(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 811 503**
(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **00 08908**

(51) Int Cl^7 : **H 04 N 7/16**

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 07.07.00.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 11.01.02 Bulletin 02/02.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *INNOVATRON SA Société anonyme* — FR.

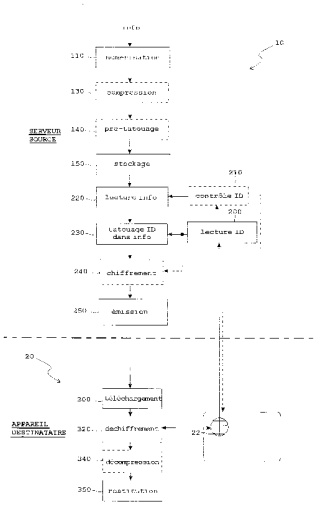
(72) **Inventeur(s) :** GRIEU FRANCOIS et MOLY JACQUES.

(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET BARDEHLE PAGENBERG ET PARTNER.

(54) PROCEDE DE DELIVRANCE DE SEQUENCES AUDIO, VIDEO OU TEXTUELLES PAR TELETRANSMISSION DE DONNEES NUMERIQUES INDIVIDUELLEMENT TATOUEES EN FONCTION DU DESTINATAIRE.

(57) Ce procédé permet la délivrance par un serveur source (10) à un appareil destinataire (20) comprenant un microcircuit (22), notamment un microcircuit de carte à puce, de séquences reproductibles par télétransmission de données numériques. Le procédé comprend les étapes de: a) transmission (200), de l'appareil au serveur, d'une requête de choix de séquence et d'une information d'identification du microcircuit; b) inclusion (230) par le serveur, dans la séquence choisie, d'un tatouage incorporant ladite information d'identification du microcircuit reçue par le serveur à l'étape a); c) émission (250) par le serveur de la séquence tatouée à l'étape b); d) réception (300) par l'appareil de cette séquence tatouée; et e) restitution (350) de la séquence par l'appareil.



FR 2 811 503 - A1

L'invention concerne l'acquisition de séquences reproductibles (telles que séquences audio, vidéo, textuelles ou analogues) auprès d'un serveur source par téléchargement de données.

Plus précisément, ce serveur source stocke des informations qui peuvent être délivrées à un appareil destinataire distant via un réseau téléinformatique, par exemple le réseau Internet.

Notamment, l'invention est applicable chaque fois que l'on cherche à délivrer à un appareil destinataire des informations à travers un réseau de communication non sécurisé, c'est-à-dire dans lequel le réseau ne permet pas d'identifier qui transmet ou reçoit l'information. Il est dans ce cas indispensable de réserver l'accès à cette information aux seuls usagers autorisés, grâce à un dispositif à microcircuit, notamment un microcircuit de carte à puce. Cette carte à puce, outre l'identification de l'usager, peut également participer au paiement de l'accès à l'information, et également au décryptage et/ou à la décompression de cette information.

On décrira l'invention principalement 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.

Le WO-A-00/11867 pour *"Procédé de délivrance certifiée d'une séquence audio, vidéo ou textuelle"* et le WO-A-00/11868 pour *"Procédé de délivrance et de paiement d'une séquence audio, vidéo ou textuelle"* (tous deux au nom d'Innovatron SA) décrivent la possibilité d'acquérir pour écoute des séquences audio, typiquement des œuvres musicales telles que des morceaux de musique ou des plages individuelles d'un enregistrement, convenablement sélectionnées par l'usager. Les morceaux de musique sont téléchargés sous forme de paquets de données numériques éventuellement signées, chiffrées et comprimées, et transmis depuis un site central au dispositif de l'usager. Le téléchargement est typiquement

réalisé via Internet, c'est-à-dire par les réseaux mondiaux interconnectés reliant des sites et des utilisateurs par des routages variables et multiples pour la transmission de données sous forme numérique.

On y prévoit avantageusement d'associer à l'appareil destinataire une carte à microcircuit pour participer à l'opération de décryptage et/ou de décompression des données ; le paiement des droits d'acquisition déclenche le téléchargement ou autorise les opérations de décryptage et/ou de décompression des données. Le WO-A-00/11866 pour *"Dispositif sécurisé décodeur d'informations chiffrées et comprimées"* (également au nom d'Innovatron SA) décrit une mise en œuvre particulière avantageuse du déchiffrement et de la décompression des signaux au moyen d'une telle carte à microcircuit.

L'un des risques qui subsiste, pour le producteur des informations qui ont été transmises, est que les informations une fois acquises par un utilisateur, celui-ci utilise non seulement ces informations après déchiffrement et décompression pour son usage personnel, mais également à des fins de duplication non autorisée.

