(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** **2 892 222**

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **05 10566**

(51) Int Cl[8] : **G 11 B 20/00** (2006.01), G 11 B 20/10, G 06 F 12/14

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 17.10.05.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 20.04.07 Bulletin 07/16.

(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) :** *THOMSON LICENSING Société anonyme* — FR.

(72) **Inventeur(s) :** DIASCORN JEAN LOUIS, DURAND ALAIN et LELIEVRE SYLVAIN.

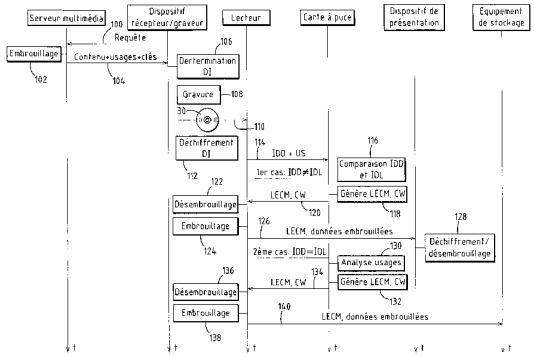
(73) **Titulaire(s) :**

(74) **Mandataire(s) :** CABINET LAVOIX.

(54) METHODE DE GRAVURE, DE MISE A DISPOSITION ET DE DISTRIBUTION SECURISEE DE DONNEES NUMERIQUES, DISPOSITIF D'ACCES ET GRAVEUR.

(57) L'invention concerne une méthode de gravure sécurisée de données numériques représentatives d'un contenu multimédia comportant une étape (108) de gravure desdites données numériques sur un disque sécurisé (30) par un graveur appartenant à un domaine sécurisé déterminé comprenant plusieurs équipements et défini par un identifiant (IDD) propre à tous les équipements du domaine, caractérisée en ce qu'elle comporte en outre une étape (108) de gravure sur le disque sécurisé (30) de l'identifiant (IDD) du domaine du graveur pour définir ce domaine comme seul domaine dans lequel la reproduction/copie du contenu multimédia est autorisé.

L'invention concerne également une méthode de mise à disposition et de distribution sécurisée de données numériques, un dispositif d'accès et un graveur.



FR 2 892 222 - A1

La présente invention concerne une méthode de gravage, de mise à disposition et de distribution sécurisée de données numériques représentatives d'un contenu multimédia.

Pour éviter la copie illégale de contenu multimédia, il est connu notamment par le document JP 2001/195826, un appareil comprenant une mémoire dans laquelle est enregistrée un identifiant propre à chaque appareil et différent des identifiants des autres appareils. L'appareil est adapté pour enregistrer des données numériques et son identifiant propre sur un support d'enregistrement lors de chaque gravure. Avant la lecture des données numériques, il est propre à comparer son identifiant à l'identifiant lu sur le support d'enregistrement et à présenter les données numériques uniquement lorsque l'identifiant enregistré sur le support d'enregistrement correspond à son identifiant.

Cet appareil respecte les droits de propriété mais ne permet de présenter les données numériques que sur un unique et même appareil.

Pour permettre une distribution plus large des données numériques tout en respectant les droits de propriété attachés à ceux-ci, il est connu de sécuriser des données numériques gravées sur un DVD sécurisé par des méthodes de protection de données telle que la méthode d'embrouillage de contenu CSS (de l'anglais CSS : Content Scrambling System).

Toutefois, avec cette méthode, les données numériques gravées sur le DVD sécurisé sont lisibles par tout lecteur autorisé, mais ne peuvent pas être copiées ou reproduites.

Par ailleurs, il est connu des méthodes de protection de données dans un domaine telles que la méthode de marque déposée « SmartRight » décrite dans le document « SmartRight Technical white paper, Version 1.7, January 2003, Thomson » et la méthode de marque déposée « eXtensible Content Protection » décrite dans les documents « xCP : eXtensible Content Protection. 2003. IBM » et « xCP Cluster Protocol, IBM Presentation to Copy Protection Technical Working Group, July 18, 2002 ». Ces méthodes permettent d'embrouiller les données numériques selon un protocole de chiffrement décodable uniquement par les équipements appartenant au même domaine. Les données numériques ainsi chiffrées ne peuvent être présentées ou copiées/reproduites que par les équipements appartenant à un domaine.

Toutefois, ces données numériques ne peuvent pas être partagées avec une personne qui n'a pas accès à ce domaine. Il n'est donc pas possible de partager ces données numériques avec un ami ou une connaissance.

Il est également connu notamment par le document US 2004/0230532, un système de gestion de copies de données numériques autorisant une ou plusieurs reproductions/copies de celles-ci par un même graveur mais interdisant la copie par un autre graveur.

Ce système comprend un serveur accessible par le réseau Internet et des graveurs/lecteurs particuliers destinés aux utilisateurs. Lors de chaque gravure, chaque graveur/lecteur est adapté pour transmettre au serveur un identifiant qui lui est propre, un identifiant du DVD et un identifiant du contenu lu sur le DVD. Le serveur contient une base de données, des moyens d'inscription des identifiants reçus par le graveur et des moyens de comparaison des identifiants stockés dans sa base de données et des identifiants reçus par le graveur pour vérifier si les identifiants envoyés par un graveur correspondent aux identifiants déjà enregistrés dans la base de données.

Toutefois, ce système est complexe et nécessite la gestion d'une base de données contenant un nombre important de données.

L'invention a pour but de proposer une méthode de distribution sécurisée de données numériques permettant un certain degré de partage des données numériques tout en respectant les droits de propriété attachés à ceux-ci.

A cet effet, l'invention a pour objet une méthode de gravure sécurisée de données numériques représentatives d'un contenu multimédia comportant une étape de gravure desdites données numériques sur un disque sécurisé par un graveur appartenant à un domaine sécurisé déterminé comprenant plusieurs équipements et défini par un identifiant propre à tous les équipements du domaine, caractérisée en ce qu'elle comporte une étape de gravure sur le disque sécurisé de l'identifiant du domaine du graveur pour définir ce domaine comme seul domaine dans lequel la reproduction/copie du contenu multimédia est autorisée.

