma bloc d'une méthode d'insertion de l'état de l'art;
- la figure 2 représente un schéma bloc d'une méthode de détection de l'état de l'art;
- la figure 3 illustre sous forme d'organigramme, les principales étapes d'un procédé de détection d'identificateur de tatouage conforme à l'invention;

- les figures 4a et 4b illustrent la méthode par recouvrement selon l'invention;
- la figure 5 représente les principaux modules d'un dispositif d'insertion d'identificateur de tatouage;
- la figure 6 représente les principaux modules d'un dispositif de détection d'identificateur de tatouage selon l'invention;
- la figure 7 illustre sous forme d'organigramme, une méthode de cryptage qui peut être utilisée par l'invention;
- la figure 8 illustre de façon détaillée, sous forme d'organigramme, l'étape de calcul de corrélation dans un premier mode de réalisation de l'invention;
- la figure 9 illustre de façon détaillée, sous forme d'organigramme, l'étape de calcul de corrélation dans un second mode de réalisation de l'invention;
- la figure 10 illustre une variante de réalisation du second mode de réalisation selon l'invention; et
- la figure 11 illustre un dispositif mettant en oeuvre le procédé selon l'invention.

[0054] La **figure 3** illustre les principales étapes d'un procédé de détection d'identificateur de tatouage conforme à l'invention.

[0055] L'étape E31 est une étape d'initialisation qui peut permettre d'effectuer des calculs au préalable et de les mémoriser comme par exemple la génération de la séquence aléatoire.

[0056] L'étape E32 consiste à préparer un premier bloc courant du signal tatoué filtré comportant un nombre N d'échantillons.

[0057] Avant d'obtenir le bloc courant, une lecture d'un bloc de Ns échantillons du signal tatoué, N étant multiple de Ns, est effectuée. Ce bloc de Ns échantillons $s_w(n)$, n=0,.., N_s-1 est celui qui est disponible en lecture sur le disque de stockage ou reçu directement par flux continu.

[0058] Ce bloc est blanchi par un filtrage inverse suivi d'un filtrage adaptatif pour donner un vecteur de signal $x_w^{sub}(n), n = 0,...,N_s - 1$. Cette étape de filtrage correspond à l'étape inverse du filtrage par le modèle psycho-acoustique effectué lors de l'insertion.

[0059] Ce vecteur de signal est mis à la suite des vecteurs précédemment reçus pour constituer le bloc courant de N échantillons $x_w(n)$,n=,0,...,N-1.

[0060] L'étape E32 est suivie de l'étape E33 dans laquelle un calcul de corrélation par une méthode de transformation rapide est effectué sur les échantillons du bloc courant et les échantillons de la séquence aléatoire générée à partir de la (des) même(s) valeur(s) d'initialisation utilisée(s) lors de l'insertion. Cette génération de séquence aléatoire peut s'effectuer juste avant le calcul de la corrélation ou bien à l'étape d'initialisation. Elle est alors dans ce dernier cas mémorisée à l'étape d'initialisation et lue lors de l'étape de calcul.

[0061] A l'étape E34, un test est effectué pour savoir si le maximum des valeurs de corrélation issues du calcul de corrélation de l'étape E33 des Ns premiers échantillons est supérieur à un seuil S.

[0062] Dans le cas où le maximum des valeurs de corrélation est supérieur au seuil S, alors l'identificateur de tatouage est détecté. Cette valeur du maximum de corrélation supérieure au seuil S indique alors le début de l'identificateur de tatouage.

[0063] Le dispositif de détection peut alors à partir de cet identificateur de tatouage déterminer la position dans le signal audio d'un message qui aurait été inséré. Ce message est placé juste après le dernier échantillon de l'identificateur de tatouage représenté par la séquence aléatoire de longueur N.

[0064] La détection du message inséré s'effectue de façon simple comme mentionné en référence à la figure 2, par un seul calcul de corrélation. Une fois le message détecté, le détecteur repart dans le mode de recherche de la synchronisation ou de l'identificateur de tatouage afin de repérer le message suivant. Dans le cas où seuls des identificateurs de tatouage ont été insérés à des endroits définis du signal, la scrutation du signal tatoué s'opère comme dans le cas précédent en continu. Quand un identificateur est détecté, un drapeau se met à 1 et le détecteur repart en mode scrutation.

[0065] Dans le cas où à l'étape E34, aucune des valeurs de corrélation des Ns premiers échantillons ne dépassent le seuil S, alors un nouveau bloc courant est pris en compte par décalage de Ns échantillons en E35.

[0066] Les **figures 4a et 4b** illustrent de façon schématique le procédé de l'invention.

[0067] Le signal tatoué représenté en 40 est reçu en continu. L'identificateur de tatouage issu d'une séquence aléatoire de longueur N est constituée de R blocs de Ns échantillons, soit de N=R*Ns échantillons. Cet identificateur de tatouage est représenté en grisé sous la référence 41 sur les figures 4a et 4b. Une analyse par bloc de N échantillons est effectuée. Ce bloc courant $x_w(n)$ pour n allant de 0 à N-1 est référencé sur la figure en 42. Un calcul de corrélation est effectué entre ce bloc courant et la séquence aléatoire w(n) générée comme lors de l'insertion. On compare ensuite les valeurs de corrélation obtenue pour les Ns premiers échantillons comme représenté en 43 sur les figures 4a et 4b. Si le maximum des valeurs de corrélation ne dépasse le seuil S alors on effectue un décalage du bloc courant à analyser d'un nombre Ns d'échantillons comme illustré sur les figures 4a et 4b.

[0068] Quand un nouveau bloc du signal tatoué de Ns échantillons est disponible par lecture sur disque de stockage (comme par exemple CD, DVD, mémoire amovible) ou reçu en flux continu, il subit une étape de filtrage inverse et de

filtrage de Wiener pour donner un vecteur de signal $\overline{x}_w^{sub}(n), n = 0,..., N_s - 1$. Il est inséré à la place des Ns dernières composantes de droite comme représenté sur les figures 4a et 4b.

[0069] Pour passer au nouveau bloc courant, le bloc précédent est décalé vers la gauche de Ns échantillons et le bloc $\overline{x}_w^{sub}(n), n = 0,..., N_s - 1$ de signal filtré est placé dans sa partie droite. C'est ce qui est indiqué sur la figure 4b où le bloc analysé en 42 devient le bloc courant. On constate sur la figure 4b que l'identificateur inséré représenté en grisé en 41 s'est décalé de N_s échantillons vers la gauche par rapport au bloc précédent représenté en 42 sur la figure 4a (et qui était le bloc courant de l'étape précédente).

[0070] Sur cette figure 4b, on constate que le calcul de corrélation donne une valeur supérieure au seuil sur les Ns premiers échantillons. Ceci indique donc la position k_s du début de l'identificateur de tatouage. On peut alors en déduire la fin de l'identificateur de tatouage connaissant sa longueur N pour éventuellement détecter un message qui aurait été inséré après l'identificateur.

[0071] Avec cette méthode d'analyse par recouvrement, un exemple de calcul de la corrélation est donné par l'expression suivante:

$$Cor(k) = \sum_{n=0}^{N-1} w(n+k)x_w(n) \qquad \text{k=0,...,N-1} \qquad (3)$$

[0072] L'équation précédente peut alors s'écrire sous la forme matricielle suivante:

$$\begin{bmatrix} Cor(0) \\ Cor(1) \\ Cor(2) \\ Cor(3) \\ . \\ Cor(n-2) \\ Cor(n-1) \end{bmatrix} = \begin{bmatrix} w(0) & w(1) & . & w(N-2) & w(N-1) \\ w(1) & w(2) & & w(N-1) & w(0) \\ w(2) & w(3) & . & w(0) & w(1) \\ w(3) & w(2) & & w(1) & w(2) \\ . & . & . & . & . \\ w(N-2) & w(N-1) & . & w(N-4) & w(N-3) \\ w(N-1) & w(0) & . & w(2) & w(N-2) \end{bmatrix} \begin{bmatrix} x_w(0) \\ x_w(1) \\ x_w(2) \\ x_w(3) \\ . \\ x_w(N-2) \\ x_w(N-1) \end{bmatrix} \qquad (4)$$

[0073] Soit en notation matricielle:

$$\overline{Cor} = \overline{w}_c \, \overline{x}_w \qquad (5)$$

La matrice $\overline{w}_c$ est une matrice circulante construite à partir de sa première ligne w^T, T étant l'opérateur de transposition.

[0074] Du fait que l'identificateur de tatouage n'est pas inséré périodiquement, la moitié inférieure de la matrice $\overline{w}_c$ va donner lieu à des termes de repliement parasites dans le produit matriciel. Pour éviter cela, le procédé selon l'invention applique un recouvrement de $N_s = N / R$ échantillons et calcule le maximum du coefficient de corrélation sur les N_s premières valeurs du vecteur de corrélation $\overline{Cor}$ comme décrit précédemment en référence aux figures 3, 4a et 4b.

[0075] Si la séquence était insérée périodiquement, à n'importe quel endroit où on se placerait dans un bloc de signal tatoué, on aurait une séquence aléatoire entière de N points (en fait une des lignes de la matrice w_c). Le décalage optimal serait donné par la ligne de la matrice qui donne le maximum du produit scalaire $w_c \, x_{w,}$ égal à N dans le cas idéal. Dans notre cas, seule une séquence de N échantillons est insérée à la fois. Par exemple, si on suppose que la séquence commence à l'échantillon n=-1 dans le signal tatoué, le maximum de corrélation sera trouvé pour la deuxième ligne de la matrice w_c. Il y aura un terme parasite donné par le w(0) en fin de ligne. Pour n = -2 le max est donné par la troisième ligne. Il y a deux termes parasites w(1) et w(0) (séquence inversée) et ainsi de suite. L'utilisation du recouvrement permet de limiter l'influence des termes parasites en ne prenant que les Ns premiers termes de la corrélation.

[0076] Dans un exemple où R=8192/1424 =8, à la place d'avoir un maximum de corrélation de N on aura un maximum de N*(8192-1)/8192= N*0.9998, si on a un décalage de 1 et de N*(8192-1024)/8192= N*0.875 dans le cas le plus défavorable d'un décalage de N_s=1024.

[0077] Pour effectuer le produit scalaire de façon performante, la séquence de la première ligne de la matrice $\overline{w}_c$ peut être prise égale à une séquence PN de longueur maximale auquel cas on aura:

$$N = 2^{Ms} - 1 \qquad (6)$$

[0078] Les valeurs usuelles de *Ms* sont de 12 et de 13 ce qui donne des séquences de synchronisation de taille 4095 et de 8191.

[0079] En référence à la **figure 5**, nous allons à présent décrire un dispositif d'insertion d'un identificateur de tatouage. Ce dispositif comporte un module d'obtention d'une séquence aléatoire w(n) à partir d'au moins une valeur d'initialisation.

