PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 :		(11) Numéro de publication internationale:	WO 00/11867
H04N 7/16, G10H 1/00	A1	(43) Date de publication internationale:	2 mars 2000 (02.03.00)

(21) Numéro de la demande internationale: PCT/FR99/02017

(22) Date de dépôt international: 19 août 1999 (19.08.99)

(30) Données relatives à la priorité:
98/10543 19 août 1998 (19.08.98) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: INNOVATRON (SOCIETE ANONYME) [FR/FR]; 1, rue Danton, F–75006 Paris (FR).

(72) Inventeur; et
(75) Inventeur/Déposant *(US seulement)*: MORENO, Roland [FR/FR]; 3, rue de l'Ancienne Comédie, F–75006 Paris (FR).

(74) Mandataire: DUPUIS–LATOUR, Dominique; Cabinet Bardehle, Pagenberg & Partner, 14, boulevard Malesherbes, F–75008 Paris (FR).

(81) Etats désignés: AE, AL, AU, BA, BB, BG, BR, CA, CN, CU, CZ, EE, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, SL, TR, TT, UA, US, UZ, VN, YU, ZA, brevet ARIPO (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

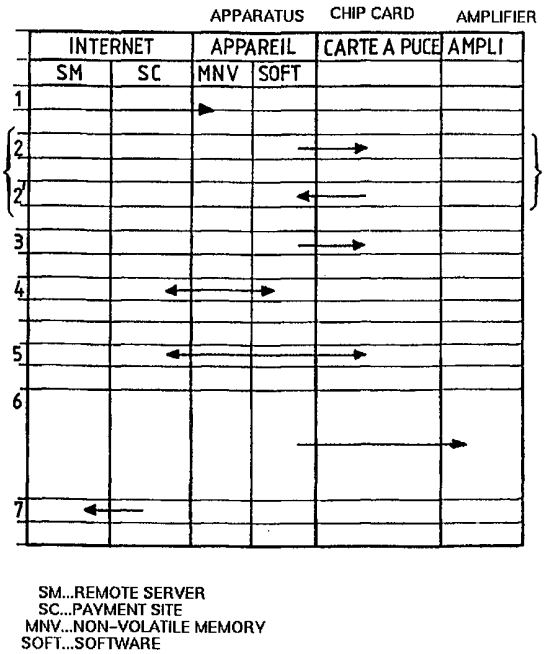
Publiée
Avec rapport de recherche internationale.

(54) Title: METHOD FOR CERTIFIED DELIVERY OF AN AUDIO, VIDEO OR TEXTUAL SEQUENCE

(54) Titre: PROCEDE DE DELIVRANCE CERTIFIEE D'UNE SEQUENCE AUDIO, VIDEO OU TEXTUELLE

(57) Abstract

The invention concerns a method comprising steps which consist in: connecting the apparatus to a remote server (SM); transmitting to this server a sequence–selecting request; receiving in response from said server an encrypted compressed flow of digital signals corresponding to the selected sequence; decompressing and decrypting the flow received and transforming it into an audio, video or textual signal capable of being reproduced and presented to the user. The method further comprises the following steps: writing into the microcircuit memory a debit information corresponding to the selected sequence; transmitting the debit rate to a remote payment site (SC), separate from the server or not; producing a corresponding cryptographic certificate from the payment site; transmitting said cryptographic certificate to the apparatus; verifying by the apparatus the conformity of said cryptographic certificate; if conformity is acknowledged, delivering said decrypted decompressed audio, video or textual signal capable of being reproduced and presented to the user.



(57) Abrégé

Ce procédé comprend les étapes consistant à: connecter l'appareil à un serveur distant (SM); émettre vers ce serveur une requête de choix de séquence; recevoir en réponse de ce serveur un flux de signaux numériques comprimés et cryptés correspondant à la séquence choisie; décomprimer et décrypter le flux reçu et le transformer en un signal audio, vidéo ou textuel apte à être reproduit et présenté à l'utilisateur. Il comporte également les étapes suivantes: inscription dans une mémoire du microcircuit d'une information de débit correspondant à la séquence choisie; transmission de l'information de débit à un site de paiement distant, distinct (SC) ou non dudit serveur; production d'un certificat cryptographique correspondant par le site de paiement; transmission à l'appareil de ce certificat cryptographique; vérification par l'appareil de la conformité de ce certificat cryptographique; en cas de conformité reconnue, délivrance des données dudit signal audio, vidéo ou textuel apte à être reproduit et présenté à l'utilisateur, décomprimées et décryptées.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

PROCEDE DE DELIVRANCE CERTIFIEE D'UNE SEQUENCE AUDIO, VIDEO OU TEXTUELLE

La présente invention concerne un procédé de délivrance de séquences audio, vidéo, textuelles ou analogues auprès d'un site distant par téléchargement de données.