Suivant des modes particuliers de réalisation, la méthode de gravure comporte une ou plusieurs des caractéristiques suivantes :

- une étape de gravure sur le disque sécurisé de droits de reproduction attachés au contenu multimédia, les droits de reproduction définissant si le

contenu multimédia est librement reproductible/copiable, si le contenu multimédia est reproductible/copiable dans le domaine déterminé uniquement ou si le contenu multimédia n'est pas reproductible/copiable.

L'invention concerne également, selon un deuxième aspect, une méthode de mise à disposition de données numériques représentatives d'un contenu multimédia dans un domaine sécurisé spécifique défini par un identifiant, à partir d'un dispositif d'accès au domaine sécurisé spécifique comprenant des moyens de mémorisation de l'identifiant de ce domaine spécifique, comprenant les étapes suivantes :

- lecture sur un disque sécurisé comprenant lesdites données numériques d'un identifiant d'un domaine sécurisé déterminé par le dispositif d'accès, l'identifiant étant préalablement gravé sur le disque sécurisé ;

- comparaison de l'identifiant lu sur le disque sécurisé avec l'identifiant stocké dans les moyens de mémorisation du dispositif d'accès ; et

- lorsque l'identifiant lu sur le disque sécurisé ne correspond pas à l'identifiant stocké dans les moyens de mémorisation du dispositif d'accès, mise à disposition par le dispositif d'accès des données numériques de façon à autoriser un premier mode d'exploitation des données numériques, et

- lorsque l'identifiant lu sur le disque sécurisé correspond à l'identifiant stocké dans les moyens de mémorisation du dispositif d'accès, mise à disposition par le dispositif d'accès des données numériques de façon à autoriser un second mode d'exploitation des données numériques.

Suivant des modes particuliers de réalisation, la méthode de mise à disposition comporte l'une ou plusieurs des caractéristiques suivantes :

- lorsque les données numériques sont mises à disposition de façon à autoriser un premier mode d'exploitation des données numériques, elle comprend une étape d'embrouillage des données numériques par le dispositif d'accès selon un protocole adapté pour interdire la reproduction/copie du contenu multimédia et pour autoriser la présentation du contenu multimédia sur un dispositif de présentation appartenant au domaine spécifique uniquement pendant la lecture des données numériques par le dispositif d'accès ;

- lorsque les données numériques sont mises à disposition de façon à autoriser un second mode d'exploitation, elle comprend en outre les étapes suivantes :

- lecture par le dispositif d'accès de droits de reproduction prégravés sur le disque sécurisé ;

- lecture sur le disque sécurisé de droits de reproduction attachés au contenu multimédia, les droits de reproduction définissant si le contenu multimédia est librement reproductible/copiable, si le contenu multimédia est reproductible/copiable dans le domaine déterminé uniquement ou si le contenu multimédia n'est pas reproductible/copiable ; et

- embrouillage des données numériques par le dispositif d'accès selon un protocole défini en fonction des droits de reproduction lus sur le disque sécurisé ;

- lorsque les droits de reproduction lus autorisent la reproduction/copie du contenu multimédia dans le domaine déterminé uniquement, la méthode comprend une étape d'embrouillage des données numériques par le dispositif d'accès selon un protocole adapté pour autoriser la reproduction/copie et la présentation du contenu multimédia uniquement sur des équipements appartenant au domaine déterminé ;

- lorsque les droits de reproduction interdisent la reproduction/copie du contenu multimédia, elle comprend une étape d'embrouillage des données numériques par le dispositif d'accès selon un protocole adapté pour interdire la reproduction/copie du contenu multimédia, et autoriser uniquement la présentation du contenu multimédia sur un dispositif de présentation appartenant au domaine déterminé pendant la lecture des données numériques par le dispositif d'accès ; et

- lorsque les droits de reproduction autorisent la reproduction/copie libre du contenu multimédia, elle comprend une étape d'embrouillage des données numériques par le dispositif d'accès selon un protocole adapté pour autoriser la reproduction/copie et la présentation du contenu multimédia sur tout équipement.

L'invention concerne également, selon un troisième aspect, une méthode de distribution sécurisée de données numériques représentatives d'un contenu multimédia, comportant les étapes suivantes :

- gravure de données numériques représentatives d'un contenu multimédia sur un DVD sécurisé à partir d'un graveur, l'étape de gravure étant réalisée selon les étapes sus-mentionnées; et

- mise à disposition desdites données numériques gravées, l'étape de mise à disposition étant réalisée selon les étapes sus-mentionnées.

Suivant des modes particuliers de réalisation, la méthode de distribution sécurisée comporte l'une ou plusieurs des caractéristiques suivantes :

- une étape de transmission des droits de reproduction attachés au contenu multimédia d'un serveur à distance vers ledit graveur, l'étape de transmission étant préalable à l'étape de gravure des droits de reproduction ; et

- une étape de chiffrement de l'identifiant et des droits de reproduction, ladite étape de chiffrement étant préalable à l'étape de gravure.

L'invention concerne également, selon un quatrième aspect, un dispositif d'accès à un domaine sécurisé spécifique, le dispositif d'accès comprenant des moyens de lecture de données numériques représentatives d'un contenu multimédia gravées sur un disque sécurisé et des moyens de mémorisation d'un identifiant du domaine spécifique auquel appartient le dispositif d'accès, les moyens de lecture sont adaptés pour lire sur le disque sécurisé un identifiant d'un domaine sécurisé déterminé, et le dispositif d'accès comporte en outre :

- des moyens de comparaison de l'identifiant enregistré dans les moyens de mémorisation avec l'identifiant lu sur le disque sécurisé ; et

- des moyens adaptés pour mettre à disposition des données numériques de façon à autoriser un premier mode d'exploitation des données numériques, lorsque l'identifiant lu sur le disque sécurisé ne correspond pas à l'identifiant stocké dans les moyens de mémorisation du dispositif d'accès, et pour mettre à disposition les données numériques de façon à autoriser un second mode d'exploitation des données numériques, lorsque l'identifiant lu sur le disque sécurisé correspond à l'identifiant stocké dans les moyens de mémorisation du dispositif d'accès.