Faute de pouvoir empêcher une telle pratique, les diffuseurs d'informations cherchent à la dissuader en incorporant dans le flux de données délivrées au destinataire un "filigrane" (*watermarking*) ou "tatouage" pratiquement imperceptible (c'est à dire inaudible ou invisible), par l'utilisateur, mais qui permet en cas de découverte d'une copie non autorisée, d'identifier le serveur ayant délivré l'information originelle.

De façon générale, cette technique consiste à ajouter au message musical une information non perceptible par l'utilisateur final, mais pouvant être révélée par des techniques appropriées, décrites 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* d'Aris Technologies (www.musicode.com) et *Audiomark* d'Alpha Tec Ltd. (www.alphatecltd.com).

Pour un signal analogique, la technique la plus simple combine par addition un signal d'identification de faible niveau codant l'information d'identi-

fication 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.

Un tel tatouage des données diffusées par le serveur ne procure cependant qu'une traçabilité limitée, car il ne révèle que des informations propres au serveur (identité de l'information source, horodatage, etc.) sans donner d'information sur le destinataire de l'information, qui peut ainsi rester anonyme.

L'un des but de l'invention est de pallier cette limitation en proposant une technique de délivrance de données tatouées offrant une meilleure traçabilité, tout en restant compatibles avec les matériels existants, en particulier micro-ordinateurs, lecteurs de cartes à microcircuit, cartes son, baladeurs numériques, graveurs de cédéroms, etc.

En effet, une technique telle que celle décrite dans le WO-A-00/11866 précité, si elle permet d'empêcher l'accès à une information musicale sous une forme numérique exploitable, est incompatible avec les standards actuels de lecteurs de carte à microcircuit, de cartes son, de baladeurs numériques et de graveurs de cédéroms. Elle ne peut donc être mise en œuvre que dans le cas d'un système "fermé", où les informations ne peuvent être diffusées qu'à des utilisateurs autorisés, par exemple des abonnés, et sous une forme impliquant nécessairement certaines restrictions d'utilisation.

La présente invention a une utilité certaine dans ce contexte, mais elle présente aussi l'avantage de permettre une mise en œuvre universelle ne nécessitant du côté de l'utilisateur aucun décodeur spécifique ni adaptation particulière d'une configuration matérielle préexistante.

Le procédé de l'invention, comme expliqué plus haut, est un procédé de délivrance par un serveur source à un appareil destinataire comportant un microcircuit, notamment un microcircuit de carte à puce, de séquences reproductibles, cette délivrance étant opérée par télétransmission de données numériques représentatives de ces séquences.

Selon l'invention, le procédé comprend les étapes suivantes :

a) transmission, de l'appareil au serveur, d'une requête de choix de séquence et d'une information d'identification du microcircuit,

b) inclusion par le serveur, dans la séquence choisie, d'un tatouage incorporant ladite information d'identification du microcircuit reçue par le serveur à l'étape a),

c) émission par le serveur de la séquence tatouée à l'étape b),

d) réception par l'appareil de cette séquence tatouée, et

e) restitution de la séquence par l'appareil.

Selon diverses caractéristiques subsidiaires avantageuses :

- il est prévu en outre, entre les étapes a) et b), une étape de contrôle d'authenticité de l'information d'identification du microcircuit ;
- il est prévu en outre, entre les étapes b) et c), une étape de chiffrement par le serveur de la séquence choisie tatouée et, entre les étapes d) et e), une étape de déchiffrement, éventuellement partiel, par l'appareil de la séquence reçue ;
- dans ce dernier cas, l'étape de chiffrement par le serveur peut comprendre avantageusement un premier chiffrement, rapide, et un second chiffrement, complexe, et l'étape de déchiffrement par l'appareil comprend un premier déchiffrement, homologue du premier chiffrement et mis en œuvre hors du microcircuit, et un second déchiffrement, homologue du second chiffrement et mis en œuvre dans le microcircuit, qui délivre les clefs du premier déchiffrement ;
- il peut également être en outre prévu, après l'étape de déchiffrement par l'appareil, une étape de rechiffrement mise en œuvre au sein du microcircuit ;
- les séquences sont mémorisées par le serveur sous forme comprimée ou sont préalablement comprimées par le serveur avant l'étape b), et il est prévu en outre, entre les étapes d) et e), une étape de décompression par l'appareil de la séquence reçue ;

- les séquences mémorisées par le serveur incorporent un pré-tatouage par une information commune indépendante de l'information d'identification du microcircuit, ou sont préalablement pré-tatouées par le serveur avant l'étape b).

◊

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

la figure 1 illustre de façon schématique les différentes étapes du procédé de l'invention.

La figure 2 illustre, sous forme de blocs fonctionnels, différents éléments impliqués dans une mise en œuvre particulière du procédé de l'invention.

◊

Le procédé de l'invention est mis en œuvre à partir d'une source d'information 10, par exemple un micro-ordinateur constituant un serveur Internet, ou même un simple support de stockage tel que cédérom ou DVD-ROM.