[0080] Ainsi, la séquence aléatoire peut être obtenue à partir d'une seule valeur d'initialisation, par exemple, une première clé K_a. Cette première clé K_a va permettre dans un premier mode de réalisation de générer directement la séquence aléatoire w(n) utilisée pour générer l'identificateur de tatouage. Dans ce cas, le module de cryptage 53 n'est pas présent.

[0081] Dans un deuxième mode de réalisation, le module de cryptage 53 est présent. L'obtention de la séquence aléatoire w(n) utilisée pour générer l'identificateur de tatouage s'effectue à partir de deux valeurs d'initialisations. La première est par exemple une première clé K_a qui va permettre de générer une séquence aléatoire intermédiaire $w_s(n)$, la deuxième est une deuxième clé K_b qui va permettre de crypter cette séquence aléatoire intermédiaire pour obtenir la séquence aléatoire w(n).

[0082] La séquence aléatoire w(n) obtenue par le module 51 va servir comme dans le dispositif d'insertion de la figure 1 à générer l'identificateur de tatouage par le module 54. Un modèle psycho-acoustique 55 est également pris en compte ainsi qu'un gain 56 pour être additionné en 57 au signal audio s(n) et former le signal tatoué $s_w(n)$.

[0083] La **figure 6** représente un dispositif de détection d'un identificateur de tatouage conforme à l'invention. Ce dispositif de détection tout comme le dispositif d'insertion comporte un module d'obtention de la séquence aléatoire qui a été utilisée pour générer l'identificateur de tatouage.

[0084] De la même façon que pour le dispositif d'insertion, ce module d'obtention de séquence aléatoire 61 peut dans un premier mode de réalisation ne comporter qu'un module de génération de la séquence aléatoire w(n) à partir de la première clé K_a ou comporter à la fois le module 62 de génération d'une séquence aléatoire intermédiaire $w_s(n)$ à partir de la première clé K_a et un module 63 de cryptage de cette séquence intermédiaire à partir de la deuxième clé K_b pour obtenir la séquence aléatoire w(n).

[0085] Ainsi, le dispositif de détection ne pourra détecter l'identificateur de tatouage que s'il connaît la ou les deux clés utilisées pour l'obtention de la séquence aléatoire.

[0086] Un exemple d'application possible dans le mode de réalisation avec une seule clé est par exemple d'associer à chaque contenu audio, un numéro d'utilisateur ou d'opérateur comme identificateur de tatouage. La clef sera déduite de ce numéro par l'intermédiaire d'une table de correspondance. Ainsi, dans le contexte de vente en ligne sécurisée de contenu audio, l'identificateur de tatouage permet de déceler les transferts ou échanges abusifs de contenu et de tracer l'origine du problème. En effet, en présence d'un contenu piraté trouvé sur un site Web, l'entité détentrice des clefs utilisateurs peut tester la détection de l'identificateur de tatouage pour chacune des clés. Celle qui permettra de détecter l'identificateur de tatouage sera donc celle qui appartient à l'utilisateur qui est à l'origine de la diffusion abusive. La détection étant très rapide, la recherche peut être effectuée rapidement pour un grand nombre de clés.

[0087] Dans le cas où l'identificateur de tatouage n'est pas utilisé seul mais est suivi d'un message, la clef de l'identificateur permet d'affirmer que le signal est tatoué lorsque la présence de l'identificateur est détectée. Dans ce cas la possibilité de détection du message peut être conditionnée par la connaissance de la même clef que celle de l'identificateur. Cependant, la clef identificateur et la clef message peuvent être différentes.

[0088] Le mode de réalisation avec deux clés, ouvre un champ d'application encore plus large et apporte une sécurité supplémentaire.

[0089] La clé K_b peut représenter un numéro de commande relative à un utilisateur ou un revendeur et la clef K_a peut être propre au propriétaire de l'oeuvre ou à une société opérant pour plusieurs opérateurs. Dans ce cas la fuite de contenus piratés peut être localisée de la façon suivante: étant donné un contenu piraté, le tiers de confiance détenteur de la clef K_a va rechercher, pour toutes les clefs K_b, celle qui donne une réponse positive en détection et qui sera donc à l'origine de la fuite.

[0090] Dans une application de contrôle d'accès dans un lecteur, la clé K_a représente un numéro d'utilisateur et la clé K_b, le numéro de l'oeuvre. Il est alors possible de tester si le numéro d'oeuvre de la licence de droit d'accès correspond à celui qui a effectivement été inséré par tatouage. Si le résultat du test est négatif, alors le contenu est piraté et le

lecteur est bloqué.

[0091] On peut remarquer également que l'une des clés peut être publique, par exemple K_b tout en gardant K_a secrète. Dans ce cas, si la clef K_b représente un numéro de contenu, elle permet de donner l'accès à ce contenu. L'association des séquences audio aux clefs K_b peut être connue de tous, par exemple par l'intermédiaire d'une base de données disponible sur internet.

[0092] Le dispositif de détection comprend également un module de filtrage référencé en 64 pour blanchir et égaliser le signal tatoué lors de la réception et ainsi former un vecteur de signal $x_w^{sub}(n)$.

[0093] Le signa $\overline{s}_w$ est d'abord filtré par un filtre inverse $A(z)$ ne comportant des coefficients qu'au numérateur. Ce filtre est calculé à partir des coefficients de corrélation du masque psychoacoustique du signal par l'algorithme de Levinson-Durbin. Ensuite, à partir du signal $\overline{s}_{wz}$ ainsi filtré, on va calculer un filtre de Wiener $F_w(z)$ qui va essayer de modéliser $\overline{w}$ par filtrage linéaire de $\overline{s}_{wz}$. En fait la minimisation entre la marque $\overline{w}$ et son estimée à partir du signal $\overline{s}_{wz}$ conduit à la résolution des équations suivantes:

$$R_{wx}\, F_w = R_{dx}$$

[0094] Où R_{wx} est une matrice de Toëplitz formée à partir de la fonction d'autocorrélation du signal $\overline{s}_{wz}$ et R_{dx} un vecteur de corrélation calculé à partir d'une séquence d'apprentissage. Comme séquence d'apprentissage on peut prendre à titre d'exemple la séquence w à différents échantillons de départ ou offset. La fonction de corrélation est ensuite calculée pour des décalages allant de 0 à M_k,M_k étant le nombre de coefficients du filtre. Le signal filtré résultant $x_w^{sub}(n)$ sera donné par:

$$x_w^{sub}(n) = \sum_{j=-M_k}^{M_k} F_w(j)\, s_{wz}(n-j)$$

[0095] L'utilisation d'un filtre de Wiener calculé à partir d'une séquence d'apprentissage permet d'améliorer la détection de l'identificateur de tatouage par rapport à une méthode n'utilisant qu'un filtrage inverse.

[0096] En effet, la séquence d'apprentissage permet de prendre en compte certaines caractéristiques de la séquence w et ainsi d'accentuer les pics éventuels de détection.

[0097] Le module de détection par corrélation 65 comprend des moyens de préparation d'un bloc courant de N échantillons du signal tatoué filtré, des moyens de calcul de corrélation entre les échantillons du bloc courant et la séquence aléatoire w(n) et des moyens de comparaison des valeurs de corrélation obtenues à un seuil S.

[0098] Ces moyens permettent la mise en oeuvre du procédé décrit en figure 3 conformément à l'invention.

[0099] Le cryptage effectué à la fois dans le module 53 et le module 63 sur une séquence aléatoire $w_s(n)$ peut être réalisé par permutation aléatoire des échantillons de la séquence $w_s(n)$ ou par une méthode de cryptage comme celle décrit par exemple dans le document B. Schneier "Applied cryptography, protocols and sources in C". John Wiley & sons, inc., 1996 p397 et 398.

[0100] Un exemple de cryptage par permutation est illustré par l'algorithme représenté en **figure 7**.

[0101] Le coeur de l'algorithme consiste à calculer une matrice de permutation au moyen d'une clef de 16 octets soit 128 bits.

[0102] Un tableau TabS est d'abord initialisé à l'étape E71 aux valeurs de 0 à N-1. Une table TabK de taille 256 octets est initialisée à l'étape E72 par répétition, autant de fois que nécessaire, du contenu de la table de clé Key contenant les 16 octets de la clé. L'entier CurPos est initialisé à 0.

[0103] Aux étapes E73 à E75, pour chaque indice i de 0 à N-1, un indice CurPos est généré aléatoirement par addition de CurPos, de TabS d'indice i et de TabK d'indice i modulo 256, la table TabK étant de taille 256, le tout étant pris modulo N. Ensuite, aux étapes E77 à E79, la table de permutation qui va servir à brouiller ou crypter la séquence aléatoire est obtenue en permutant les deux valeurs qu'elle contient à l'indice curpos et à l'indice i en s'aidant de la variable intermédiaire TmpVal.

[0104] On se retrouve donc avec une table de permutation qui contient pour $i = 0, ..., N-1$, le rang de l'échantillon qui doit être permuté. Pour brouiller la séquence aléatoire, il suffit maintenant de lire la table de permutation TabS(i) pour i = 0, N - 1 et de permuter le contenu de w_s d'indice i avec le contenu de w_s d'indice TabS(i). La séquence cryptée, calculée une fois pour toute peut être stockée en mémoire.

[0105] Une méthode de génération d'une séquence PN est par exemple une méthode telle que décrite dans le document B. Schneier. "Applied cryptography, protocols and sources in C". John Wiley & sons, inc., 1996, pages 372 à 375. Les points de bouclage du registre sont donnés par le polynôme générateur de la séquence.

[0106] A titre d'exemple, pour le cas *Ms* =12, un des polynômes générateur primitif est donné par poly(x) = 1 + x + x^4 + x^6 + x^12 soit poly=ca0 en hexadécimal ou encore 1100 1010 0000 en binaire. Les points de bouclage correspondent alors aux bits égaux à 1 dans la décomposition binaire de poly.

[0107] Une façon de générer une séquence PN de façon optimale avec un minimum d'opérations binaires est maintenant décrite. Les coefficients du polynôme générateur de puissance élevée sont en correspondance avec les bits de poids faible du registre à décalage, le bit de sortie étant en poids fort.

[0108] Le code descriptif de cette méthode est donné ci-dessous:

```
int state;
N = 1 << Ms) - 1
int poly = 0xca0;
state = 1;
w[0] = -2 * (state >> (Ms - 1) & 1) + 1;
for(i = 1; i < N; i++)
 {
 state = ((state << 1) & N) | (xor(poly & state)&1);
 w[i] = -2 * (state >> (Ms - 1) & 1) + 1;
}
```

[0109] L'entier state contient l'état courant du registre à décalage, chaque cellule du registre étant représentée par un emplacement binaire de l'entier state. Il est initialisé à 1. Pour le calcul de l'état state à l'instant suivant, le contenu state est décalé vers la gauche de la position d'un bit, on effectue ensuite un masque en faisant une opération binaire "et" du résultat avec N l'entier contenant M_s bits de poids faible à 1. Il ne reste plus qu'à insérer en position de bit de poids faible, par addition au moyen d'une opération binaire "ou", l'opération de "ou exclusif' (xor) des bits du produit bit à bit de l'état du registre avec le polynôme générateur (poly & state).