On décrira l'invention dans le cadre de séquences audio, car il s'agit là de l'application la plus immédiate compte tenu des capacités actuelles des réseaux de diffusion ; toutefois, l'invention peut être transposée directement à l'acquisition d'autres types de séquences, notamment de données vidéo (images fixes ou images animées de télévision) ou de séquences textuelles. Elle s'applique de la même façon à l'acquisition de séquences formant fichiers de données de nature informatique, par exemple des données nécessaires au téléchargement d'un logiciel, ou pour permettre l'exécution par l'utilisateur d'un logiciel nécessitant un échange de données avec un site distant.

Les appareils de reproduction sonore peuvent fonctionner à partir de diverses sources, telles que des supports enregistrés (disques, bandes, etc.) ou transmises à distance (radiodiffusion).

Ces sources présentent toutes divers inconvénients :

- l'utilisation des supports enregistrés présuppose que l'utilisateur se soit au préalable déplacé pour les acheter ou les emprunter, avec bien entendu les difficultés qu'il peut rencontrer pour obtenir des enregistrements rares ou anciens, difficiles à trouver ;
- les sources radiodiffusées, quant à elles, présentent l'inconvénient d'un choix limité au nombre de stations captées par l'utilisateur, et de l'impossibilité de choisir le moment de début d'écoute, l'utilisateur étant astreint aux horaires de diffusion de la station qu'il reçoit.

Les techniques modernes de compression des données rendent possible aujourd'hui la transmission du son, et particulièrement de la musique enregistrée, via un réseau téléinformatique (par exemple un réseau Internet) dans d'excellentes conditions techniques, c'est-à-dire compatibles avec le plus haut degré de qualité sonore aujourd'hui partout exploité.

Ces possibilités sont en particulier offertes dans le cas d'une compression de

type "MP3", avec un débit d'environ 60 000 bps (bits par seconde), du même ordre que celui des modems couramment disponibles aujourd'hui, les données étant décomprimables en temps réel, à la vitesse de l'écoute. Des perspectives encore plus favorables peuvent même être envisagées avec des transmissions à plus grand débit telles que transmissions sur réseau RNIS ou sur réseau câblé, ou transmission de données numérisées par satellite sur les canaux à grand débit de télévision.

Ces techniques rassemblent un grand nombre d'avantages :

- très vaste choix de plages (morceaux musicaux),
- possibilité de sélection des plages à volonté depuis l'installation,
- possibilité du choix du moment de début d'écoute,
- absence de support matériel enregistré (donc gain de place et moindre coût de l'appareil du fait de l'absence d'éléments mécaniques),
- qualité sonore de type "numérique", c'est-à-dire très supérieure à celle des émissions radiodiffusées.

L'invention concerne plus précisément le paiement des droits de diffusion en fonction du choix effectué par l'utilisateur, de la même manière que lorsque ce dernier achète un support d'enregistrement.

Le but de l'invention est de proposer un procédé sécurisé de paiement de ces droits, permettant de contrer les tentatives de fraudes telles que téléchargement sans paiement des droits ou reproduction non autorisée des séquences.

Elle concerne également la répartition de ces droits entre les divers éditeurs de musique, en cherchant à éviter les inconvénients des paiements de droits par les radiodiffuseurs, qui ne tiennent pas compte, si ce n'est d'une façon statistique donc approximative, de l'audience réelle au moment de la diffusion de telle ou telle plage musicale.

Plus précisément, selon un premier de ses aspects, la présente invention vise un procédé de délivrance de séquences audio, vidéo ou textuelles à un appareil d'un usager coopérant avec un microcircuit, notamment un microcircuit de carte à puce, par télétransmission de données numériques représentatives de ces séquences, procédé comprenant les étapes consistant à :

- connecter l'appareil à un serveur distant,
- émettre vers ce serveur une requête de choix de séquence,

- recevoir en réponse de ce serveur un flux de signaux numériques comprimés et cryptés correspondant à la séquence choisie,
- décomprimer et décrypter le flux reçu et le transformer en un signal audio, vidéo ou textuel apte à être reproduit et présenté à l'utilisateur,

ce procédé étant caractérisé en ce qu'il comporte également les étapes suivantes :

- inscription dans une mémoire du microcircuit d'une information de débit correspondant à la séquence choisie,
- transmission de l'information de débit à un site de paiement distant, distinct ou non dudit serveur,
- production d'un certificat cryptographique correspondant par le site de paiement,
- transmission à l'appareil de ce certificat cryptographique,
- vérification par l'appareil de la conformité de ce certificat cryptographique,
- en cas de conformité reconnue, délivrance des données dudit signal audio, vidéo ou textuel apte à être reproduit et présenté à l'utilisateur, décomprimées et décryptées.