Cette source d'information est reliée à un appareil destinataire 20 qui peut notamment être un dispositif de type "tuner Internet" tel que décrit dans les WO-A-00/11867 et WO-A-00/11868 précités. Un tel tuner Internet comporte des moyens, intégrés ou séparés, de reproduction sonore, divers circuits de décompression, décryptage, paiement, contrôle d'accès, etc., notamment des circuits mettant en œuvre une ou plusieurs cartes à microcircuit, ainsi que des moyens de connexion à un site distant (site central ou bien délocalisé en plusieurs sites).

L'appareil destinataire 20 est équipé d'un microcircuit de sécurité 22, notamment le microcircuit d'une carte à puce, capable de stocker des informations dans une mémoire permanente et d'effectuer des calculs cryptographiques sur des informations (clefs) stockées dans ce microcircuit, et non lisibles de l'extérieur du microcircuit.

Le microcircuit de sécurité 22 peut être par exemple un *ST16SF48* de STMicroelectronics, encarté dans une carte selon ISO/IEC 7816-1 à -3, et

relié par un lecteur de carte à microcircuit conforme à ces standards ou de manière équivalente (aussi bien amovible que permanente) par exemple à travers un bus de type USB.

La mémoire du microcircuit 22 contient au moins un identifiant propre au microcircuit, tel que numéro de série ou de contrat, qui le différencie des autres microcircuits du même modèle utilisés dans l'application de l'invention. L'information originelle destinée à être diffusée est tout d'abord numérisée (étape 110) et avantageusement comprimée (étape 130), par exemple selon ISO/IEC 11172 - MPEG 1.

Optionnellement, l'information numérisée et comprimée peut faire l'objet, de manière en elle-même connue, d'un pré-tatouage (étape 140) avec des informations communes à de multiples diffusions ultérieures, par exemple une identification des ayants-droit de l'information considérée ou du serveur.

Ce pré-tatouage est opéré selon l'une des diverses techniques connues mentionnées plus haut en tenant compte du fait que, dans certaines techniques, ce pré-tatouage peut être opéré avant compression, c'est-à-dire que l'ordre des étapes 130 et 140 peut être inversé en fonction des besoins.

L'information ainsi traitée est alors stockée (étape 150), par exemple inscrite sur un disque dur de manière à permettre sa relecture chaque fois que la diffusion en sera demandée par un utilisateur.

Lorsqu'un utilisateur souhaite télécharger une information particulière qu'il souhaite obtenir, il transmet à partir de son appareil 20, outre une requête de sélection de l'information (pour indiquer par exemple au serveur la séquence musicale qu'il a choisie et qu'il souhaite obtenir), l'identifiant du microcircuit 22.

Cet identifiant de microcircuit est lu par le serveur (étape 200) qui opère très préférentiellement un contrôle (étape 210) pour être certain que cet identifiant est authentique, par exemple en soumettant le microcircuit à une épreuve et en vérifiant cette épreuve.

A titre d'exemple d'épreuve, on peut utiliser un cryptosystème symétrique tel que DES avec une clef secrète KA globale ; à la fabrication du microcircuit, on inscrit dans celui-ci l'identifiant I et une clef cryptographique dérivée KAI = DES(KA,I). Pour authentifier le microcircuit, le serveur choi-

sit au hasard et transmet au microcircuit une épreuve E ; le microcircuit calcule alors R = DES(KAI,E), puis le serveur vérifie que R = DES(DES(KA,I),E), ce qui démontre l'authenticité du microcircuit et de son identifiant I.

En variante, on peut avantageusement utiliser un cryptosystème asymétrique à clef publique telle que RSA, avec l'avantage que le serveur n'a alors pas besoin de disposer d'une information secrète.

Une fois l'identifiant du microcircuit lu et contrôlé, le serveur lit (étape 220) l'information demandée par le destinataire, qui avait été stockée à l'étape 150.

Le serveur opère alors (étape 230) un tatouage de l'identifiant, lu à l'étape 200, dans l'information demandée, lue à l'étape 220.

Le tatouage réalisé ainsi en amont de toute diffusipn par le serveur peut l'être dans un environnement sûr, à l'abri des risques de fraude ou d'intrusion dans le système.

Très préférentiellement, le serveur opère alors (étape 240) un chiffrement de l'information, également à partir de l'identifiant lu à l'étape 200, de telle manière que la possession d'un microcircuit adéquat, de préférence seulement celui possédant l'identifiant tatoué, soit nécessaire au déchiffrement.

Il peut également signer l'information de manière que l'appareil de l'utilisateur puisse détecter une altération éventuelle.

On notera que cette étape de chiffrement de l'information à partir d'un identifiant du microcircuit (ou d'un autre identifiant spécifique à la carte et/ou à l'utilisateur) est une étape en elle-même connue et qu'il y a lieu de distinguer de l'étape 230 de tatouage selon l'invention, incorporant spécifiquement et nécessairement un identifiant du microcircuit ou donnée analogue.