[0110] La fonction xor(n) calcule un ou exclusif des bits de l'entier n en argument.

[0111] La méthode décrite précédemment permet d'obtenir la séquence à partir d'une implantation du registre à décalage par une seule ligne de code ne nécessitant que peu d'opérations binaires: une opération de "décalage", trois opérations "et", une opération "ou" et une opération "ou exclusif" et ce quel que soit le polynôme générateur. En effet, ces opérations sont effectuées sur les bits d'un entier représentant dans chaque cas le registre à décalage de génération de la séquence.

[0112] Dans l'état de l'art, par exemple la référence de Schneier citée précédemment page 375, l'implantation du registre à décalage version Fobinacci demande plus d'opérations binaires: sept opérations de "décalage", deux opérations "et", une opération "ou" et cinq opérations "ou exclusif'.

[0113] Cette séquence PN ainsi générée est utilisable par exemple dans le premier mode de réalisation décrit en référence à la figure 8.

[0114] La figure 8 illustre de façon détaillée, sous forme d'organigramme, l'étape de calcul de corrélation E33 de la figure 3 dans le cas d'un premier mode de réalisation de l'invention. Ce premier mode de réalisation utilise la méthode de transformée rapide d'Hadamard comme méthode de transformation rapide.

[0115] Ainsi, à l'issue de l'étape E32, un bloc courant $x_w(n)$ de N échantillons a été préparé.

[0116] L'opération suivante E81 consiste à permuter le vecteur $\bar{x}_w(n)$, c'est-à-dire à le ré indicer en fonction d'une première permutation Pe. A l'issue de cette étape de permutation, on obtient un vecteur $xe(i)$, $i = 0,..., N-1$.

[0117] Un exemple de code implémentant cette fonction est le suivant:

```
xe[0] = 0;
for (i = 0; i < N; i++)
  xe[TabPe[i]] = xw[i];
 }
```

[0118] La transformée d'Hadamard est ensuite appliquée à l'étape E82 au vecteur $xe(i)$, $i = 0,..., N-1$. On peut retrouver une explication de la méthode d'Hadamard dans le document A. Alrutz, M. R. Schroëder "A fast Hadamard transform method for the evaluation of measurement using pseudo random test signals", Proceeding of the 11th conference on acoustics, Paris, 1983.

[0119] Un exemple de mode opératoire de la transformée d'Hadamard est présenté ci-dessous:

```
void FastHadamard(double *x, long N)
```

```
    {
    long i, il, j, k, k1, k2;
    double temp;
    Kp = (1<<N)-1;
    k1 = Kp;
    for (k = 0; k < N; k++)
       {
      k2 = k1 >> 1;
      for (j = 0; j < k2; j++)
          {
          for (i = j; i < Kp; i = i + k1)
              {
              il = i + k2;
              temp = x[i] + x [i1] ;
               xe[i1] = xe[i] - xe[i1];
              xe[i] = temp;
              }
          }
      kl = k1 >> 1;
      }
}
```

[0120] L'étape E82 est suivie de l'étape E83 dans laquelle une seconde permutation Ps est appliquée au vecteur résultant de la transformée d'Hadamard, afin d'obtenir les valeurs de corrélation correspondant à l'ordre des instants d'échantillonnage de départ.

[0121] Un exemple de code implémentant cette fonction est le suivant:

```
for (i = 0; i < N-1; i++)
 {
  cor[i] = xe[TabPs[i]];
 }
cor[N-1] = 0;
```

[0122] A l'issue de l'étape E83, on obtient des valeurs de corrélation Cor(k) qui peuvent être utilisées directement à l'étape E34 décrite en référence à la figure 3.

[0123] Dans un mode de réalisation amélioré, une étape E84 de correction est mise en oeuvre.

[0124] En effet, en examinant l'équation (4), on constate que:

- des termes parasites à l'origine du repliement apparaissent à la fin de la matrice carrée. Il s'agit de $w(0)$ sur la deuxième ligne, de $w(0)$ et $w(1)$ sur la troisième ligne, de $w(0)$ $w(1)$ et $w(2)$ sur la quatrième ligne. La contribution $C^-(k)$ de ces termes parasites est à retrancher de $Cor(k)$.
- des termes utiles manquent. En effet la séquence de la deuxième ligne commence à $w(1)$, il manque donc la contribution de $w(0)$. Celle de la troisième ligne commence à $w(2)$, il manque donc la contribution de $w(0)$ et de $w(1)$. La référence de temps étant prise à n=0, ces valeurs sont à pondérer avec le signal tatoué antérieur à la trame courante $x_w(-1)$, $x_w(-2)$, $x_w(-3)$, ... et la contribution $C^+(k)$ de ces termes manquants est à ajouter à $Cor(k)$.

[0125] La contribution $C^-(k)$ est égale à:

$$C^-(k) = \sum_{j=0}^{k-1} w(j)\, x_w(N-k+j) \qquad (7)$$

[0126] Celle de $C^+(k)$ est égale à:

$$C^{+}(k) = \sum_{j=0}^{k-1} w(j)\, x_{w}(-k+j) \qquad (8)$$

[0127] La valeur de la corrélation corrigée sera donnée en fonction de l'intercorrélation non corrigée $Cor^{nc}(k)$ par:

$$Cor(k) = Cor^{nc}(k) + C^{+}(k) - C^{-}(k) \qquad k = 0, ..., N_s - 1 \qquad (9)$$

[0128] Comme nous sommes en situation de recouvrement seuls les N_s premiers coefficients d'intercorrélation sont pris en compte et sont donc à corriger.

[0129] La correction introduite par l'équation (9) est donc appliquée à l'étape E84. A l'issue de cette étape, les valeurs de corrélation corrigées Cor(k) sont comparées à un seuil à l'étape E34 comme décrit en référence à la figure 3.

[0130] Les permutations Pe et Ps sont définies par des tables respectives *TabPe* et *TabPs* qui sont calculées à l'étape d'initialisation E31 de la figure 3.

[0131] La table de permutation *TabPe* à affecter aux valeurs de $\bar{x}_w$ du vecteur de signal d'entrée est calculée par exemple par le code ci-dessous en fonction du polynôme générateur nommé "poly", de la fonction "xor" et de *Ms* le degré du polynôme générateur. Cette table de permutation est ensuite stockée en mémoire.

```
N = (1 << Ms) - 1;
state = 1;

TabPe[0] state;

for(i = 1; i < N; i++)
  {
  state = ((state << 1) & N) | (xor(poly & state) &1);
  TabPe[i] = state;
}
```

[0132] L'état du registre state va prendre toutes les valeurs comprises entre 1 et N-1 mais dans un ordre qui sera caractérisé par la table de permutation. L'état state est d'abord initialisé à 1. Pour calculer l'état state à l'instant suivant, les bits de state à l'instant courant sont décalés vers la gauche d'une position et masqués par l'entier ayant M_s bits de poids faible à 1. On ajoute au résultat de cette opération, en position de bit de poids faible, le résultat du ou exclusif du produit du polynôme par l'état (poly & state) masqué par l'entier 1. Ici de nouveau la séquence de permutation est calculée en faisant appel au nombre minimum d'opérations binaires comme décrit précédemment pour la génération de la séquence PN.

[0133] *TabPs,* la table de la permutation Ps à affecter sur les valeurs de $\bar{xe}$ en sortie de la transformée d'Hadamard est calculée par le code représenté ci-dessous en fonction du polynôme générateur "poly" et de *Ms* le degré du polynôme générateur. Cette table de permutation est ensuite stockée en mémoire.

```
N = (1 << Ms) - 1;
int state = 1 << (Ms - 1);// Initialisation du registre à décalage

TabPs[0] = state;

for(i = 1; i < N; i++)
  {
  state = (state >> 1) ^(poly * (state & 1));
  TabPs[i] =state;
}
```

[0134] La variable d'état du registre state est d'abord initialisée à 2^{Ms}-1. Ensuite, pour calculer l'état state à l'instant suivant, les bits de state à l'instant courant sont d'abord décalés d'une position vers la droite. L'état à l'instant suivant est le résultat de l'opération "ou exclusif' bit à bit du résultat de l'opération précédente avec le produit du polynôme par l'état (poly & state) masqué par l'entier 1. Ici de nouveau la séquence de permutation est calculée en faisant appel au

nombre minimum d'opérations binaires.

[0135] En référence à la **figure 9**, nous allons à présent décrire un second mode de réalisation pour l'étape de calcul de corrélation E33. Dans ce mode de réalisation, la méthode de transformation rapide est une méthode de transformation de Fourier.

[0136] Ainsi, à l'issue de l'étape E32, un bloc courant $\overline{x}_w(n)$ de N échantillons a été préparé.

[0137] L'opération suivante E91 consiste à calculer la transformée de Fourier du vecteur $\overline{x}_w(n)$ pour obtenir la transformée $\overline{X}_w$.

[0138] Dans ce mode de réalisation, le calcul de la corrélation s'effectue selon l'équation (10) suivante:

$$Cor(k) = \sum_{n=0}^{N-1} w(n)\, x_w(n+k) \qquad (10)$$

La transformée de Fourier de *Cor(k)* est donnée par:

$$FFT(\overline{Cor}) = \overline{W}^{*}\ \overline{X}_w \qquad (11)$$

où $\overline{W}^{*}$ et $\overline{X}_w$ sont respectivement les transformées de Fourier de $\overline{w}$ et de $\overline{x}_w$. En conséquence:

$$\overline{Cor} = FFT^{-1}(\overline{W}^{*}\ \overline{X}_w) \qquad (12)$$

[0139] La transformée de la séquence aléatoire $\overline{w}$, qu'elle soit issue d'une séquence générée avec une seule clé ou une séquence générée par une première clé et cryptée par une seconde est soit effectuée lors de l'étape E91, soit effectuée à l'étape d'initialisation puis stockée comme pour l'obtention de la séquence aléatoire.

[0140] Dans le cas où la séquence aléatoire est cryptée, cette séquence n'est pas générée selon le procédé de génération de séquence PN décrit précédemment mais selon une génération de séquence aléatoire basée par exemple sur une génération de nombres aléatoires.

[0141] Lors de l'étape d'initialisation E31, le complexe conjuguée $\overline{W}^{*}$ de la transformée de Fourier $\overline{W}$ est également calculé et stocké en mémoire.