Selon divers mode de mise en œuvre subsidiaires avantageux :

- le certificat est un certificat intrinsèque dont est fonction la clef cryptographique permettant le déchiffrement ;
- une information de titulaire de droits est associée à chaque information de séquence, et le site de paiement attribue à leurs titulaires respectifs les paiements correspondant aux séquences choisies ;
- le procédé comprend en outre une étape d'inclusion, par le microcircuit, d'un filigrane dans le signal audio, vidéo ou textuel apte à être reproduit et présenté à l'utilisateur, ce filigrane incorporant un identifiant du microcircuit ;
- les données du signal audio, vidéo ou textuel sont, au choix de l'utilisateur de l'appareil, délivrées sous forme analogique ou bien numérique, et l'information de débit est une information différenciée en fonction de ce choix.

Selon un second de ses aspects, la présente invention vise un procédé de délivrance de séquences audio, vidéo ou textuelles à un appareil d'un usager coopérant avec un microcircuit, notamment un microcircuit de

carte à puce, par télétransmission de données numériques représentatives de ces séquences, procédé comprenant les étapes consistant à :

a) connecter l'appareil à un serveur distant,

b) émettre vers ce serveur une requête de choix de séquence,

c) recevoir en réponse de ce serveur un flux de signaux numériques comprimés et cryptés correspondant à la séquence choisie,

d) inscrire dans une mémoire du microcircuit une information de débit correspondant à la séquence choisie,

e) décomprimer et décrypter le flux reçu et le transformer en un signal audio, vidéo ou textuel apte à être reproduit et présenté à l'utilisateur,

ce procédé étant caractérisé en ce que, à l'étape (e), le décryptage est opéré par des moyens incluant ledit microcircuit utilisé pour opérer à l'étape (d) l'inscription de l'information de débit.

Avantageusement, ce procédé comprend en outre une étape d'inclusion, par le microcircuit, d'un filigrane dans le signal audio, vidéo ou textuel apte à être reproduit et présenté à l'utilisateur, ce filigrane incorporant un identifiant du microcircuit.

◊

On va maintenant décrire un exemple de mise en œuvre de l'invention, en référence aux dessins annexés.

La figure 1 est un schéma par blocs fonctionnels des différents éléments constituant un appareil permettant la mise en œuvre de l'invention.

La figure 2 est un schéma par blocs illustrant une variante de la figure 1, avec un degré d'intégration supérieur des éléments.

La figure 3 illustre les échanges de signaux entre les différents sites ou blocs intervenant dans la mise en œuvre du procédé de l'invention.

◊

Sur la figure 1, la référence 10 désigne une unité classique ampli/préampli stéréo alimentant une paire de haut-parleurs 12. L'unité 10 peut être soit intégrée au reste de l'appareil (qui se présente alors extérieurement sous la forme habituelle d'un amplificateur de chaîne haute fidélité) ou extérieure à

celui-ci (l'appareil se présentant alors sous forme d'un boîtier de même type qu'un lecteur de CD, tuner, etc. connecté à l'une des entrées d'un amplificateur classique).

On notera que l'appareil peut être réalisé aussi bien sous forme d'un appareil dédié (comme décrit ici) que d'une extension à un micro-ordinateur, voire même être seulement constitué par un micro-ordinateur multimédia associé à un lecteur de carte à puce.

L'appareil comprend un afficheur 14 susceptible de présenter à l'utilisateur une série de plages musicales, ainsi que des moyens de sélection de ces plages musicales, par exemple sous forme d'une molette 16 (pour faire défiler les plages) combinée à un bouton-poussoir 18 de validation.

L'appareil comporte également un processeur programmable 20 comprenant essentiellement une unité centrale de traitement CPU 22 et une mémoire non volatile MNV 4, indépendamment de ses ressources propres en mémoires morte ROM 26 et vive RAM 28. Le processeur 20 reçoit les informations de sélection et de validation provenant de la molette 16 et du bouton-poussoir 18, et il pilote l'afficheur 14.

La mémoire non volatile 24 peut éventuellement incorporer un disque dur de faible volume, si les contraintes techniques particulières en imposent la nécessité, ou être simplement constituée d'un "disque solide", c'est-à-dire d'une mémoire à semiconducteurs de grande dimension, par exemple 32 Mo.

L'appareil est également relié à un modem 30 chargé d'interfacer l'appareil avec le réseau téléphonique 32, typiquement à une vitesse de 56 000 bps.

L'appareil comporte également un circuit de commutation 34 permettant la sélection entre, d'une part, la réception d'une source audio par le modem 30 et, d'autre part, les autres entrées habituelles de l'amplificateur (CD, tuner, cassette, etc.) regroupées sur le dessin sous forme d'une entrée "auxiliaire" 36.

Le processeur 20 est en outre relié à une carte à puce 38, dont le rôle sera expliqué plus bas, par l'intermédiaire d'un lecteur 40.

L'utilisation de cet appareil a lieu essentiellement de la manière suivante.

A la mise sous tension, par exemple par appui sur le bouton 18, l'appareil se connecte automatiquement par le réseau téléphonique 32 à un site distant ou "site discothèque", dont l'adresse, Internet ou autre, est enregistrée de façon permanente dans la mémoire non volatile 24.