L'étape de chiffrement 240 quant à elle, peut être spécifique de la carte, c'est-à-dire nécessiter la lecture d'une donnée spécifique à celle-ci, mais cette caractéristique n'est pas nécessaire, et il est possible (bien que moins avantageux) de prévoir un chiffrement non spécifique à la carte.

Enfin (étape 250) le serveur transmet à l'appareil destinataire 20 l'information ainsi traitée.

Le destinataire télécharge alors (étape 300) l'information issue des trai-

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

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 ADSL ou sur réseau câblé, ou transmission de données numérisées par satellite sur les canaux à grand débit de télévision.

Si une étape 240 de chiffrement a été prévue en amont, l'appareil destinataire opère un déchiffrement (étape 320) de l'information reçue, au moyen du microcircuit 22.

Si une étape (non indiquée sur les dessins) de signature a été prévue en amont, l'appareil destinataire opère une vérification.

Si une étape 130 de compression a été prévue en amont, l'appareil destinataire opère une décompression (étape 340) de l'information déchiffrée.

Enfin (étape 350) l'appareil restitue l'information demandée.

Très avantageusement, si un chiffrement/déchiffrement est prévu (étapes 240 et 320) on utilise un procédé de chiffrement à deux niveaux (par exemple de type connu en soi), dans lequel la masse de l'information est chiffrée et déchiffrée par un premier cryptosystème rapide, dans lequel n'intervient pas le microcircuit, et dont la clef est calculée par un second cryptosystème. Le microcircuit intervient pour la production des clefs et la mise en œuvre du second déchiffrement 320. L'information peut éventuellement être divisée en séquences numérotées, chiffrées indépendamment en fonction de leur numéro.

On peut par exemple utiliser pour le cryptosystème rapide un OU exclusif avec une séquence cryptographique générée par un automate fini (combinaison de registres à décalage) et, pour le cryptosystème lent, un système à base DES avec une clef secrète KC globale. A la fabrication du microcircuit, on inscrit dans celui-ci l'identifiant I et une clef cryptographi-

que dérivée KCI = DES (KC,I). A l'étape de chiffrement 240, pour la séquence n° N destinée au microcircuit d'identifiant I, le serveur calcule une clef de séquence KS = DES (DES(KC,I),N), initialise le cryptosystème rapide avec cette valeur, puis chiffre la séquence avec le cryptosystème rapide. A l'étape de déchiffrement 320, le microcircuit calcule DES (KCI,N) et transmet ce résultat, qui initialise le cryptosystème rapide, permettant ainsi à celui-ci de déchiffrer la séquence.

Une carte donnée ne peut ainsi servir à déchiffrer que les messages qui ont été tatoués pour elle.

Dans la mise en œuvre que l'on vient de décrire, l'information délivrée à l'utilisateur en sortie de carte à microcircuit est une information déchiffrée et comprimée (la décompression de l'étape 340 n'ayant pas besoin d'être opérée dans un environnement sécurisé tel que celui d'un microcircuit de carte à puce).

En variante, on peut prévoir que l'information délivrée en sortie du microcircuit est une information qui n'est que partiellement déchiffrée, ou encore une information rechiffrée par le microcircuit ("surchiffrement") avant transfert vers l'extérieur, afin de ne pas être utilisable si elle est interceptée.

Ce rechiffrement est opéré dans un environnement sûr (celui du microcircuit), à l'état numérique et comprimé, de manière à permettre le stockage numérique de l'information sous forme tatouée, sans possibilité d'élimination ou de filtrage de ce tatouage.

Exemple de mise en oeuvre

La figure 2 illustre, sous forme de blocs fonctionnels, différents éléments impliqués dans un exemple particulier de mise en œuvre du procédé de l'invention.

Cette configuration est destinée à permettre la diffusion d'un contenu multimédia (audio, vidéo, jeux, etc.) du serveur source 10, où ce contenu multimédia est préparé et rendu disponible de la manière que l'on va décrire, vers l'appareil destinataire d'un client :

- en s'assurant que le contenu ne sera disponible que pour les clients qui se seront acquitté d'un droit de visualisation,

- en permettant également de garantir les paiements et faire respecter les règles définies par les ayants-droit (par exemple un nombre limité de visualisations autorisées),
- en procurant enfin une certaine traçabilité permettant, en cas de fraude, de pouvoir remonter au serveur et/ou déterminer l'acheteur à l'origine de la copie.

Le client dispose à cet effet d'un appareil destinataire 20 qui est un ensemble matériel et logiciel constitué autour d'un équipement de type connu tel que micro-ordinateur, décodeur de TV numérique (notamment du type "*set top box*"), ou encore téléphone portable apte à échanger des données numériques conformément aux normes GSM, WAP, GPRS, UMTS ou autres.