[0142] A l'étape E92, le produit de $\overline{W}^{*}\ \overline{X}_w$ dans le domaine de Fourier est effectué. On obtient ainsi $\overline{Y}(k) = \overline{X}_w(k)\overline{W}^{*}(k)$ pour k allant de 0 à N-1. Puis, à l'étape E93, on applique une transformée de Fourier inverse de ce produit pour en déduire l'intercorrélation comme décrit par l'équation (12).

[0143] On obtient ainsi les valeurs de corrélation Cor(k) que l'on compare à un seuil pour les Ns premiers échantillons comme décrit à l'étape E34 en référence à la figure 3.

[0144] Comme dans le mode de réalisation utilisant la transformation d'Hadamard, des termes parasites apparaissent, ces termes pouvant être éliminés en appliquant la correction décrite par les équations 7, 8 et 9 précédentes.

[0145] Cette façon de procéder, nécessite une FFT de grande taille lorsque l'identificateur de tatouage a une taille importante, par exemple $N = 4096$ ou N = 8192 , cas usuels pour les signaux audionumériques.

[0146] Pour éviter cela, une première variante de réalisation de ce second mode de réalisation est maintenant décrite en référence à la figure 10.

[0147] Cette solution consiste à calculer la corrélation pour des blocs en recouvrement, en segmentant le calcul de la FFT en plusieurs FFT de tailles plus petites, de nouveau en recouvrement. Par exemple pour une taille de 8192, on pourra effectuer R = 8 FFT de taille 1024 et sommer les résultats des intercorrélations partielles.

[0148] La technique proposée consiste à subdiviser la séquence $x_w(n)$ en sous-séquences $x_{wi}(n)$ qui se recouvrent comme suit:

$$x_{wi}(n) = x_w(n + N_s i)\ \ n = 0,1,\cdots,2N_s - 1,\ i = 0,1,\cdots,R-1 \qquad (14)$$

et la séquence $w(n)$ en sous-séquences $w_i(n)$ telles que :

$$w_i(n) = \begin{cases} w(n + N_s i) & n = 0,1,\cdots,N_s - 1 \\ 0 & n = N_s,\cdots,2N_s - 1 \end{cases} \qquad i = 0,1,\cdots,R-1 \quad (15)$$

[0149] On peut remarquer que la séquence $x_{wi}(n)$ i = 0,..., R - 1 comprend en fait N+N_S termes, la dernière sous-séquence étant égale à $x_{w\,R\text{-}1}(n) = x_w(n+N_S(R\text{-}1))$ n = 0,1,$\cdots$2N_S-1

[0150] Pour chaque paire de sous-séquence $x_{wi}(n)$ et $w_i(n)$ de longueur $2N_S$, la séquence $Cor_i(m)$ représentant la corrélation périodique de $x_{wi}(n)$ et $w_i(n)$ est calculée. Ce qui s'écrit avec les séquences originales x_w(n) et $w(n)$:

$$Cor_i(m) = \sum_{n=0}^{N_s-1} x_w(n + iN_s)\, w(n + iN_s + m) \quad m = 0,1,\cdots,N_s \qquad (16)$$

[0151] En sommant ces corrélations partielles sur les R sous-blocs, on obtient la corrélation totale entre les deux séquences. Il existe cependant une méthode plus efficace pour calculer les intercorrélations en passant par la FFT.

[0152] Pour cela on calcule $X_{wi}(k)$ et $W_i(k)$, les FFT des signaux $x_{wi}(n)$ et w_i(n) puis le produit:

$$Y_i(k) = \overline{W}_i^*(k)\ \overline{X}_{wi}(k) \quad (17)$$

[0153] En sommant les contributions sur les R sous-trames de $\overline{Y}_i$ dans le domaine fréquentiel et en effectuant une transformée de Fourier inverse, on obtient l'intercorrélation cherchée:

$$\overline{Cor} = IFFT\left(\sum_{i=0}^{R-1} \overline{Y}_i\right) \qquad (18)$$

[0154] Ainsi, en référence à la **figure 10**, on obtient à l'étape E110 les séquences $\overline{W}_i^*\ i = 0,...,R-1$ supposées avoir été calculées à l'initialisation par FFT de $\overline{w}_i$ défini par l'équation (15).

[0155] Ensuite pour chaque sous-bloc en recouvrement de i=0 E120 à i=R-1 E160, on calcule la transformée de Fourier de $x_{wi}(n)$ à l'étape E130 puis on effectue le produit complexe $\overline{Y}_i = W_i^*\ \overline{X}_{wi}$ à l'étape E140 et on somme le résultat dans le tableau de nombres complexes $\overline{Z}$ à l'étape E150. Lorsque les R contributions de $\overline{Y}_i = W_i^*\ \overline{X}_{wi}$ ont été sommées on sort de la boucle en réponse positive au test E160 et l'intercorrélation s'obtient en calculant la FFT inverse de $\overline{Z}$ à l'étape E170. La taille de la FFT inverse est de 2 N_S.

[0156] Nous allons à présent décrire une seconde variante du second mode de réalisation de l'étape E33 de calcul de corrélation.

[0157] Pour cela, on utilise pour le calcul de l'intercorrélation en recouvrement l'équation (19), l'intercorrélation intervenant cette fois en fonction des échantillons de la séquence retournée de $\overline{x}_w$ (signe - de $x_w(n\text{-}k)$):

$$Cor(k) = \sum_{n=0}^{N-1} w(n)\, x_w(n-k) \qquad (19)$$

La transformée de Fourier de $\overline{Cor}$ sera alors donnée par la relation suivante:

$$FFT(\overline{Cor}) = \overline{W}\ \overline{X}^{*}_{w} \qquad (20)$$

[0158] Pour avoir une valeur de la corrélation sans repliement avec l'intercorrélation utilisant la séquence retournée, il nous faut de nouveau utiliser le recouvrement de:

$$x_{wi}(n) = x_w(n - N_s + N_s i)\ \ n = 0,1,\cdots,2N_s - 1,\ i = 0,\cdots,R-1 \quad (21)$$

et un nouveau partionnement $\overline{w}$ dans lequel les zéros sont introduits au début de bloc et non plus à la fin comme dans l'équation (15):

$$w_i(n) = \begin{cases} 0 & n = 0,1,\cdots,N_s - 1 \\ w(n + N_s i) & n = N_s,\cdots,2N_s - 1 \end{cases} \qquad i = 0,1,\cdots,R-1 \quad (22)$$

[0159] On remarquera que dans le cas présent la séquence $x_{wi}(n)$ i=0,...,R-1 utilisée pour le partitionnement comprend les échantillons $x_w(-N_s+1)$,..., $x_w(-1)$, $x_w(0)$, $x_w(-N_s-1)$.

[0160] Le calcul de la corrélation sera donné par le même procédé que celui décrit en référence à la figure 10, à ceci près que $\overline{w}_i$ est donné par l'équation (22) et que le tableau de complexe $\overline{Y}_i$ est donné à l'étape E 140 par:

$$Y_i(k) = \overline{W}_i(k)\ \overline{X}^{*}_{wi}(k) \qquad (23)$$

[0161] Selon un mode de réalisation choisi et représenté à la **figure 11,** un dispositif mettant en oeuvre l'invention est par exemple un micro-ordinateur 210 qui comporte de façon connue, notamment une unité de traitement 220 équipée d'un microprocesseur, une mémoire morte de type ROM 230, une mémoire vive de type RAM 240. Le micro-ordinateur 210 peut comporter de manière classique et non exhaustive les éléments suivants: un clavier, un écran, un microphone, un haut-parleur, une interface de communication, un lecteur de disque, un moyen de stockage...

[0162] La mémoire morte 230 comporte des registres mémorisant un programme d'ordinateur PG comportant des instructions de programme adaptées à mettre en oeuvre un procédé de détection d'identificateur de tatouage selon l'invention tel que décrit en référence à la figure 3. Ce programme PG est ainsi adapté à préparer un bloc courant de N échantillons d'un signal tatoué reçu en entrée 250, à effectuer un calcul de corrélation par une méthode de transformation rapide entre les échantillons du bloc courant et ceux de la séquence aléatoire obtenue à partir d'au moins une valeur d'initialisation reçu en entrée 260 et à comparer les valeurs de corrélations résultantes à un seuil pour en déduire la position de l'identificateur de tatouage en sortie 270.

[0163] Lors de la mise sous tension, le programme PG stocké dans la mémoire morte 230 est transféré dans la mémoire vive qui contiendra alors le code exécutable de l'invention ainsi que des registres pour mémoriser les variables nécessaires à la mise en oeuvre de l'invention.

[0164] De manière plus générale un moyen de stockage, lisible par un ordinateur ou par un microprocesseur, intégré ou non au dispositif, éventuellement amovible, mémorise un programme mettant en oeuvre le procédé de détection d'identificateur de tatouage selon l'invention.

Revendications

1. Procédé de détection d'un identificateur de tatouage dans un signal audio, l'identificateur de tatouage ayant été inséré dans le signal audio à partir d'une séquence aléatoire d'une longueur de N échantillons, N étant multiple de Ns, obtenue par au moins une valeur d'initialisation, le procédé étant **caractérisé en ce qu'**il comporte les étapes suivantes:

    - préparation d'un bloc courant de N échantillons à partir du signal tatoué;
    - calcul de corrélation par une méthode de transformation rapide entre les échantillons du bloc courant et ceux

de la séquence aléatoire obtenue à partir de la au moins une valeur d'initialisation;
- comparaison à un seuil prédéterminé des valeurs de corrélation issues du calcul de corrélation des Ns premiers échantillons;
- itération des étapes précédentes avec un bloc courant décalé par rapport au bloc précédent de Ns échantillons tant que le maximum des dites valeurs de corrélation n'est pas supérieure au seuil prédéterminé, le maximum des valeurs de corrélation supérieur au seuil prédéterminé indiquant le début de l'identifïcateur de tatouage

2. Procédé selon la revendication 1, **caractérisé en ce que** l'identificateur de tatouage indique la position dans le signal audio d'un message inséré.

3. Procédé selon l'une quelconque des revendications 1 ou 2, **caractérisé en ce que** l'étape de préparation de bloc courant comprend une étape de filtrage inverse du signal tatoué et une étape de filtrage de Wiener utilisant un filtre calculé à partir d'une fonction de corrélation d'une séquence d'apprentissage de l'identificateur de tatouage.

4. Procédé selon l'une quelconque des revendications 1 à 3, **caractérisé en ce que** la au moins une valeur d'initialisation est une clé (K_a) qui permet de générer la séquence aléatoire.

5. Procédé selon l'une quelconque des revendications 1 à 3, **caractérisé en ce que** la séquence aléatoire est obtenue par deux valeurs d'initialisation, la première étant une première clé (K_a) permettant de générer une séquence aléatoire intermédiaire, la seconde étant une seconde clé (K_b) permettant de crypter la séquence aléatoire intermédiaire pour obtenir la séquence aléatoire.