L'invention concerne également, selon un cinquième aspect, un graveur appartenant à un domaine sécurisé comprenant plusieurs équipements et défini par un identifiant propre à tous les équipement dudit domaine, le graveur étant adapté pour graver sur un disque sécurisé des données numériques représentatives d'un contenu multimédia, il est propre à graver sur le disque sécurisé l'identifiant du domaine du graveur pour définir ce domaine comme seul domaine dans lequel la reproduction/copie du contenu multimédia est autorisé.

Suivant des modes particuliers de réalisation, le graveur comporte l'une ou plusieurs des caractéristiques suivantes :

- il est propre à graver des droits de reproduction attachés à un contenu multimédia, les droits de reproduction définissant si le contenu multimédia est librement reproductible/copiable ou si le contenu multimédia est reproductible/copiable dans un domaine déterminé uniquement ou si le contenu multimédia n'est pas reproductible/copiable ; et

- les droits de reproduction attachés à un contenu multimédia comprennent le nombre de reproductions autorisées du contenu multimédia.

L'invention sera mieux comprise à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple et faite en se référant aux dessins, sur lesquels :

- la figure 1 est un schéma sous forme de bloc fonctionnel d'une partie du système permettant la mise en œuvre de la méthode de distribution selon l'invention ;

- la figure 2 est un schéma sous forme de bloc fonctionnel d'une autre partie du système permettant la mise en œuvre de la méthode de distribution selon l'invention ; et

- la figure 3 est un schéma illustrant les étapes de la méthode de distribution selon l'invention.

Le système 2 dans lequel la méthode selon l'invention est mise en œuvre est illustré sur les figures 1 et 2. Ce système 2 se rapporte à un ensemble d'équipements informatiques disposant soit d'un graveur de DVD soit d'un lecteur de DVD et appartenant à des utilisateurs différents et susceptibles d'échanger des DVDs. Les équipements étant répartis dans des domaines sécurisés différents.

Les équipements appartenant à un domaine sécurisé possèdent chacun dans une mémoire un même identifiant représentatif de ce domaine et une clé de domaine. Les équipements de ce domaine sont capables de communiquer au travers d'un réseau, des données numériques embrouillées par cette clé de domaine. Un équipement n'appartenant pas à ce domaine sécurisé ou appartenant à un autre domaine sécurisé n'est pas capable de lire les données embrouillées transitant dans ce réseau ou les données embrouillées stockées sur un équipement du réseau.

Comme visible sur la figure 1, le système 2 comporte un fournisseur de contenu 4 propre à mettre à la disposition d'un dispositif récepteur 6 des données numériques par l'intermédiaire d'un réseau de distribution 8, tel que le réseau Internet.

Le fournisseur de contenu 4 comprend un serveur multimédia 10 relié à une base de données 12.

La base de données 12 est propre à stocker des données numériques représentatives de contenus multimédias, telles que par exemple des séquences de données audios, vidéos ou textuelles ou des fichiers de données informatiques utilisés pour la mise en œuvre de logiciels.

Les données numériques sont codées sous forme de paquets, par exemple selon la norme MPEG-2 (ISO/IEC 13818-1).

Dans la base de données 12, chaque contenu multimédia est associé à un ou plusieurs usages ou droits de reproduction et à un prix variant en fonction de ces usages ou droits.

Les usages identifient le type de protection attaché à la copie ou à la reproduction du contenu multimédia. Dans l'exemple du mode de réalisation décrit, les usages définissent si le contenu multimédia est librement copiable/reproductible, s'il est copiable sur un DVD sécurisé ou s'il est à la fois copiable sur un DVD sécurisé et copiable/reproductible dans un unique domaine correspondant au domaine auquel appartient le graveur ayant gravé le contenu sur le DVD sécurisé.

Le serveur multimédia 10 comprend des moyens 14 pour envoyer ou pour recevoir des données numériques vers le réseau de distribution 8 ou depuis ce réseau, et un module d'embrouillage 16 de ces données numériques.

Le module d'embrouillage 16 est adapté pour embrouiller les données selon le système CSS.

Le dispositif récepteur 6 est un ordinateur ou un décodeur numérique (ou « set top box » en anglais). Il est généralement disposé chez un utilisateur qui désire accéder à des programmes vidéo, par l'intermédiaire du réseau de distribution 8.

Le dispositif récepteur 6 appartient à un domaine sécurisé par un système de protection tel que par exemple le système de marque déposée SmartRight.

Les équipements appartenant à ce domaine sécurisé possèdent chacun dans une mémoire un même identifiant IDD représentatif de ce domaine et une clé de domaine DIK.

Le dispositif récepteur 6 possède un processeur 18, un module de chiffrement/déchiffrement 20, une interface utilisateur 22 du type clavier, écran ou télécommande et une interface réseau 24 pour envoyer ou recevoir des données.

Le processeur 18 est propre à exécuter les protocoles du système de protection de données SmartRight ainsi que les protocoles du système de protection CSS correspondant au système de protection utilisé par le module d'embrouillage 16. A cet effet, il comprend notamment une clé maître MK et un identifiant IDD du domaine auquel le dispositif récepteur 6 appartient.

L'interface 24 est adaptée pour recevoir des flux de données du réseau de distribution 8 par téléchargement en temps réel (« streaming » en anglais), c'est-à-dire en visualisant le contenu au fur et à mesure du chargement, ou par téléchargement préalable (« downloading » en anglais) permettant une visualisation en différé du contenu.