A cet équipement sont associés :

- un logiciel d'application client 21,
- un microcircuit 22, par exemple le microcircuit d'une carte à puce accessible via un lecteur connecté à un micro-ordinateur ou intégré à un décodeur,
- éventuellement un moyen de stockage de masse 23 tel que disque dur, mémoire flash, etc.,
- un périphérique 24 de restitution du contenu multimédia, par exemple moniteur de télévision, amplificateur audio, assistant numérique personnel, graveur de disque compact, etc.

Le contenu multimédia est tout d'abord préparé au niveau du serveur source 10, de la manière suivante.

Ce contenu, désigné "contenu de valeur" sur la figure 2, est accompagné de "règles d'usage" qui définissent les restrictions d'utilisation, le nombre de copies utilisées, la durée de péremption, etc. Ces règles peuvent être éventuellement des règles non spécifiques, appliquées par défaut lorsque le contenu de valeur n'est associé à aucune règle propre.

Le contenu multimédia peut également comprendre des informations, désignées "contenu sans valeur", ne nécessitant pas de mesures de protection particulières, par exemple biographie de l'interprète, paroles d'une chanson, jaquette de présentation, etc.

Les règles d'usage sont incorporées au contenu de valeur, par exemple et de manière en elle-même connue par tatouage, puis l'ensemble est dé-

coupé en blocs, signé et chiffré, pour produire enfin :

- d'une part le contenu de valeur, sous forme de blocs signés et chiffrés, ce contenu de valeur incorporant les règles d'usage,
- d'autre part, un "titre d'accès" associé, qui permettra de contrôler l'accès au contenu multimédia et sa restitution par l'appareil destinataire de la manière que l'on indiquera plus bas (le terme "titre" étant entendu dans son acception juridique (comme dans "titre de transport" ou "titre de créance"), c'est-à-dire comme certificat constatant un acte juridique ou matériel susceptible de produire des effets – ici l'autorisation de reproduction ou de duplication du contenu.
- et éventuellement le contenu sans valeur, simplement découpé en blocs.

Cet ensemble de données est stocké par le serveur, ce stockage correspondant à l'étape 150 de la figure 1 décrite plus haut.

L'utilisateur client peut accéder à ces données de la manière suivante.

Le transaction serveur-client s'effectue de manière sécurisée entre le serveur et le microcircuit 22, selon des techniques en elles-mêmes connues, le logiciel d'application client 21 servant de passerelle entre le serveur et le microcircuit.

Pour assurer la sécurisation, le microcircuit et le serveur échangent des certificats, avec au moins :

- un premier certificat, du microcircuit vers le serveur, pour certifier que l'utilisateur du microcircuit a bien acquitté le prix correspondant au contenu de valeur précisément identifié, et
- un second certificat, du serveur vers le microcircuit, pour transmettre à ce dernier le titre d'accès, ce titre pouvant éventuellement contenir une clef de décryptage.

Ces certificats sont signés et cryptés à l'aide de clefs conservées d'une manière sécurisée dans le microcircuit et dans le serveur. Les transactions entre ces deux organes sont ainsi sécurisées, même au travers d'un canal non sûr (réseau téléphonique, réseau câblé, Internet, etc.).

Une fois ces opérations effectuées, l'ensemble des blocs du contenu demandé (contenu de valeur et contenu sans valeur) est transmis à l'appareil destinataire.

Toute opération en provenance ou à destination d'un périphérique, y com-

pris le périphérique de restitution local 24, ne peut se faire qu'au travers du microcircuit 22, ce dernier ne répondant à cet effet qu'à des commandes dûment signées et authentifiées.

Après préparation et transfert du contenu multimédia, l'appareil destinataire dispose du contenu de valeur, crypté avec les règles qui doivent en régir l'accès, et éventuellement d'un ensemble d'informations non secrètes (contenu sans valeur, qui peut être affiché par le périphérique de restitution 24, ou bien simplement ignoré).

On va tout d'abord décrire une mise en œuvre dans laquelle le contenu de valeur est restitué en "*streaming*" c'est-à-dire restitué sous une forme intelligible aux sens humains au fur et à mesure de sa réception, sensiblement à la vitesse à laquelle il est transmis, sans stockage permanent dans le dispositif utilisateur (qui ne stocke qu'une quantité limitée d'informations, par exemple correspondant à une seconde de restitution pour amortir les fluctuations de courte durée du moyen de transmission).

Les blocs sont transmis à l'appareil destinataire qui émet une commande de déchiffrement au microcircuit en lui passant le bloc. Le microcircuit n'accepte bien entendu ces commandes que si elles ont été convenablement signées et authentifiées. Il calcule la signature du bloc et vérifie les conditions d'accès, en particulier le fait que l'utilisateur a bien le droit de recevoir le contenu en "streaming" et qu'il s'est bien acquitté du paiement des droits de lecture ; il utilise pour cela le titre d'accès qu'il a reçu suite au paiement, avec les règles qui ont été tatouées et/ou incluses dans le contenu de valeur.