6. Procédé selon l'une quelconque des revendications 1 à 4, **caractérisé en ce que** la méthode de transformation rapide est une méthode du type d'Hadamard qui comporte les étapes suivantes:

- permutation des échantillons du bloc courant selon une première table de permutation;
- application de la transformée d'Hadamard aux échantillons ainsi permutés;
- permutation des échantillons du vecteur résultant de la transformée d'Hadamard selon une seconde table de permutation pour obtenir les valeurs de corrélations.

7. Procédé selon la revendication 6, **caractérisé en ce qu'**il comporte une étape préalable d'initialisation dans laquelle les première et seconde tables de permutation ainsi que la séquence aléatoire sont calculées et mémorisées.

8. Procédé selon la revendication 7, **caractérisé en ce que** le calcul de la séquence aléatoire, de la première et de la seconde table de permutation est optimisé par un nombre minimum d'opération binaires réalisées sur les bits d'un entier représentant dans chaque cas le registre à décalage de génération de la séquence ou de la table.

9. Procédé selon l'une quelconque des revendications 1 à 5, **caractérisé en ce que** la méthode de transformation rapide est par une méthode de type transformée de Fourier qui comporte les étapes suivantes:

- application d'une transformée de Fourier au bloc courant;
- calcul d'un produit sur les échantillons résultant de la transformée du bloc courant et ceux du complexe conjuguée de la séquence aléatoire ayant subi une transformée de Fourier;
- application d'une transformée inverse de Fourier pour obtenir les valeurs de corrélation.

10. Procédé selon la revendication 9, **caractérisé en ce qu'**il comporte une étape d'initialisation dans laquelle la transformée de Fourier de la séquence aléatoire et son complexe conjugué sont calculés et mémorisés.

11. Procédé selon l'une des revendications 1 à 5, **caractérisé en ce que** la méthode de transformation rapide est une méthode de type transformée de Fourier qui comporte les étapes suivantes:

- segmentation en sous-séquences du bloc courant;
- segmentation en sous-séquences de la séquence aléatoire, la deuxième moitié de la sous-séquence aléatoire étant mise à zéro;
- application d'une transformée de Fourier aux sous-séquences du bloc courant et aux sous-séquences de la séquence aléatoire;
- calcul de corrélations partielles par le produit sur les échantillons résultant de la transformée des sous-séquences du bloc courant et ceux du complexe conjugué des sous-séquences de la séquence aléatoire;

- sommation des corrélations partielles calculées;
- application d'une transformée de Fourier inverse à la somme issue de l'étape de sommation pour obtenir les valeurs de corrélation.

12. Procédé selon l'une des revendications 1 à 5, **caractérisé en ce que** la méthode de transformation rapide est une méthode de type transformée de Fourier qui comporte les étapes suivantes:

- segmentation en sous-séquences du bloc courant;
- segmentation en sous-séquences de la séquence aléatoire, la première moitié de la sous-séquence aléatoire étant mise à zéro;
- application d'une transformée de Fourier aux sous-séquences du bloc courant et aux sous-séquences de la séquence aléatoire;
- calcul de corrélations partielles par le produit sur le complexe conjugué des échantillons résultant de la transformée des sous-séquences du bloc courant et ceux des échantillons résultant des sous-séquences de la séquence aléatoire;
- sommation des corrélations partielles calculées;
- application d'une transformée de Fourier inverse à la somme issue de l'étape de sommation pour obtenir les valeurs de corrélation.

13. Dispositif de détection d'un identificateur de tatouage dans un signal audio, l'identificateur de tatouage ayant été inséré dans le signal audio à partir d'une séquence aléatoire d'une longueur de N échantillons, N étant multiple de Ns, obtenue par au moins une valeur d'initialisation, **caractérisé en ce qu'**il comporte:

- des moyens de préparation d'un bloc courant de N échantillons à partir du signal tatoué;
- des moyens de calcul de corrélation par une méthode de transformation rapide entre les échantillons du bloc courant et ceux de la séquence aléatoire obtenue à partir de la au moins une valeur d'initialisation;
- des moyens de comparaison à un seuil prédéterminé des valeurs de corrélation issues du calcul de corrélation des Ns premiers échantillons;
- des moyens d'obtention d'un nouveau bloc courant par décalage de Ns échantillons par rapport au bloc précédent mis en oeuvre tant que le maximum des dites valeurs de corrélation n'est pas supérieure au seuil prédéterminé.

14. Programme d'ordinateur comprenant des instructions de code pour la mise en oeuvre des étapes d'un procédé de détection d'identificateur de tatouage conforme à l'une des revendications 1 à 12, lorsque ledit programme est exécuté par un processeur.

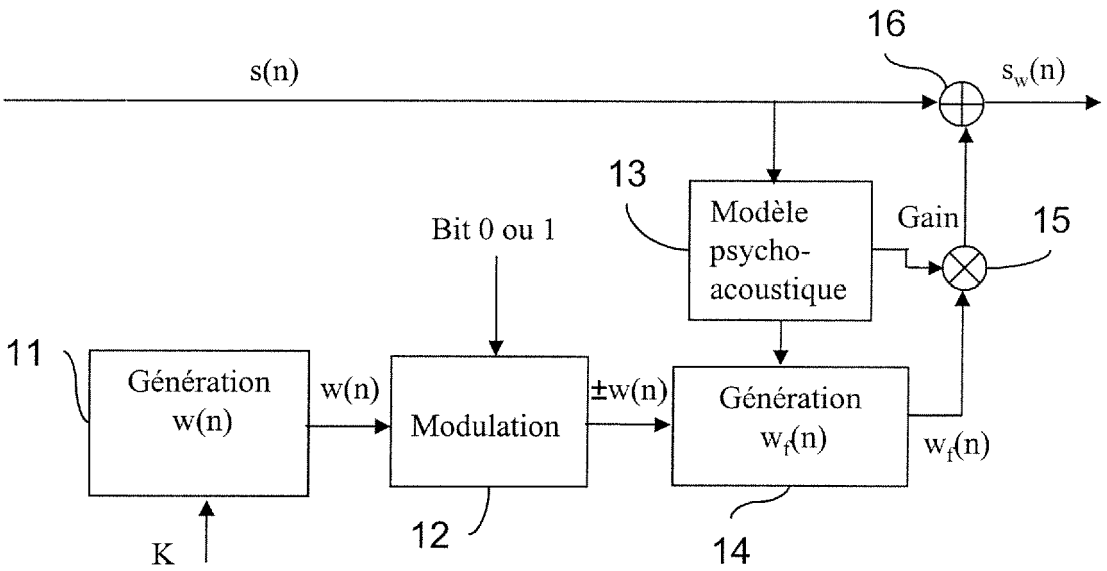

Fig.1 (Etat de l'art)

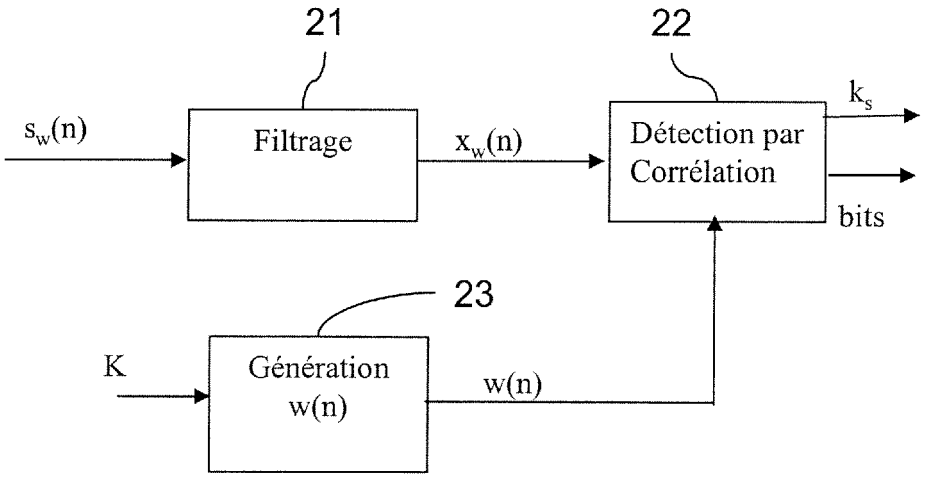

Fig.2 (Etat de l'art)

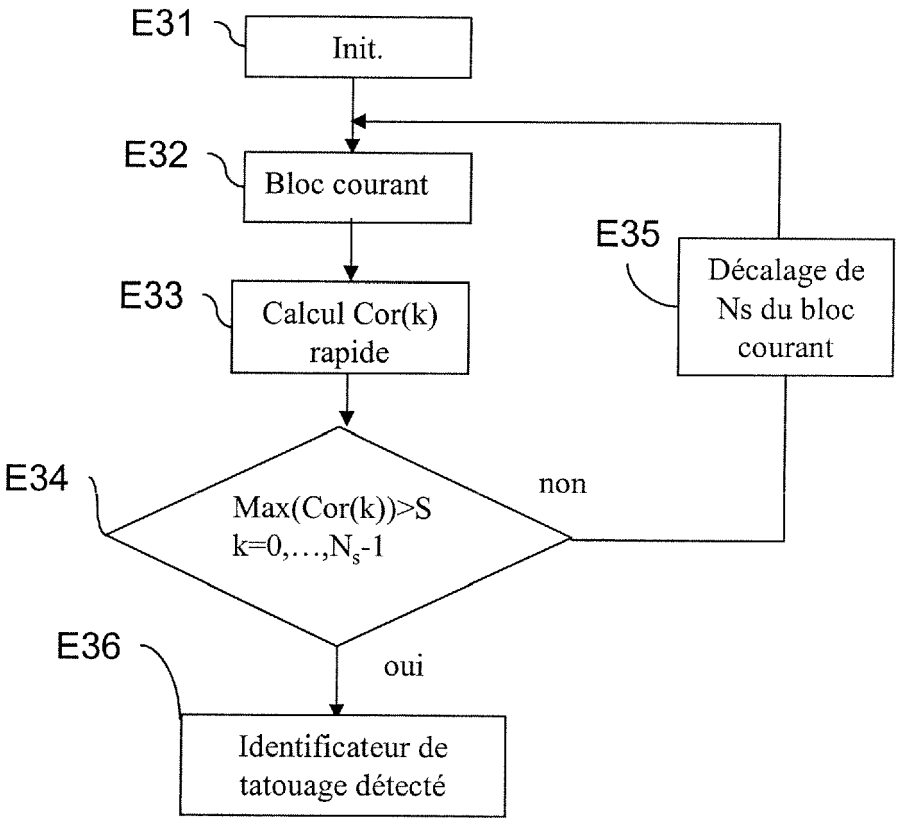
E31
Init.
E32
Bloc courant
E33
Calcul Cor(k) rapide
E34
Max(Cor(k))>S
k=0,…,Ns-1
non
E35
Décalage de Ns du bloc courant
oui
E36
Identificateur de tatouage détecté