Le programme principal pilotant le processeur 20 permet alors la "navigation" sur ce site, ce programme incorporant par exemple un sous-ensemble d'un logiciel de navigation classique, spécialement adapté et simplifié pour les besoins du dispositif de l'invention.

L'utilisateur va ainsi naviguer dans un répertoire de plages musicales, qu'il pourra faire défiler et sélectionner au moyen de la molette 16 et du bouton-poussoir 18.

Le cas échéant, le système de navigation et l'afficheur pourront être adaptés pour faciliter l'accès par sélection de genres ou sous-genres musicaux, ou encore par sélection croisée entre genres musicaux (classique, jazz, opéra, etc.) et type d'œuvres (éditions originales, nouveautés, titres les plus/les moins demandés, etc.. L'afficheur 14 pourra alors se présenter sous forme d'un tableau à double entrée sélectionnable par des commandes appropriées en abscisse et en ordonnée (écran tactile, double rangée de boutons, etc.) permettant de désigner une intersection ligne/colonne.

Une fois la sélection de la plage musicale opérée, le processeur 20 adresse un ordre au site distant afin de permettre le téléchargement de la plage musicale choisie.

Ce téléchargement peut être opéré en temps réel (audition au fur et à mesure du chargement) ou quasi-réel, en prévoyant dans le processeur une mémoire tampon, par exemple pour accroître les performances de décompression et/ou de décryptage.

La carte à puce 38 est utilisée pour permettre le décryptage et, éventuellement, le paiement des droits attachés à l'œuvre musicale de la plage sélectionnée.

Il peut être avantageux d'utiliser une structure telle que celle illustrée figure 2, présentant un degré d'intégration supérieur – et donc une plus grande sécurité à l'encontre des fraudes.

Les circuits de sécurité/décryptage/paiement sont inclus dans un bloc 42, avantageusement réalisé sous forme d'un ensemble monolithique, circuit intégré ou circuiterie hybride noyée dans un matériau de protection empêchant tout accès non destructif aux éléments du circuit.

Ce bloc 42 comporte un microcircuit 44 recevant les informations d'identification 52 du flux brut (c'est-à-dire crypté et comprimé) issu du modem 30 et chargé de générer les clés 48 nécessaires au décryptage, et constitué typi-

quement par le microcircuit d'une carte à puce. En variante, il peut être constitué par un module de type dit SAM (*Security Access Module*), éventuellement associé à d'autre modules SAM dans le décodeur.

Le bloc 42 comporte également un module de décryptage 50 recevant l'information musicale 52 du flux brut issu du modem 30 et traitant celui-ci au moyen des clés 48 pour délivrer en sortie un flux 54 décrypté et comprimé.

Le bloc 42 comporte en outre un module de décompression 56, par exemple de type MP3 à 44,1 kHz, 16 bits stéréo, à une cadence compatible avec une écoute en temps réel, délivrant en sortie le flux de données décrypté et décomprimé 58 appliqué en entrée de l'amplificateur 10.

Dans une variante de mise en œuvre, on prévoit une sortie numérique des données, avantageusement en un format normalisé prescrit tel que le format SDMI (*Secure Digital Music Initiative*, dont les spécifications sont publiées sur le site Internet www.sdmi.org). Ce format peut comporter un identifiant, avantageusement provenant de la carte à puce et, par ailleurs, le paiement des droits pourra être différent selon que cette sortie numérique est activée ou non.

Dans une mise en œuvre particulièrement avantageuse, c'est la même carte 38 qui sert non seulement au décryptage, mais également au paiement des droits attachés à l'œuvre musicale. Ce paiement peut être effectué à partir de procédures télélogicielles connues telles que "cybercash", "virtual-money", etc.

Les données devant être échangées pour permettre le paiement sont illustrées de façon schématique sur la figure 3.

Ce processus de paiement implique des échanges de signaux entre les points suivants :

- site "musical" SM, qui est un site Internet propre à l'éditeur de musique correspondant à la plage musicale choisie,
- site "corporatif" SC, commun aux divers éditeurs participant au système et chargé de répartir les droits entre ces derniers,
- mémoire non volatile MNV de l'appareil, pour le stockage temporaire des données,
- logiciel SOFT de l'appareil,
- carte à puce 38,
- amplificateur 10.

Les différentes étapes référencées 1 à 7 sur la figure sont les suivantes :

1. Le site musical SM correspondant à la plage sélectionnée par l'utilisateur envoie à l'appareil un fichier MP3, ou un bloc de données MP3, à l'appareil, qui stocke ces informations dans sa mémoire non volatile MNV.
2. L'échange de données entre l'appareil et la carte à puce (flux 2 et 2') réalise un premier décodage des données, opéré dans le bloc 50 de la figure 2.
3. L'appareil inscrit alors dans la mémoire de la carte à puce une information de débit, correspondant à la plage choisie et à l'éditeur de musique correspondant.
4. L'appareil se connecte au site corporatif SC ; l'information de débit stockée à l'étape 3 est alors transmise au site corporatif, qui émet un certificat cryptographique.
5. Ce certificat cryptographique est transmis au décodeur, qui vérifie sa conformité et, si tel est le cas, autorise la délivrance (étape 6 ci-dessous) des données décomprimées et décryptées.
6. De manière conditionnelle (voir l'étape 5 ci-dessus), le logiciel délivre à l'amplificateur les données à écouter, décomprimées et décryptées.
7. A intervalles réguliers, le site corporatif crédite l'éditeur de musique particulier des droits débités dans l'appareil.