Le dispositif récepteur 6 est relié à un graveur 28 de DVD 30 par exemple de type DVD-R, DVD-RW, DVD+R, DVD+RW ou DVD-RAM.

Le DVD 30 comprend une zone de départ 32 prégravée par un ensemble de clés disques sécurisées selon le protocole du système de protection CSS, une zone de stockage 34 et une zone 36 d'enregistrement de données numériques.

La zone de stockage 34 est une zone particulière du DVD qui peut être gravée par tout graveur. Pour un DVD du type DVD-R la zone de stockage 34 est constituée par exemple, par une zone appelée champ 2 RMD. Ce champ est défini dans le document « DVD Specifications for Recordable Disc for General, Part 1, Physical Specifications, Version 2.0, May 2000 ».

Comme visible sur la figure 2, le système 2 selon l'invention comprend en outre un lecteur de DVD 40 constituant un dispositif d'accès à un domaine sécurisé par le système de protection SmartRight. Le lecteur 40 est relié à un lecteur de carte à puce 42 destiné à recevoir une carte à puce 44.

Le lecteur 40 comporte des moyens 45 de lecture de DVD et des moyens 46 de mémorisation d'une clé maître MK' connectés à un module chiffrement/déchiffrement 48.

Le lecteur 40 comprend en outre un module d'embrouillage/ désembrouillage 50 et une interface réseau 52 pour envoyer et recevoir des données numériques par l'intermédiaire d'un réseau de distribution 54 tel que par exemple un réseau domestique, un réseau intranet ou un réseau Internet.

La carte à puce 44 contient un processeur sécurisé 56. Ce processeur 56 est adapté pour mémoriser de manière sécurisée un identifiant IDL spécifique du domaine auquel appartient le lecteur 40 et une clé de chiffrement DOK de ce domaine.

Le processeur 56 est propre à comparer des données, à recevoir et à transférer des données depuis et vers le lecteur 40, à générer des nombres aléatoires et à les encoder selon le protocole de protection SmartRight.

Le système 2 comprend en outre un dispositif de présentation 60 de type téléviseur, un graveur 62 et un équipement de stockage 64.

Le dispositif de présentation 60 et le graveur 62 comprennent chacun une interface réseau 70, 72 pour recevoir des données numériques du lecteur 40 ou rechercher des données numériques sur l'équipement de stockage 64. Ils appartiennent au même domaine sécurisé que le lecteur 40.

Le dispositif de présentation 60 comprend un module de désembrouillage 66. Il est connecté à un lecteur de carte à puce 43 recevant une carte à puce 47 stockant l'identifiant IDL et la clé de chiffrement DOK de ce domaine dans un processeur sécurisé 57.

L'équipement de stockage 64 est accessible par tout équipement connecté au réseau de distribution 54 et notamment par des équipements n'appartenant pas au domaine défini par l'identifiant IDL.

Sur la figure 3, des axes verticaux représentent l'axe du temps et les traits horizontaux illustrent les échanges entre les équipements du système représentés sur les figures 1 et 2.

Lors d'une première étape 100, un utilisateur sélectionne par l'intermédiaire de l'interface utilisateur 22 du dispositif récepteur, une séquence vidéo, par exemple un film ou une émission particulière qu'il souhaite graver sur un DVD 30.

Le graveur 28 lit l'ensemble des clés disques sécurisées gravées sur la zone du départ 32 du DVD et transmet cet ensemble de clés disques sécurisées au dispositif récepteur 6.

Le module de chiffrement/déchiffrement 20 du dispositif récepteur 6 récupère la clé disque DK à partir de cet ensemble de clés sécurisées et de la clé maître MK.

Le dispositif récepteur 6 construit alors un message de requête de contenu vidéo qu'il émet à l'adresse du serveur multimédia 10. Cette requête contient un identifiant de la séquence vidéo commandée, un identifiant du dispositif récepteur 6, la clé disque DK qui vient d'être obtenue, une indication des usages demandés ainsi qu'un ordre de paiement.

A l'étape suivante 102, le serveur multimédia 10 recherche le contenu vidéo demandé dans la base de données 12, l'embrouille à l'aide de clés titres et chiffre les clés titres à l'aide de la clé disque DK réceptionnée selon le protocole CSS.

A l'étape 104, le serveur multimédia 10 transmet au dispositif récepteur 6 le contenu vidéo embrouillé par les clés titres, les clés titres chiffrées par la clé disque DK et une indication des usages achetés par l'utilisateur.

Au cours d'une étape 106, le module de chiffrement/déchiffrement 20 du dispositif récepteur détermine et chiffre une information de domaine DI. Cette information de domaine DI comprend les usages achetés par l'utilisateur ainsi que l'identifiant IDD du domaine auquel appartient le dispositif récepteur.

Par exemple, l'information de domaine DI a la forme suivante :

DI=AES[DDK](IDD||US)

- dans laquelle AES est un standard de chiffrement (en anglais « Advanced Encryption Standard ») ;

- «|| » est un opérateur de concaténation ;

- DDK est une clé adaptée au standard de chiffrement AES, dérivée de la clé disque DK, par exemple en concaténant des '0' aux bits de poids faible de la clé DK pour obtenir une clé de la taille requise par AES ;

- IDD est l'identifiant du domaine du dispositif récepteur ;

- US est une transcription dans le format SmartRight des usages attachés au contenu vidéo.

A l'étape 108, le graveur 28 grave le contenu vidéo embrouillé sur la zone d'enregistrement de données 36 et l'information de domaine DI sur la zone de stockage 34.

Ainsi, l'utilisateur possède un DVD 30 comprenant un contenu vidéo protégé selon la spécification CSS ainsi qu'un identifiant IDD caractérisant le domaine particulier dans lequel ce contenu multimédia a été gravé et auquel le DVD est rattaché.