Fig.3

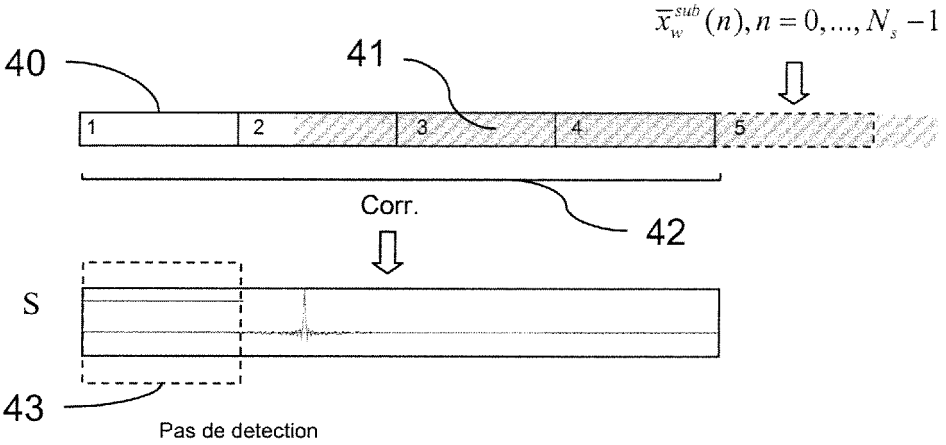
$\overline{x}_w^{sub}(n), n = 0,...,N_s - 1$
40
41
1
2
3
4
5
Corr.
42
S
43
Pas de detection

Fig.4a

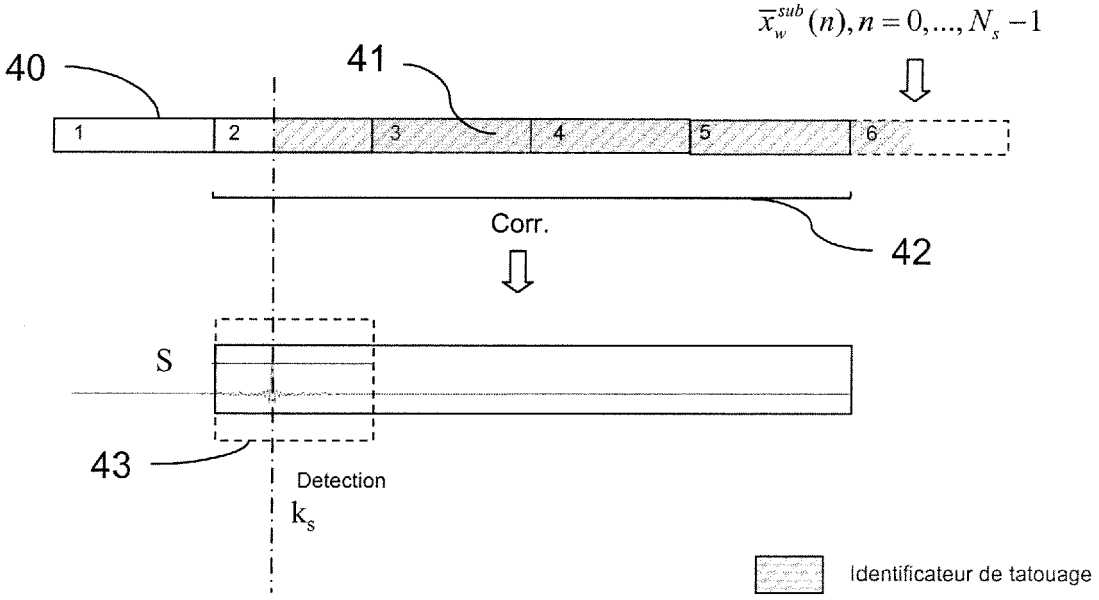
$\overline{x}_w^{sub}(n), n = 0,...,N_s - 1$
40
41
1
2
3
4
5
6
Corr.
42
S
43
Detection
k_s
Identificateur de tatouage

Fig.4b

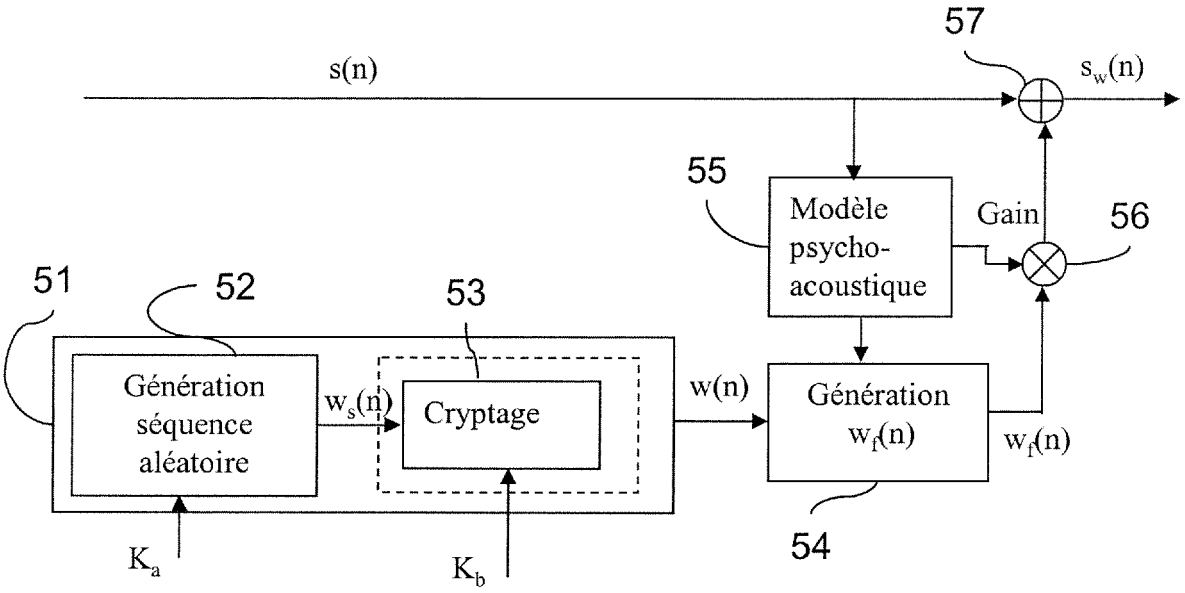
57
s(n)
$s_w(n)$
55
Modèle psycho-acoustique
Gain
56
51
52
53
Génération séquence aléatoire
$w_s(n)$
Cryptage
w(n)
Génération $w_f(n)$
$w_f(n)$
54
K_a
K_b

Fig.5

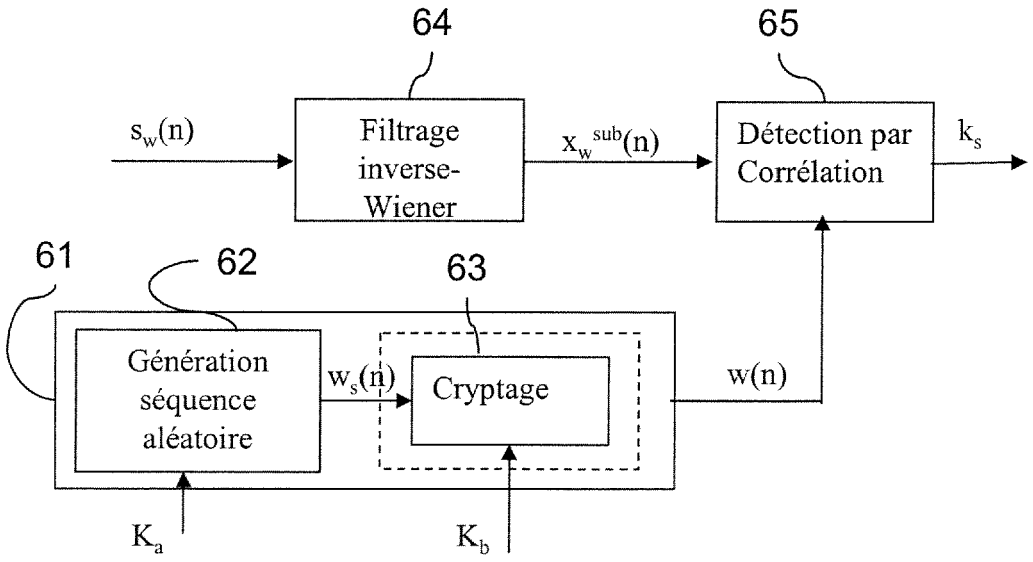
64
65
$s_w(n)$
Filtrage inverse-Wiener
$x_w^{sub}(n)$
Détection par Corrélation
k_s
61
62
63
Génération séquence aléatoire
$w_s(n)$
Cryptage
w(n)
K_a
K_b