Si toutes les conditions sont bien respectées, le microcircuit déchiffre le contenu, le rechiffre éventuellement avec une clef associée au périphérique de restitution, et transmet ce contenu au périphérique de restitution 24.

Le périphérique 24 peut alors restituer le contenu multimédia.

Lorsque le streaming n'est pas possible ou pas souhaité, le contenu est simplement téléchargé, c'est-à-dire que les informations correspondantes sont stockées intégralement et de manière permanente dans le moyen de stockage 23 pour restitution ultérieure.

La procédure décrite ci-dessus est alors adaptée de la manière suivante.

Le logiciel d'application client 21 sert de passerelle entre le serveur sour-

ce 10, le microcircuit 22 et le périphérique de restitution 24. Le périphérique 24 et le microcircuit 22 peuvent éventuellement s'identifier, par exemple par échange de certificats contenant des données aléatoires. Ils peuvent également échanger des clefs entre eux pour communiquer de manière chiffrée.

Le logiciel d'application client 21 transmet des commandes signées et cryptées au microcircuit 22 en y attachant les blocs. Bien entendu, le microcircuit n'accepte ces commandes que si elles ont été convenablement signées et authentifiées

Le microcircuit calcule la signature du bloc et vérifie les conditions d'accès, en particulier le fait que l'utilisateur a bien le droit de copier le contenu et qu'il s'est bien acquitté du paiement des droits de lecture ; il utilise pour cela le titre d'accès qu'il a reçu suite au paiement, avec les règles qui ont été tatouées et incluses dans le contenu de valeur.

Si toutes les conditions sont bien respectées, le microcircuit déchiffre le contenu, le rechiffre éventuellement avec une clef associée au périphérique de restitution, et transmet ce contenu au périphérique 23, qui peut alors stocker ce contenu multimédia, à partir duquel la restitution sera effectuée ultérieurement..

Dans le cas où l'utilisateur tente de transférer le contenu téléchargé vers un autre moyen de stockage, le microcircuit 22 n'autorisera la recopie que pour un contenu dont il a les droits d'accès, à moins qu'il ne s'agisse d'un contenu marqué "libre de droits". Dans le cas où les droits sont présents, il n'y a pas en principe de recopie, puisque le contenu est déjà stocké sur le moyen de stockage de l'appareil de l'utilisateur.

REVENDICATIONS

1. Un procédé de délivrance par un serveur source (10) à un appareil destinataire (20) comportant un microcircuit (22), notamment un microcircuit de carte à puce, de séquences reproductibles, cette délivrance étant opérée par télétransmission de données numériques représentatives de ces séquences, procédé caractérisé par les étapes suivantes :

a) transmission (200), de l'appareil au serveur, d'une requête de choix de séquence et d'une information d'identification du microcircuit,

b) inclusion (230) par le serveur, dans la séquence choisie, d'un tatouage incorporant ladite information d'identification du microcircuit reçue par le serveur à l'étape a),

c) émission (250) par le serveur de la séquence tatouée à l'étape b),

d) réception (300) par l'appareil de cette séquence tatouée, et

e) restitution (350) de la séquence par l'appareil.

2. Le procédé de la revendication 1, comprenant en outre, entre les étapes a) et b), une étape (210) de contrôle d'authenticité de l'information d'identification du microcircuit.

3. Le procédé de la revendication 1, comprenant en outre, entre les étapes b) et c), une étape (240) de chiffrement par le serveur de la séquence choisie tatouée et, entre les étapes d) et e), une étape (320) de déchiffrement par l'appareil de la séquence reçue.

4. Le procédé de la revendication 3, dans lequel l'étape (240) de chiffrement par le serveur comprend un premier chiffrement, rapide, et un second chiffrement, complexe, et l'étape de déchiffrement par l'appareil comprend un premier déchiffrement, homologue du premier chiffrement et mis en œuvre hors du microcircuit, et un second déchiffrement, homologue du second chiffrement et mis en œuvre dans le microcircuit, qui délivre les clefs du premier déchiffrement.

5. Le procédé de la revendication 3, comprenant en outre, après l'étape (320) de déchiffrement par l'appareil, une étape de rechiffrement mise en

œuvre au sein du microcircuit.

6. Le procédé de la revendication 3, dans lequel l'étape (320) de déchiffrement par l'appareil est une étape de déchiffrement partiel.

7. Le procédé de la revendication 1, dans lequel les séquences sont mémorisées par le serveur sous forme comprimée ou sont préalablement comprimées (130) par le serveur avant l'étape b), et dans lequel il est prévu en outre, entre les étapes d) et e), une étape (340) de décompression par l'appareil de la séquence reçue.

8. Le procédé de la revendication 1, dans lequel les séquences mémorisées par le serveur incorporent un pré-tatouage par une information commune indépendante de l'information d'identification du microcircuit, ou sont préalablement pré-tatouées (140) par le serveur avant l'étape b).