Au cours d'une étape 110, l'utilisateur souhaite rendre le contenu vidéo téléchargé disponible aux équipements du domaine défini par l'identifiant IDL.

A cet effet, le DVD 30 est introduit dans le lecteur 40 appartenant à ce domaine. Les moyens de lecture 45 du lecteur lisent l'ensemble des clés disques sécurisées dans la zone de départ 32 du DVD ainsi que l'information de domaine DI stockée dans la zone de stockage 34 du DVD.

Au cours d'une étape 112, le module de chiffrement/déchiffrement 48 récupère la clé disque DK à partir de l'ensemble des clés disques sécurisées et de la clé maître MK' qui est contenue dans le lecteur 40 (selon le principe de la spécification CSS). Il déduit de cette clé disque DK une clé dérivée DDK et déchiffre, à l'aide de cette clé DDK, l'information de domaine DI pour récupérer les usages US et l'identifiant IDD du domaine dans lequel le DVD 30 a été gravé.

Au cours d'une étape 114, le lecteur 40 transmet les usages US et l'identifiant IDD à la carte à puce 44.

Au cours d'une étape 116, le processeur 56 de la carte à puce vérifie si l'identifiant IDD gravé sur le DVD correspond à l'identifiant IDL qu'il mémorise.

Si l'identifiant IDD gravé sur le DVD 30 ne correspond pas à l'identifiant IDL de la carte à puce, le DVD 30 n'a pas été gravé par un graveur appartenant au même domaine que le lecteur 40.

Dans ce cas, au cours d'une étape 118, le processeur 56 de la carte à puce génère des mots de contrôle notés généralement CW (de l'anglais « Control Word ») et des messages de contrôle notés LECM (de l'anglais « Local Entitlement Control Message »). Les messages de contrôle LECM comprennent les mots de contrôle CW chiffrés de manière à n'être déchiffrable que grâce à la clé de domaine DOK, l'identifiant IDL du domaine du lecteur 40, un contrôle d'intégrité et les usages US protégés par un calcul d'intégrité. Ces messages de contrôle LECM ne peuvent être déchiffrés que par les équipements appartenant au même domaine que le lecteur 40.

Lorsque l'identifiant IDD est différent de l'identifiant IDL, les mots de contrôle CW contenus dans les messages de contrôle LECM sont surchiffrés.

Selon le protocole de protection de domaine SmartRight, des messages de contrôle LECM comprenant des mots de contrôle CW surchiffrés indiquent à tout équipement recevant ces messages de contrôle LECM et des données numériques attachées à ceux-ci que les données numériques reçues peuvent être présentées uniquement pendant la lecture du DVD et ne peuvent pas être copiées ou reproduites.

Au cours d'une étape 120, le processeur 56 de la carte à puce transmet les messages de contrôle LECM et les mots de contrôle CW générés au lecteur 40.

Au cours d'une étape 122, le module d'embrouillage/désembrouillage 50 du lecteur désembrouille les données numériques gravées sur la zone 36 du DVD à l'aide de la clé DK obtenue à l'étape 112.

Au cours d'une étape 124, le module d'embrouillage/désembrouillage 50 du lecteur embrouille les données numériques désembrouillées au cours de l'étape 122, à l'aide des mots de contrôle CW générés par le processeur 56 de la carte à puce.

Au cours d'une étape 126, le lecteur 40 transmet au dispositif de présentation 60 par l'intermédiaire du réseau de distribution 54, les données numériques embrouillées à l'aide des mots de contrôle CW ainsi que les messages de contrôle LECM générés par le processeur 56.

Au cours d'une étape 128, le processeur 57 de la carte à puce connecté au dispositif de présentation 60 déchiffre les messages de contrôle LECM et le module de désembrouillage 66 désembrouille les données numériques réceptionnées de sorte que le dispositif affiche la vidéo transmise au travers du réseau 54.

Ainsi, le dispositif de présentation 60 affiche le contenu vidéo de manière simultanée à la lecture du DVD 30 par le lecteur 40.

Le graveur 62 a également accès à ces données numériques transmises par l'intermédiaire du réseau de distribution 54. Toutefois, le graveur 62 peut, par commodité pour l'utilisateur, empêcher la reproduction ou la copie de ces données sur un DVD, car si une telle copie est effectuée, cette copie sera inutilisable car les mots de contrôle CW sont surchiffrés.

Ce mode de présentation de données numériques est connu par le protocole SmartRight sous le nom de protocole « view-only » et est décrit notamment dans le document « SmartRight Technical white paper, Version 1.7, January 2003, Thomson ».

Lorsque l'identifiant IDD est égal à l'identifiant IDL, le processeur 56 de la carte à puce analyse les usages US achetés lors de la gravure du DVD au cours d'une étape 130.

Lorsque ces usages permettent la reproduction ou la copie du contenu vidéo dans un domaine uniquement, le processeur 56 génère au cours d'une étape 132, des mots de contrôle CW et des messages de contrôle LECM contenant ces mots de contrôle CW chiffrés par la clé de domaine DOK de telle sorte que ces messages de contrôle LECM ne puissent être déchiffrés que par les équipements appartenant au même domaine que le lecteur 40, c'est-à-dire au domaine d'identifiant IDL=IDD et comprenant la clé de domaine DOK.

Au cours d'une étape 134, les messages de contrôle LECM et les mots de contrôle CW sont transmis au lecteur 40.

Au cours d'une étape 136, les données numériques lues sur le DVD sont désembrouillées selon la même méthode que la méthode décrite au cours de l'étape 122.

Au cours d'une étape 138, ces données numériques désembrouillées au cours de l'étape 136 sont embrouillées par les mots de contrôle CW générés au cours de l'étape 132.

Au cours d'une étape 140, les données numériques embrouillées et les messages de contrôle LECM sont transmis à l'équipement de stockage 64 par l'intermédiaire du réseau de distribution 54 pour y être enregistrés.