Fig.6

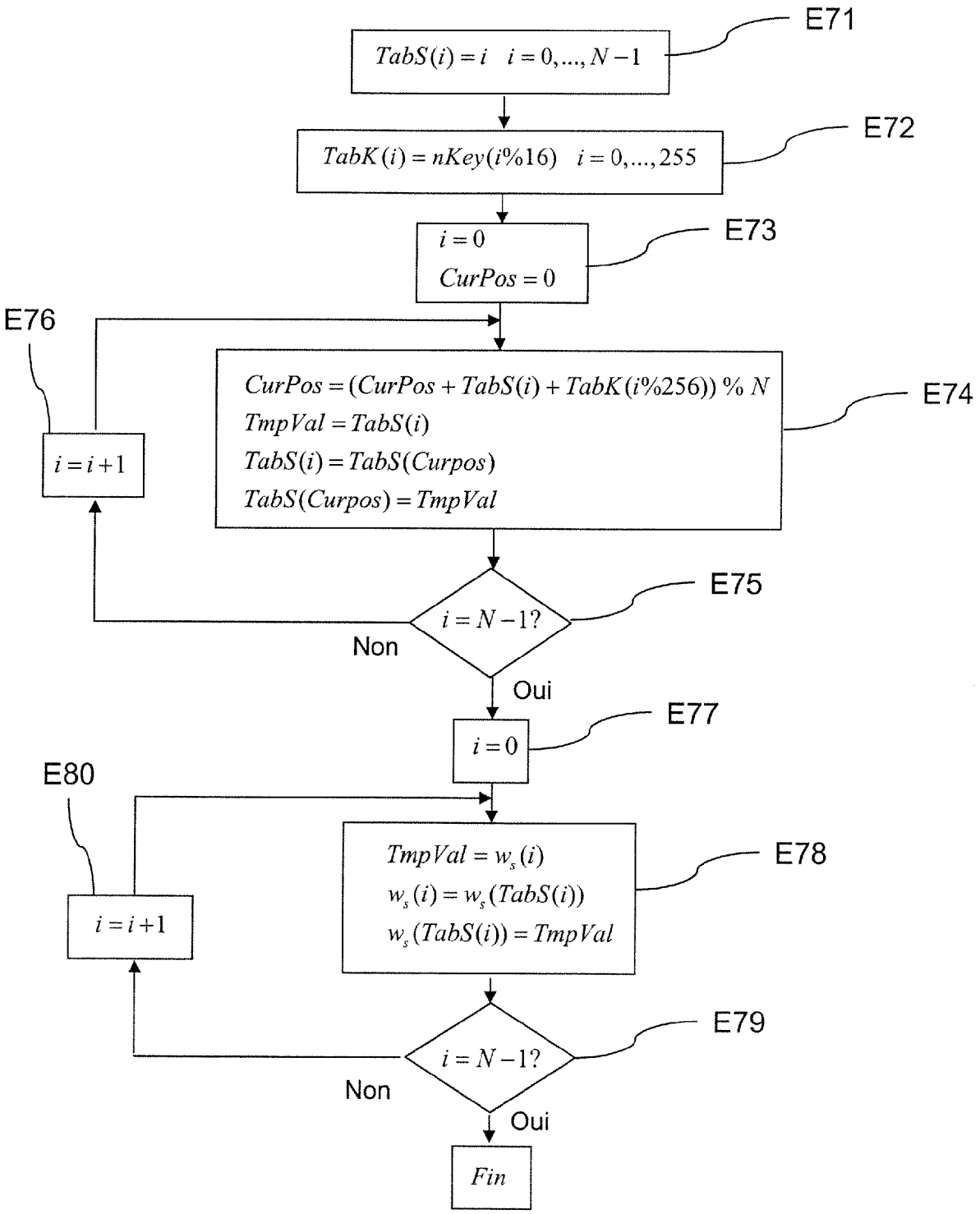
E71
TabS(i) = i i = 0,..., N −1
E72
TabK(i) = nKey(i%16) i = 0,...,255
E73
i = 0
CurPos = 0
E76
i = i +1
E74
CurPos = (CurPos + TabS(i) + TabK(i%256)) % N
TmpVal = TabS(i)
TabS(i) = TabS(Curpos)
TabS(Curpos) = TmpVal
E75
i = N −1?
Non
Oui
E77
i = 0
E80
i = i +1
E78
TmpVal = w_s(i)
w_s(i) = w_s(TabS(i))
w_s(TabS(i)) = TmpVal
E79
i = N −1?
Non
Oui
Fin

Fig.7

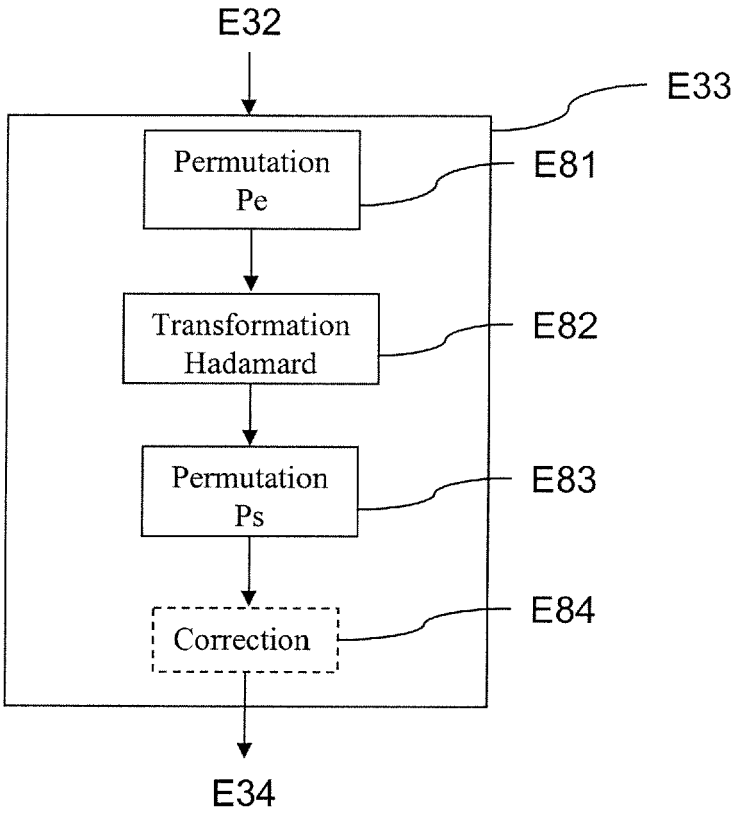
E32
E33
Permutation
Pe
E81
Transformation
Hadamard
E82
Permutation
Ps
E83
Correction
E84
E34

Fig.8

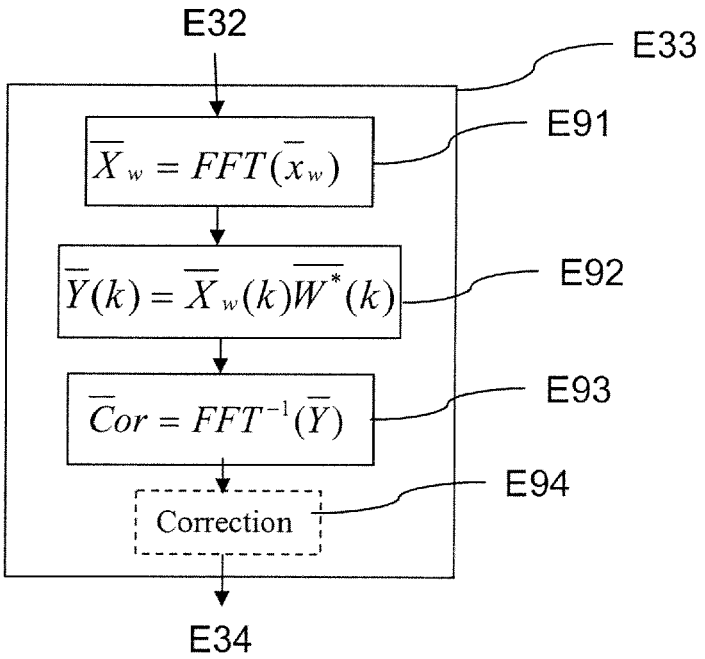
E32
E33
$\overline{X}_w = FFT(\overline{x}_w)$
E91
$\overline{Y}(k) = \overline{X}_w(k)\overline{W^*}(k)$
E92
$\overline{Cor} = FFT^{-1}(\overline{Y})$
E93
Correction
E94
E34

Fig.9

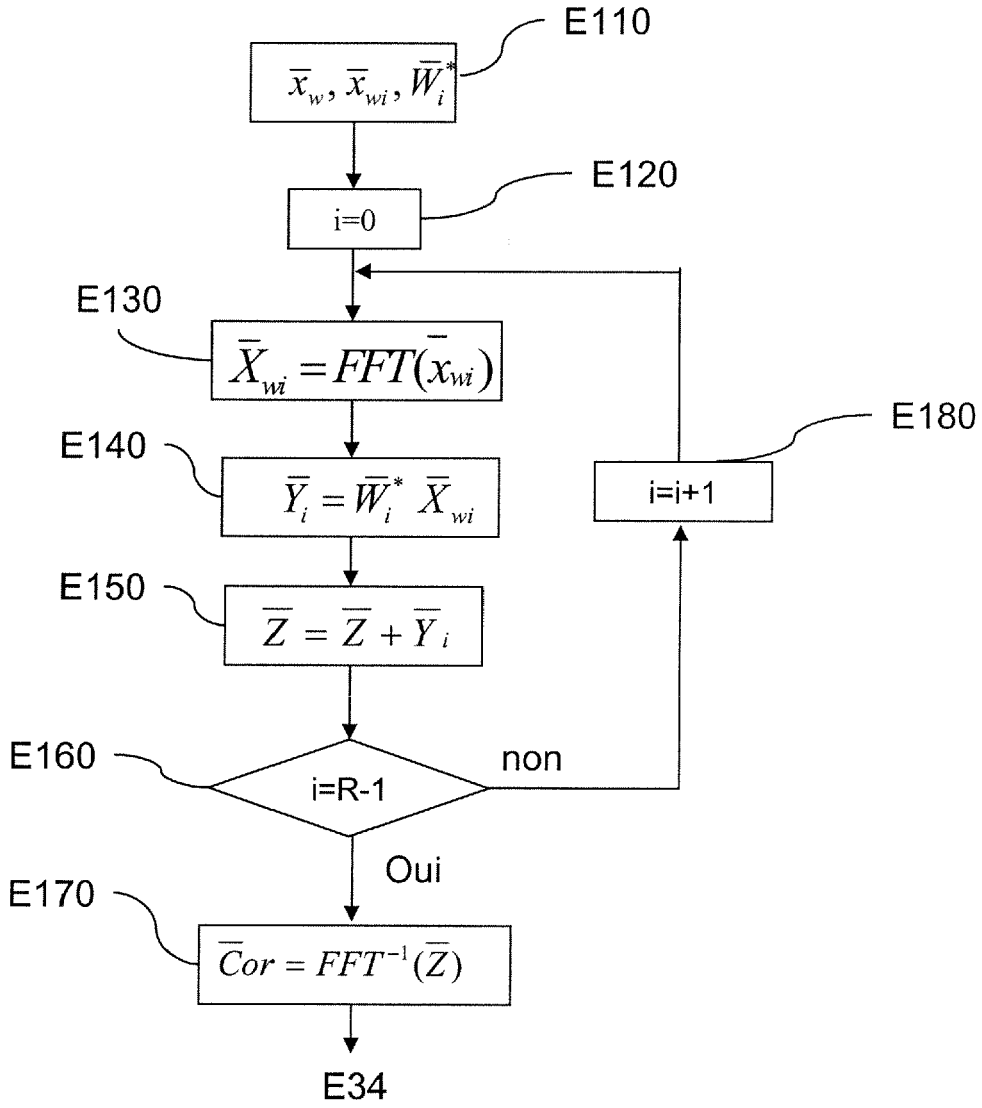
E110
$\bar{x}_w, \bar{x}_{wi}, \bar{W}_i^*$
E120
i=0
E130
$\bar{X}_{wi} = FFT(\bar{x}_{wi})$
E140
$\bar{Y}_i = \bar{W}_i^* \bar{X}_{wi}$
E150
$\bar{Z} = \bar{Z} + \bar{Y}_i$
E160
i=R-1
non
Oui
E170
$\bar{C}or = FFT^{-1}(\bar{Z})$
E34
E180
i=i+1