La vérification du certificat cryptographique à l'étape 7 peut être opérée par la carte elle-même ou, optionnellement, par un circuit SAM distinct.

Par ailleurs, dans un mode de réalisation particulier, le certificat peut être un certificat intrinsèque, c'est-à-dire dont est fonction la clef cryptographique qui permettra le déchiffrement des données à écouter.

Le débit peut être opéré par divers moyens connus : utilisation d'une carte prépayée (carte à décompte), d'une carte d'abonnement avec débit ultérieur de l'abonné, par exemple sur la facture qu'il reçoit de son fournisseur Internet, système de fidélisation, de plages gratuites promotionnelles, etc.

Le processus de paiement peut être résumé par l'algorithme en métalangage suivant.

```
Amplificateur :
        while counter > Max
                Exec (Payment_Process)
                Exec Receive_New_Key)
        wend
        Exec (Pay_Then_Decode)
        END
Site distant :
        Receive_Card_Counter
        while Counter > Max
                Exec Payment_Process
        wend
        Download_Music
        return

Payment_Process (amplificateur) :
        Payment_Process_Protocol
        if payment is NOT OK then END
        Receive_New_Key
        return
Payment_Process (site distant) :
        Receive_Royalties_Data from Card
        if Royalties_Data is NOT OK then END
        Debit_Customer_Royalties_Sum
        Credit_Publisher
        Send_New_Key
        set Card_Counter = Ø
        return
```

Par ailleurs, dans une variante de réalisation on pourra exploiter les possibilités cryptographiques offertes par la combinaison de trois données (ou sources de données) particulières :

- identité carte ;
- données d'exploitation (musique numérisée) ;
- germe aléatoire (fixe ou périodique).

Ainsi, la modulation peut-elle être rendue fonction d'une identité propre à l'amplificateur-client, c'est-à-dire indécodable par un intrus qui tenterait indûment de décoder les plages musicales qui ne lui sont pas destinées.

En outre, un tel dispositif permettrait une tarification proportionnelle à la durée d'écoute, dès lors que la périodicité du germe aléatoire pourrait être suffisamment brève. Par exemple : une unité de compte toutes les soixante secondes.

Dans une mise en œuvre particulière, il est possible de prévoir l'inclusion d'un "filigrane" (*watermarking*) dans le flux de données.

La technique d'inclusion d'un "filigrane" ou "tatouage" est en elle-même connue, et décrite par exemple dans Petitcolas et coll., Information Hiding – a Survey, *Proceedings of the IEEE*, 87(7) : 1062-1078, juillet 1999, ou Boney et coll., Digital Watermarks for Audio Signals, *European Signal Processing Conference, EUSIPCO '96,* Trieste, Italie, septembre 1996, ainsi que dans les US-A-5 828 325, US-A-5 613 004, US-A-5 687 191 et US-A-5 822 360, ou dans les présentations des systèmes *Musicode* de Aris Techologies (www.musicode.com) et *Audiomark* d'Alpha Tec Ltd. (www.alphatecltd.com).

L'invention propose cependant de la mettre en œuvre :

- au niveau du site musical, pour "filigraner" ou "tatouer" le flux de données codé (comprimé et chiffré) diffusé vers à l'utilisateur, et/ou
- au niveau du décodeur, localement et au sein même de la carte au cours des opérations de décryptage et de décompression, pour "filigraner" ou "tatouer" le flux de données décrypté et décomprimé en sortie, le filigrane incorporant un identifiant de la carte ayant servi au décryptage et à la décompression de ces données.

De façon générale, cette technique consiste à ajouter au message musical une information inaudible, mais pouvant être révélée par des techniques appropriées.

Pour un signal analogique, la technique la plus simple combine par addition un signal d'identification de faible niveau codant l'information d'identification de manière très redondante, par exemple en ajoutant une porteuse de 10 kHz de niveau inaudible par rapport au message musical et modulée en phase à 100 bits/s ; la révélation se fait par des techniques de filtrage avec corrélation. Pour un signal numérique des opérations de

même nature peuvent être faites de manière numérique. Plus simplement, le message d'identification peut être multiplexé avec le message d'origine et ignoré à la reproduction sonore (mais dans ce cas le message d'identification peut être facilement retiré).

De nombreuses techniques existent visant à rendre le tatouage indétectable, difficile à retirer ou à masquer, et altérant peu le message. Certaines permettent le tatouage de la musique comprimée sous forme numérique sans même la décomprimer, ce qui est bien adapté au cas de l'invention.