Seuls les équipements appartenant au même domaine que le lecteur 40 peuvent déchiffrer les messages de contrôle LECM et reproduire/copier ou présenter les données numériques stockées sur l'équipement 64.

Si au cours de l'étape 130, les usages analysés définissent que les données numériques sont librement copiables/reproductibles, le processeur 56 de la carte à puce génère des messages de contrôle LECM contenant des mots de contrôle non chiffrés.

Puis, les étapes 134 à 140 sont répétées. Toutefois dans ce cas, tout équipement et même les équipements qui n'appartiennent pas au domaine

d'identifiant IDD=IDL peuvent lire, présenter ou copier les données numériques, car celles-ci ne sont pas embrouillées par des clés cryptographiques sécurisées.

Si au cours de l'étape 130, le processeur 56 détermine que les données numériques ne sont pas reproductibles/copiables, alors il génère des messages de contrôle LECM et des mots de contrôle CW surchiffrés et les étapes 120 à 128 sont répétées. Dans ce cas, les données numériques seront tout de même présentables par un dispositif de présentation appartenant au domaine identifié par l'identifiant IDL.

La méthode selon l'invention peut également être implémentée dans un système de protection de domaine protégé selon la méthode de marque déposée xCP (de l'anglais: Extensible Content Protection) décrite dans les documents « xCP : eXtensible Content Protection. 2003. IBM » et « xCP Cluster Protocol, IBM Presentation to Copy Protection Technical Working Group, July 18, 2002 ».

Selon ce procédé de protection de domaine, chaque domaine ou groupe d'équipements est défini par un identifiant de groupe ID appelé « cluster ID ».

Le graveur comprend des moyens de mémorisation de l'identifiant de groupe ID et est adapté pour calculer l'information de domaine DI. Cette information DI est obtenue par application d'une fonction de hachage aux données concaténées comprenant la clé disque DK du DVD, l'identifiant de groupe ID et un indicateur de copie propre à prendre la valeur 0 ou 1 selon que cette copie soit autorisée ou non.

Le graveur est adapté pour graver l'information de domaine DI sur le DVD.

Le dispositif récepteur recevant le DVD gravé détermine si le DVD a été gravé dans son domaine en construisant sa propre information de domaine DI'. A cet effet, il reprend l'identifiant de son propre domaine, il positionne l'indicateur de copie sur une valeur correspondant à une copie autorisée et reprend la clé disque DK lue sur le DVD.

Si l'information de domaine DI du DVD et l'information de domaine DI' du dispositif récepteur ainsi construite correspondent, alors la copie est autorisée et le dispositif récepteur désembrouille puis embrouille les données numériques selon le protocole xCP de ce domaine.

Si l'information de domaine DI du DVD et l'information de domaine DI' du dispositif récepteur ainsi construite ne correspondent pas, l'opération de copie est interdite.

En variante, cette méthode de distribution sécurisée peut être utilisée avec un DVD sécurisé selon le système CPPM (de l'anglais « Content Protection for Precorded Media »), le système CPRM (de l'anglais «Content Protection for Recordable Media »), le système BD CPS pour disque à rayon bleu (de l'anglais « Blue-ray disc copy protection system) ou le système Vidi pour disque DVD+R /DVD+RW.

En variante, le graveur grave sur le DVD uniquement les données numériques et l'identifiant de domaine mais pas les usages ou droits de reproduction attachés aux données numériques. Dans ce cas, lorsque le lecteur lit un identifiant, la carte à puce génère des mots de contrôle et des messages de contrôle selon un protocole autorisant uniquement la copie/reproduction dans le domaine identifié sur le disque. Lorsque le DVD ne comprend pas d'identifiant, la carte à puce génère des mots de contrôle et des messages de contrôle surchiffrés selon un protocole empêchant la copie/reproduction par tout équipement. Dans ce cas, les données numériques sont tout de même présentables par un dispositif de présentation appartenant au domaine.

En variante, le DVD est mis dans le commerce prégravé sous une forme dans laquelle il contient des données numériques représentatives d'un contenu multimédia et des usages associés. Avant la première utilisation de ce DVD et pour que le DVD puisse être lu par un équipement, ce DVD doit être positionné dans un graveur propre à graver l'identifiant du domaine auquel le graveur appartient. Dans ce cas, le DVD ou le lecteur est conditionné pour ne fonctionner que lorsque le DVD contient un identifiant de domaine.

Avantageusement, cette méthode de distribution sécurisée autorise une certaine liberté de partage des données numériques avec des amis ou connaissance ainsi qu'un partage avec les équipements reliés au même domaine tout en protégeant les droits de propriété intellectuelles attachés à ces données numériques.

Avantageusement, les disques sécurisés sur lesquels une copie/reproduction du contenu multimédia a été gravée, sont uniquement lisibles et présentables dans le domaine défini par l'identifiant gravé sur le disque

sécurisé sur lequel la version téléchargée du contenu multimédia et l'identifiant de domaine ont été gravés. Par contre, ce dernier disque sécurisé, c'est-à-dire le disque contenant la version téléchargée du contenu multimédia et l'identifiant de domaine, peut être lu et présenté sur n'importe quel dispositif de présentation CSS autorisé dans tout domaine.

REVENDICATIONS

1. Méthode de gravure sécurisée de données numériques représentatives d'un contenu multimédia comportant une étape (108) de gravure desdites données numériques sur un disque sécurisé (30) par un graveur (28) appartenant à un domaine sécurisé déterminé comprenant plusieurs équipements et défini par un identifiant (IDD) propre à tous les équipement du domaine, caractérisée en ce qu'elle comporte en outre une étape de gravure (108) sur le disque sécurisé (30) de l'identifiant (IDD) du domaine du graveur (28) pour définir ce domaine comme seul domaine dans lequel la reproduction/copie du contenu multimédia est autorisée.