Fig.10

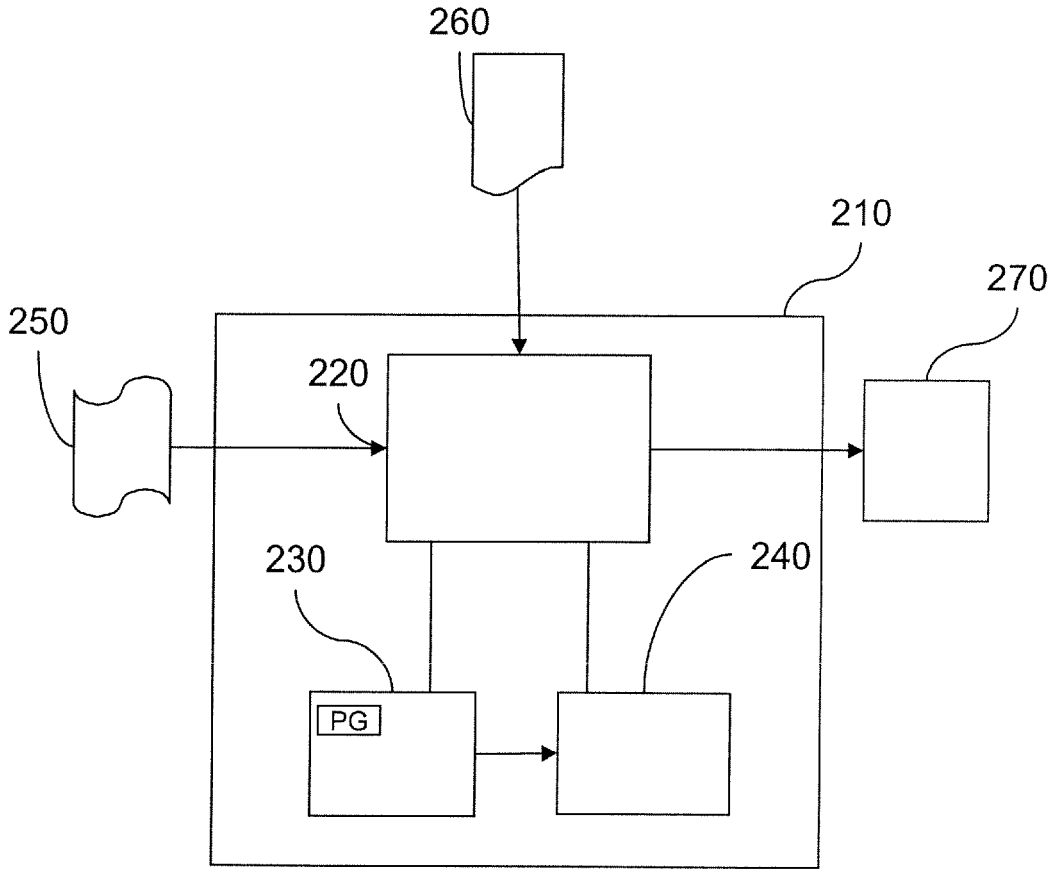

Fig.11

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 07 30 1153

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
E	EP 1 837 875 A (THOMSON BRANDT GMBH [DE]) 26 septembre 2007 (2007-09-26) * le document en entier *	1,2,4, 9-14	INV. G10L19/00
X	PARASKEVI BASSIA ET AL: "Robust Audio Watermarking in the Time Domain" IEEE TRANSACTIONS ON MULTIMEDIA, IEEE SERVICE CENTER, PISCATAWAY, NJ, US, vol. 3, no. 2, juin 2001 (2001-06), XP011036241 ISSN: 1520-9210 * alinéa [00IV] *	1,2,4, 13,14	
A	WO 98/37513 A (TELSTRA R & D MAN PTY LTD [AU]; JOHNSON ANDREW [AU]; BIGGAR MICHAEL [A) 27 août 1998 (1998-08-27) * abrégé; revendications 15,16,18,19,21-26; figures 2,6 *	1,2,4-14	
A	US 6 983 057 B1 (HO ANTHONY TUNG SHUEN [SG] ET AL) 3 janvier 2006 (2006-01-03) * abrégé; revendications 37,40,43,46-52 *	1,2,4-14	DOMAINES TECHNIQUES RECHERCHES (IPC)
A	EP 1 594 122 A (THOMSON BRANDT GMBH [DE]) 9 novembre 2005 (2005-11-09) * alinéa [0019] - alinéa [0020]; revendications 4-7 *	1,2,4,5, 9-14	G06T H04N G11B G10L
A	WO 02/49363 A (KENT RIDGE DIGITAL LABS [SG]; XU CHANGSHENG [SG]) 20 juin 2002 (2002-06-20) * page 14, ligne 13 - page 16; revendications 4-6 *	1,2,4,5, 13,14	

-/--

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	20 décembre 2007	Brans, Tim

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 07 30 1153

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
A	BARAS C ET AL: "An Audio Spread-Spectrum Data Hiding System with an Informed Embedding Strategy Adapted to a Wiener Filtering Based Receiver" MULTIMEDIA AND EXPO, 2005. ICME 2005. IEEE INTERNATIONAL CONFERENCE ON AMSTERDAM, THE NETHERLANDS 06-06 JULY 2005, PISCATAWAY, NJ, USA,IEEE, 6 juillet 2005 (2005-07-06), pages 1022-1025, XP010843215 ISBN: 0-7803-9331-7 * abrégé *	3	
A	MUNTEAN T ET AL: "Audio digital watermarking based on hybrid spread spectrum" WEB DELIVERING OF MUSIC, 2002. WEDELMUSIC 2002. PROCEEDINGS. SECOND INTERNATIONAL CONFERENCE ON 9-11 DEC. 2002, PISCATAWAY, NJ, USA,IEEE, 9 décembre 2002 (2002-12-09), pages 150-155, XP010626956 ISBN: 0-7695-1623-8 * alinéa [03.2]; figures 3,6 *	1,2,4, 9-14	DOMAINES TECHNIQUES RECHERCHES (IPC)
A	KIROVSKI D ET AL: "SPREAD-SPECTRUM WATERMARKING OF AUDIO SIGNALS" IEEE TRANSACTIONS ON SIGNAL PROCESSING, IEEE SERVICE CENTER, NEW YORK, NY, US, vol. 51, no. 4, avril 2003 (2003-04), pages 1020-1033, XP001171826 ISSN: 1053-587X * abrégé *	1,13,14	

-/--

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	20 décembre 2007	Brans, Tim

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P04C02)

Office européen des brevets

RAPPORT DE RECHERCHE EUROPEENNE

Numéro de la demande
EP 07 30 1153

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendication concernée	CLASSEMENT DE LA DEMANDE (IPC)
A	CVEJIC N AND SEPPANEN T: "IMPROVING AUDIO WATERMARKING SCHEME USING PSYCHOACOUSTIC WATERMARK FILTERING" PROCEEDINGS OF IEEE INTERNATIONAL SYMPOSIUM ON SIGNAL PROCESSING AND INFORMATION TECHNOLOGY, CAIRO, EGYPT, 28 décembre 2001 (2001-12-28), - 30 décembre 2001 (2001-12-30) XP008078163 * alinéa [0003]; figure 3 *	1,13,14	
A	HADDAD MOHSEN ET AL: "OPTIMAL DETECTOR FOR AN ADDITIVE WATERMARKING SCHEME BASED ON HUMAN AUDITORY SYSTEM" PROCEEDINGS OF THE SPIE, SPIE, BELLINGHAM, VA, US, vol. 6072, 17 février 2006 (2006-02-17), pages 60721Z-1, XP008078028 ISSN: 0277-786X * abrégé *	1,3,13, 14	
D,A	WO 2004/010376 A (KONINKL PHILIPS ELECTRONICS NV [NL]; BRUEKERS ALPHONS A M L [NL]; HAIT) 29 janvier 2004 (2004-01-29) * abrégé *	1,13,14	DOMAINES TECHNIQUES RECHERCHES (IPC)
D,A	ALRUTZ AND M R SCHROEDER H: "A FAST HADAMARD TRANSFORM ALGORITHM FOR THE EVALUATION OF MEASUREMENTS USING PSEUDORANDOM TEST SIGNALS" ICA. PROCEEDINGS OF THE INTERNATIONAL CONGRESS ON ACOUSTICS, XX, XX, no. 11TH, 1983, pages 235-238, XP008075716 * abrégé *	6-8	

Le présent rapport a été établi pour toutes les revendications

Lieu de la recherche	Date d'achèvement de la recherche	Examinateur
La Haye	20 décembre 2007	Brans, Tim

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet antérieur, mais publié à la date de dépôt ou après cette date
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

7

EPO FORM 1503 03.82 (P04C02)

ANNEXE AU RAPPORT DE RECHERCHE EUROPEENNE RELATIF A LA DEMANDE DE BREVET EUROPEEN NO. EP 07 30 1153

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche européenne visé ci-dessus.
Lesdits members sont contenus au fichier informatique de l'Office européen des brevets à la date du
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets.

20-12-2007

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1837875 A	26-09-2007	WO 2007107455 A1	27-09-2007
WO 9837513 A	27-08-1998	US 7269734 B1	11-09-2007
		US 2007230739 A1	04-10-2007
US 6983057 B1	03-01-2006	AUCUN	
EP 1594122 A	09-11-2005	AUCUN	
WO 0249363 A	20-06-2002	US 2004059918 A1	25-03-2004
WO 2004010376 A	29-01-2004	AT 341043 T	15-10-2006
		AU 2003281648 A1	09-02-2004
		BR 0305626 A	19-10-2004
		CN 1672172 A	21-09-2005
		DE 60308686 T2	16-08-2007
		ES 2270060 T3	01-04-2007
		JP 2005534053 T	10-11-2005
		US 2006156002 A1	13-07-2006

EPO FORM P0460

Pour tout renseignement concernant cette annexe : voir Journal Officiel de l'Office européen des brevets, No.12/82

RÉFÉRENCES CITÉES DANS LA DESCRIPTION

Cette liste de références citées par le demandeur vise uniquement à aider le lecteur et ne fait pas partie du document de brevet européen. Même si le plus grand soin a été accordé à sa conception, des erreurs ou des omissions ne peuvent être exclues et l'OEB décline toute responsabilité à cet égard.

Documents brevets cités dans la description

- WO 2004010376 A **[0025]**

Littérature non-brevet citée dans la description

- **A. ALRUTZ ; M. R. SCHROËDER.** A fast Hadamard transform method for the évaluation of measurement using pseudo random test signals. *Proceeding of the 11th conférence on acoustics,* 1983 **[0021]**
- **B. SCHNEIER.** Applied cryptography, protocols and sources in C. John Wiley & sons, inc, 1996, 397, 398 **[0099]**
- **B. SCHNEIER.** Applied cryptography, protocols and sources in C. John Wiley & sons, inc, 1996, 372-375 **[0105]**
- **A. ALRUTZ ; M. R. SCHROËDER.** A fast Hadamard transform method for the evaluation of measurement using pseudo random test signals. *Proceeding of the 11th conference on acoustics,* 1983 **[0118]**