REVENDICATIONS

1. Un procédé de délivrance de séquences audio, vidéo ou textuelles à un appareil d'un usager coopérant avec un microcircuit (44), notamment un microcircuit de carte à puce (38), par télétransmission de données numériques représentatives de ces séquences, procédé comprenant les étapes consistant à :

- connecter l'appareil à un serveur distant (SM),
- émettre vers ce serveur une requête de choix de séquence,
- recevoir en réponse de ce serveur un flux de signaux numériques comprimés et cryptés correspondant à la séquence choisie,
- décomprimer et décrypter le flux reçu et le transformer en un signal audio, vidéo ou textuel apte à être reproduit et présenté à l'utilisateur,

ce procédé étant caractérisé en ce qu'il comporte également les étapes suivantes :

- inscription dans une mémoire du microcircuit d'une information de débit correspondant à la séquence choisie,
- transmission de l'information de débit à un site de paiement distant, distinct (SC) ou non dudit serveur,
- production d'un certificat cryptographique correspondant par le site de paiement,
- transmission à l'appareil de ce certificat cryptographique,
- vérification par l'appareil de la conformité de ce certificat cryptographique,
- en cas de conformité reconnue, délivrance des données dudit signal audio, vidéo ou textuel apte à être reproduit et présenté à l'utilisateur, décomprimées et décryptées.

2. Le procédé de la revendication 1, dans lequel le certificat est un certificat intrinsèque dont est fonction la clef cryptographique permettant le déchiffrement.

3. Le procédé de la revendication 1, dans lequel une information de titulaire de droits est associée à chaque information de séquence, et dans lequel le site de paiement attribue à leurs titulaires respectifs les paie-

ments correspondant aux séquences choisies.

4. Le procédé de la revendication 1, comprenant en outre une étape d'inclusion, par le microcircuit, d'un filigrane dans le signal audio, vidéo ou textuel apte à être reproduit et présenté à l'utilisateur, ce filigrane incorporant un identifiant du microcircuit.

5. Le procédé de la revendication 1, dans lequel les données du signal audio, vidéo ou textuel sont, au choix de l'utilisateur de l'appareil, délivrées sous forme analogique ou bien numérique, et dans lequel l'information de débit est une information différenciée en fonction de ce choix.