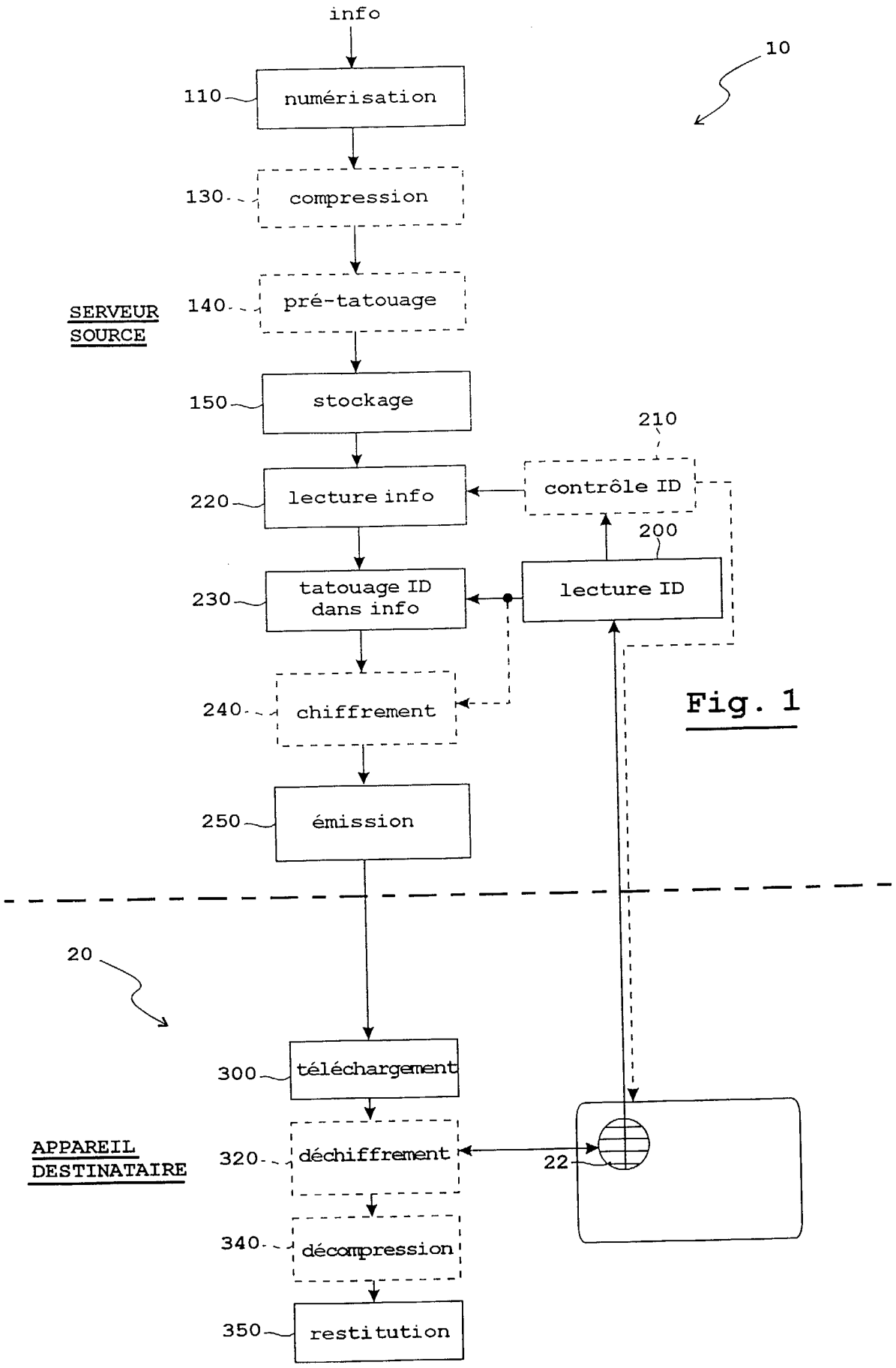

info
10
110
numérisation
130
compression
SERVEUR SOURCE
140
pré-tatouage
150
stockage
210
contrôle ID
220
lecture info
200
lecture ID
230
tatouage ID dans info
240
chiffrement
250
émission
20
300
téléchargement
APPAREIL DESTINATAIRE
320
déchiffrement
22
340
décompression
350
restitution