2. Méthode de gravure sécurisée selon la revendication 1, caractérisée en ce qu'elle comporte en outre une étape (108) de gravure sur le disque sécurisé (30) de droits de reproduction (US) attachés au contenu multimédia, les droits de reproduction (US) définissant si le contenu multimédia est librement reproductible/copiable, si le contenu multimédia est reproductible/copiable dans le domaine déterminé uniquement ou si le contenu multimédia n'est pas reproductible/copiable.

3. Méthode de mise à disposition sécurisée de données numériques représentatives d'un contenu multimédia dans un domaine sécurisé spécifique défini par un identifiant (IDL), à partir d'un dispositif d'accès (40,42,44) au domaine sécurisé spécifique comprenant des moyens de mémorisation (56) de l'identifiant (IDL) de ce domaine spécifique, caractérisée en ce qu'elle comporte les étapes suivantes :

- lecture (112) sur un disque sécurisé (30) comprenant lesdites données numériques d'un identifiant (IDD) d'un domaine sécurisé déterminé par le dispositif d'accès (40,42,44), l'identifiant (IDD) étant préalablement gravé sur le disque sécurisé (30) ;

- comparaison (116) de l'identifiant (IDD) lu sur le disque sécurisé (30) avec l'identifiant (IDL) stocké dans les moyens de mémorisation (56) du dispositif d'accès (40,42,44) ; et

- lorsque l'identifiant (IDD) lu sur le disque sécurisé (30) ne correspond pas à l'identifiant (IDL) stocké dans les moyens de mémorisation (56) du dispositif d'accès (40,42,44), mise à disposition (118,122,124,128) par le

dispositif d'accès (40,42,44) des données numériques de façon à autoriser un premier mode d'exploitation des données numériques, et

- lorsque l'identifiant (IDD) lu sur le disque sécurisé (30) correspond à l'identifiant (IDL) stocké dans les moyens de mémorisation (56) du dispositif d'accès (40,42,44), mise à disposition (130,132,136,138) par le dispositif d'accès (40,42,44) des données numériques de façon à autoriser un second mode d'exploitation des données numériques.

4. Méthode de mise à disposition sécurisée selon la revendication 3, caractérisée en ce que lorsque les données numériques sont mises à disposition de façon à autoriser un premier mode d'exploitation des données numériques, elle comprend une étape d'embrouillage (124) des données numériques par le dispositif d'accès (40,42,44) selon un protocole adapté pour interdire la reproduction/copie du contenu multimédia et pour autoriser la présentation du contenu multimédia sur un dispositif de présentation (60) appartenant au domaine spécifique uniquement pendant la lecture des données numériques par le dispositif d'accès (40,42,44).

5. Méthode de mise à disposition sécurisée selon l'une quelconque des revendications 3 et 4, caractérisée en ce que lorsque les données numériques sont mises à disposition de façon à autoriser un second mode d'exploitation, elle comprend en outre les étapes suivantes :

- lecture (130) par le dispositif d'accès (40,42,44) de droits de reproduction (US) prégravés sur le disque sécurisé (30) ;

- lecture (112) sur le disque sécurisé (30) de droits de reproduction (US) attachés au contenu multimédia, les droits de reproduction (US) définissant si le contenu multimédia est librement reproductible/copiable, si le contenu multimédia est reproductible/copiable dans le domaine déterminé uniquement ou si le contenu multimédia n'est pas reproductible/copiable ; et

- embrouillage (132,138) des données numériques par le dispositif d'accès (40,42,44) selon un protocole défini en fonction des droits de reproduction (US) lus sur le disque sécurisé (30).

6. Méthode de mise à disposition sécurisée selon la revendication 5, caractérisée en ce que lorsque les droits de reproduction (US) lus autorisent la reproduction/copie du contenu multimédia dans le domaine déterminé uniquement, la méthode comprend une étape (138) d'embrouillage des données

numériques par le dispositif d'accès (40,42,44) selon un protocole adapté pour autoriser la reproduction/copie et la présentation du contenu multimédia uniquement sur des équipements (60,62) appartenant au domaine déterminé.

7. Méthode de mise à disposition sécurisée selon la revendication 5, caractérisée en ce que lorsque les droits de reproduction (US) interdisent la reproduction/copie du contenu multimédia, elle comprend une étape (124) d'embrouillage des données numériques par le dispositif d'accès (40,42,44) selon un protocole adapté pour interdire la reproduction/copie du contenu multimédia, et autoriser uniquement la présentation du contenu multimédia sur un dispositif de présentation (60) appartenant au domaine déterminé pendant la lecture des données numériques par le dispositif d'accès (40,42,44).

8. Méthode de mise à disposition sécurisée selon la revendication 5, caractérisée en ce que lorsque les droits de reproduction (US) autorisent la reproduction/copie libre du contenu multimédia, elle comprend une étape d'embrouillage des données numériques par le dispositif d'accès (40,42,44) selon un protocole adapté pour autoriser la reproduction/copie et la présentation du contenu multimédia sur tout équipement (60,62,64).

9. Méthode de distribution sécurisée de données numériques représentatives d'un contenu multimédia, caractérisée en ce qu'elle comporte les étapes suivantes :

- gravure (108) de données numériques représentatives d'un contenu multimédia sur un DVD sécurisé (30) à partir d'un graveur (28), l'étape de gravure étant réalisée par la méthode de gravure selon l'une quelconque des revendications 1 à 2 ; et

- mise à disposition (118,122,124,128,130,132,136,138) desdites données numériques gravées, l'étape de mise à disposition étant réalisée selon l'une quelconque des revendications 3 à 8.

10. Méthode de distribution sécurisée selon la revendication 9, l'étape de gravure étant réalisée par la méthode de gravure selon la revendication 2, caractérisée en ce qu'elle comporte en outre une étape (104) de transmission des droits de reproduction (US) attachés au contenu multimédia d'un serveur à distance (10) vers ledit graveur (28), l'étape de transmission (104) étant préalable à l'étape (108) de gravure des droits de reproduction (US).