FIG_1

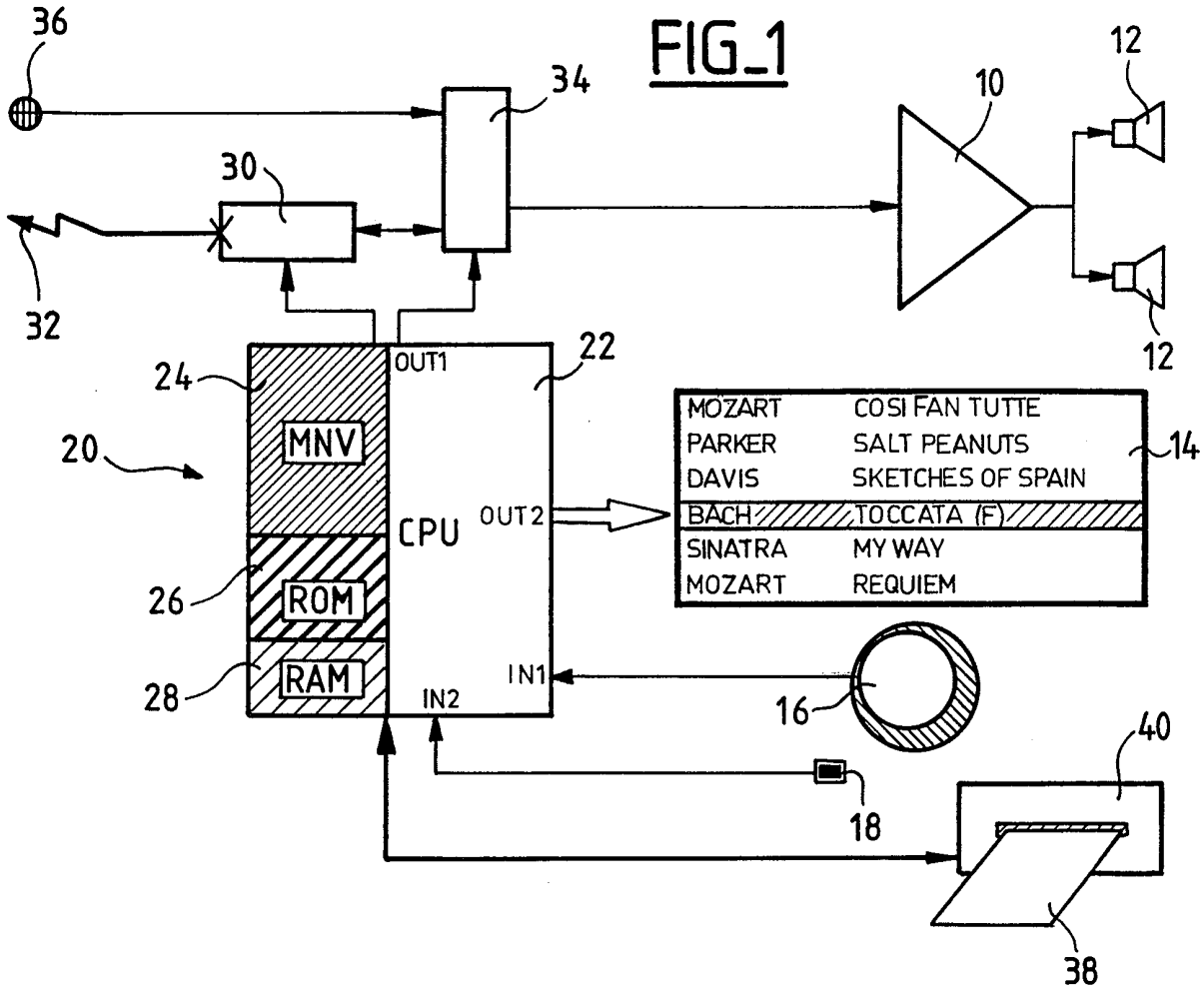

36
34
30
32
10
12
12
24
OUT1
22
20
MNV
CPU
OUT2
26
ROM
28
RAM
IN1
IN2
16
18
40
38
MOZART COSI FAN TUTTE
PARKER SALT PEANUTS
DAVIS SKETCHES OF SPAIN
BACH TOCCATA (F)
SINATRA MY WAY
MOZART REQUIEM
14

FIG_2

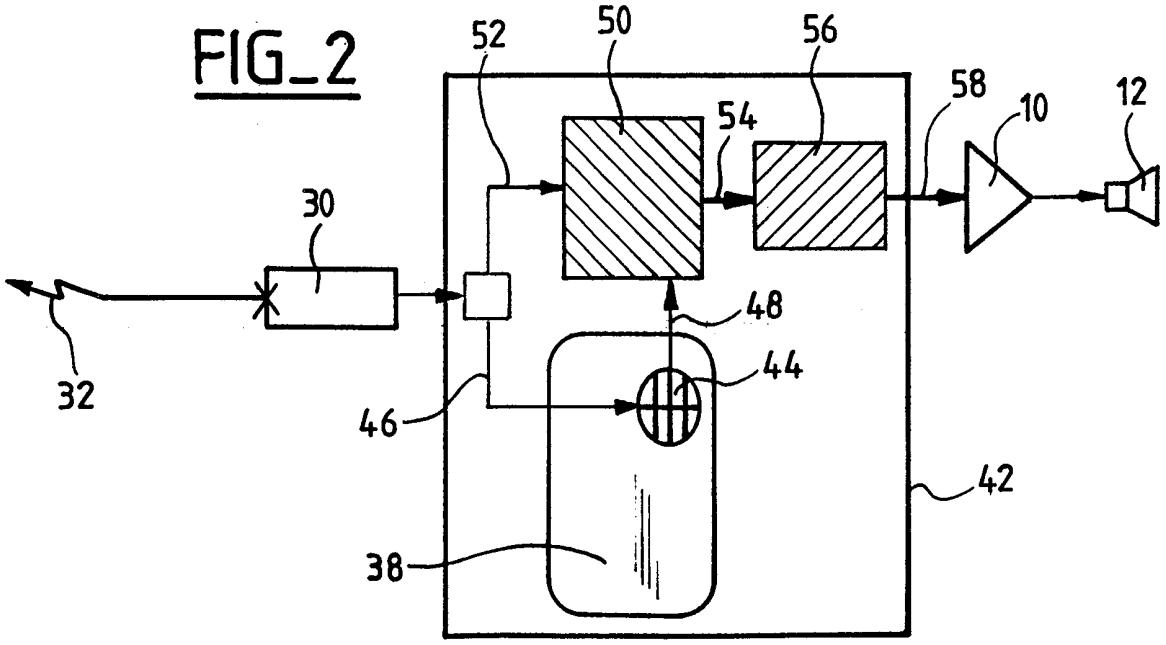
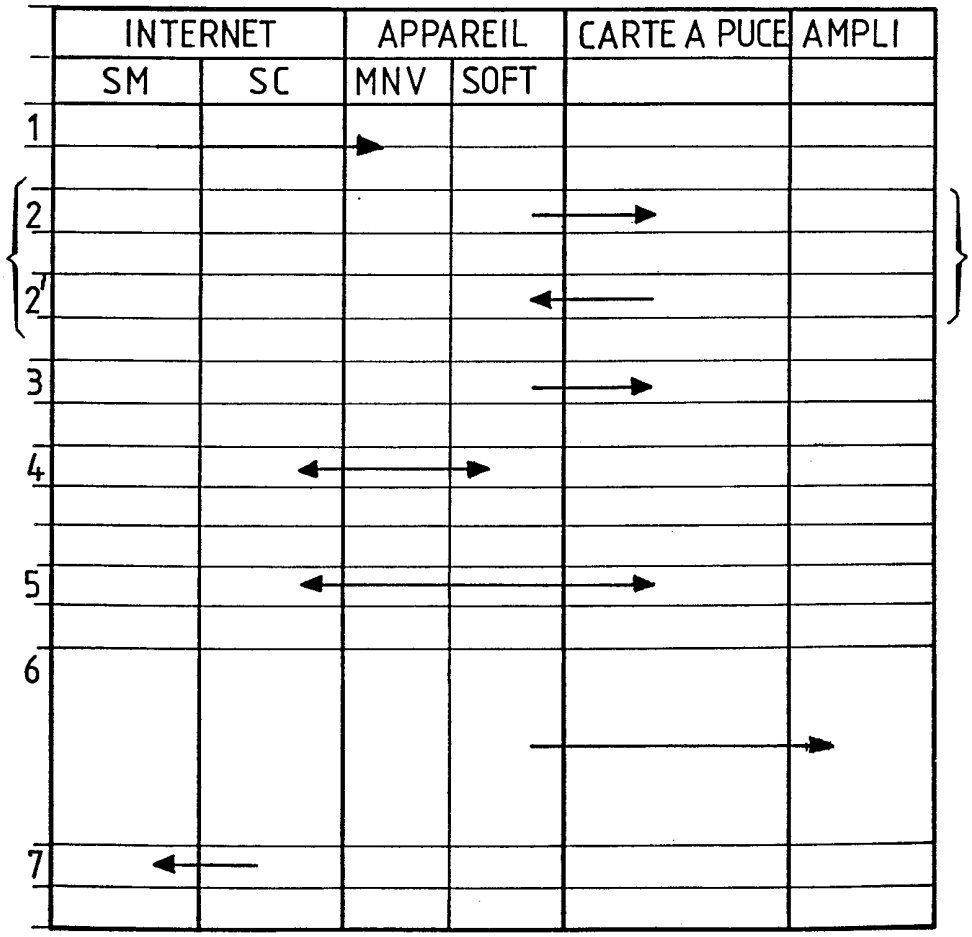