Fig. 1

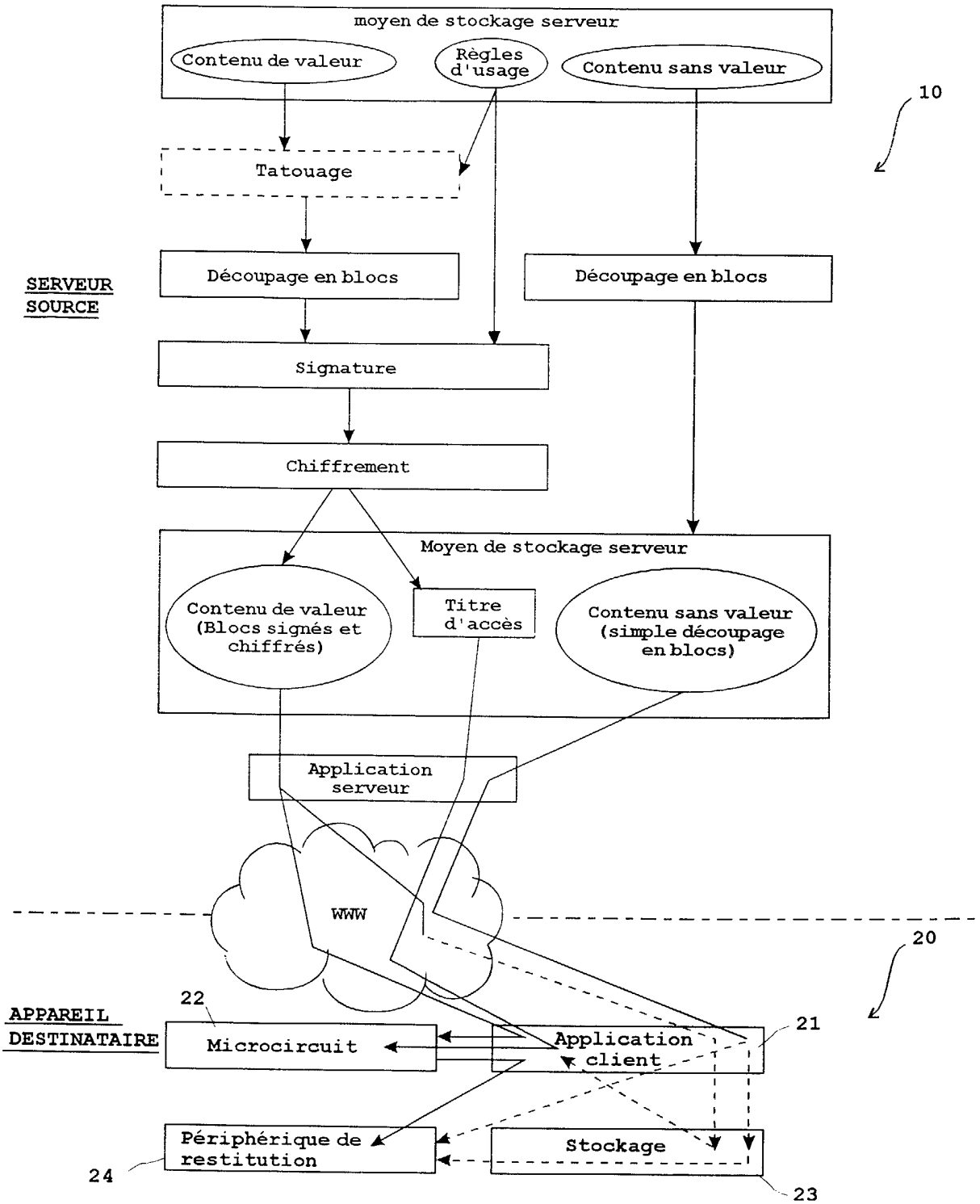

moyen de stockage serveur
Contenu de valeur
Règles d'usage
Contenu sans valeur
10
Tatouage
SERVEUR SOURCE
Découpage en blocs
Découpage en blocs
Signature
Chiffrement
Moyen de stockage serveur
Contenu de valeur (Blocs signés et chiffrés)
Titre d'accès
Contenu sans valeur (simple découpage en blocs)
Application serveur
WWW
20
APPAREIL DESTINATAIRE
22
Microcircuit
Application client
21
Périphérique de restitution
24
Stockage
23

Fig. 2

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2811503

N° d'enregistrement national

FA 590141
FR 0008908

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
Y	WO 00 30354 A (DISCOVERY COMMUNICAT INC) 25 mai 2000 (2000-05-25) * page 20, ligne 13 - page 26, ligne 28 * * page 36, ligne 30 - page 39, ligne 4 * * page 46, ligne 7 - page 47, ligne 30 * * figures 6,10,13 * ---	1-8	H04N7/16
Y	WO 99 19822 A (MICROSOFT CORP) 22 avril 1999 (1999-04-22) * page 5, ligne 22 - page 19, ligne 14 * * figures 1-7 * ---	1-8	
D,A	WO 00 11867 A (MORENO ROLAND ;INNOVATRON SOCIETE ANONYME (FR)) 2 mars 2000 (2000-03-02) * page 2, ligne 28 - page 4, ligne 17 * * page 10, ligne 8 - ligne 26 * -----	1-8	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.CL.7)
			H04N

Date d'achèvement de la recherche	Examinateur
26 mars 2001	Van der Zaal, R

CATÉGORIE DES DOCUMENTS CITÉS

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 bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)