52
50
56
58
10
12
54
30
32
48
44
46
42
38

FIG_3


INTERNET
APPAREIL
CARTE A PUCE
AMPLI
SM
SC
MNV
SOFT
1
2
2'
3
4
5
6
7

INTERNATIONAL SEARCH REPORT

Inte ional Application No
PCT/FR 99/02017

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04N7/16 G10H1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04N G10H

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	PEYRET P ET AL: "SMART CARDS PROVIDE VERY HIGH SECURITY AND FLEXIBILITY IN SUBSCRIBERS MANAGEMENT" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS,US,IEEE INC. NEW YORK, vol. 36, no. 3, page 744-752 XP000162915 ISSN: 0098-3063 the whole document ---	1-5
Y	US 5 636 276 A (BRUGGER ROLF) 3 June 1997 (1997-06-03) the whole document ---	1-5
A	EP 0 723 371 A (THOMSON MULTIMEDIA SA) 24 July 1996 (1996-07-24) -----	

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 November 1999	16/11/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Van der Zaal, R

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/FR 99/02017

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5636276 A	03-06-1997	DE 4413451 A	14-12-1995
		AT 169762 T	15-08-1998
		DE 59503112 D	17-09-1998
		EP 0678851 A	25-10-1995
		ES 2119344 T	01-10-1998
		GR 3027730 T	30-11-1998
EP 0723371 A	24-07-1996	FR 2729521 A	19-07-1996
		JP 8307850 A	22-11-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 99/02017

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04N7/16 G10H1/00

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04N G10H

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	PEYRET P ET AL: "SMART CARDS PROVIDE VERY HIGH SECURITY AND FLEXIBILITY IN SUBSCRIBERS MANAGEMENT" IEEE TRANSACTIONS ON CONSUMER ELECTRONICS,US,IEEE INC. NEW YORK, vol. 36, no. 3, page 744-752 XP000162915 ISSN: 0098-3063 le document en entier	1-5
Y	US 5 636 276 A (BRUGGER ROLF) 3 juin 1997 (1997-06-03) le document en entier	1-5
A	EP 0 723 371 A (THOMSON MULTIMEDIA SA) 24 juillet 1996 (1996-07-24)	

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
9 novembre 1999	16/11/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Van der Zaal, R

1

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs . membres de familles de brevets

Der e internationale No
PCT/FR 99/02017

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 5636276 A	03-06-1997	DE 4413451 A	14-12-1995
		AT 169762 T	15-08-1998
		DE 59503112 D	17-09-1998
		EP 0678851 A	25-10-1995
		ES 2119344 T	01-10-1998
		GR 3027730 T	30-11-1998
EP 0723371 A	24-07-1996	FR 2729521 A	19-07-1996
		JP 8307850 A	22-11-1996