11. Méthode de distribution sécurisée selon la revendication 10, caractérisée en ce qu'elle comprend une étape (106) de chiffrement de l'identifiant (IDD) et des droits de reproduction (US), ladite étape de chiffrement (106) étant préalable à l'étape de gravure (108).

12. Dispositif d'accès (40,42,44) à un domaine sécurisé spécifique, le dispositif d'accès (40,42,44) comprenant des moyens (45) de lecture de données numériques représentatives d'un contenu multimédia gravées sur un disque sécurisé (30) et des moyens (56) de mémorisation d'un identifiant (IDL) du domaine spécifique auquel appartient le dispositif d'accès (40,42,44), caractérisé en ce que les moyens (45) de lecture sont adaptés pour lire sur le disque sécurisé (30) un identifiant (IDD) d'un domaine sécurisé déterminé, et en ce que le dispositif d'accès (40,42,44) comporte en outre :

- des moyens (56) de comparaison de l'identifiant (IDL) enregistré dans les moyens (56) de mémorisation avec l'identifiant (IDD) lu sur le disque sécurisé (30) ; et

- des moyens (50) adaptés pour mettre à disposition des données numériques de façon à autoriser un premier mode d'exploitation des données numériques, lorsque l'identifiant (IDD) lu sur le disque sécurisé (30) ne correspond pas à l'identifiant (IDL) stocké dans les moyens de mémorisation (56) du dispositif d'accès (40,42,44), et pour mettre à disposition les données numériques de façon à autoriser un second mode d'exploitation des données numériques, lorsque l'identifiant (IDD) lu sur le disque sécurisé (30) correspond à l'identifiant (IDL) stocké dans les moyens de mémorisation (56) du dispositif d'accès (40,42,44).

13. Graveur (28) appartenant à un domaine sécurisé comprenant plusieurs équipements et défini par un identifiant (IDD) propre à tous les équipement dudit domaine, le graveur (28) étant adapté pour graver sur un disque sécurisé (30) des données numériques représentatives d'un contenu multimédia, caractérisé en ce qu'il est propre à graver sur le disque sécurisé (30) l'identifiant (IDD) du domaine du graveur (28) pour définir ce domaine comme seul domaine dans lequel la reproduction/copie du contenu multimédia est autorisé.

14. Graveur (28) selon la revendication 13, caractérisé en ce qu'il est propre à graver des droits de reproduction (US) attachés à un contenu

multimédia, les droits de reproduction (US) définissant si le contenu multimédia est librement reproductible/copiable ou si le contenu multimédia est reproductible/copiable dans un domaine déterminé uniquement ou si le contenu multimédia n'est pas reproductible/copiable.

15. Graveur (28) selon la revendication 14, caractérisé en ce que les droits de reproduction (US) attachés à un contenu multimédia comprennent le nombre de reproductions autorisées du contenu multimédia.

THOMSON

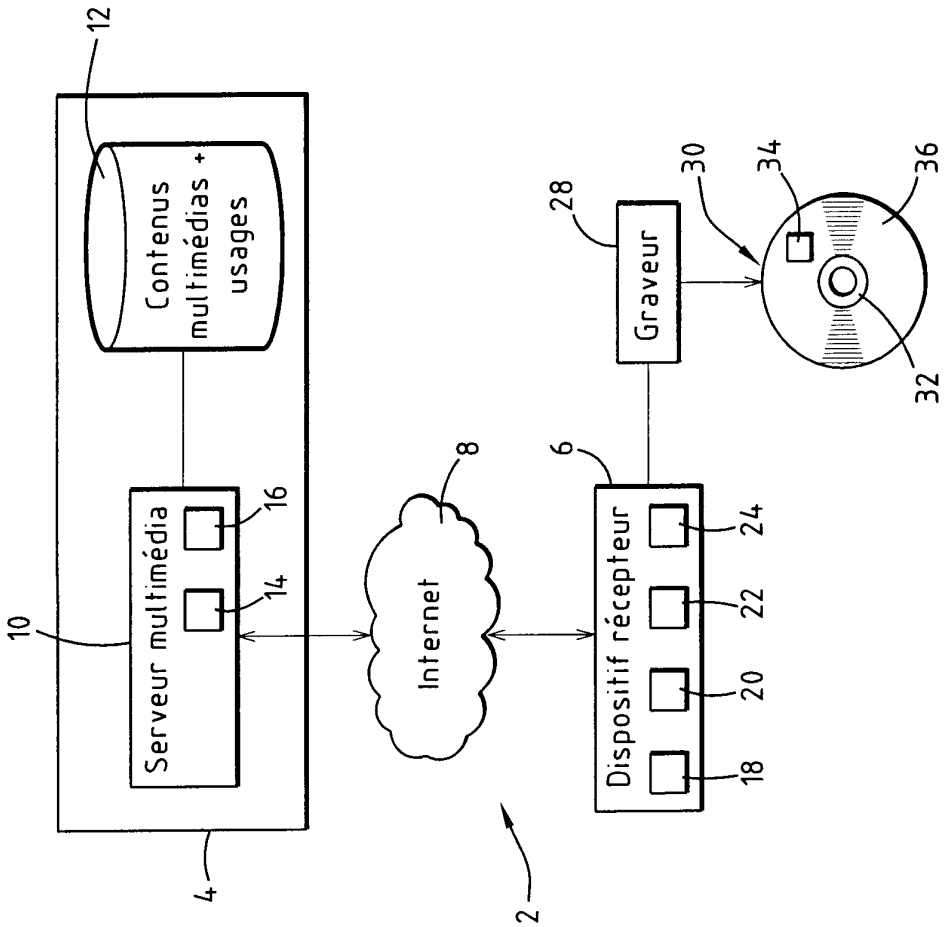


FIG.1

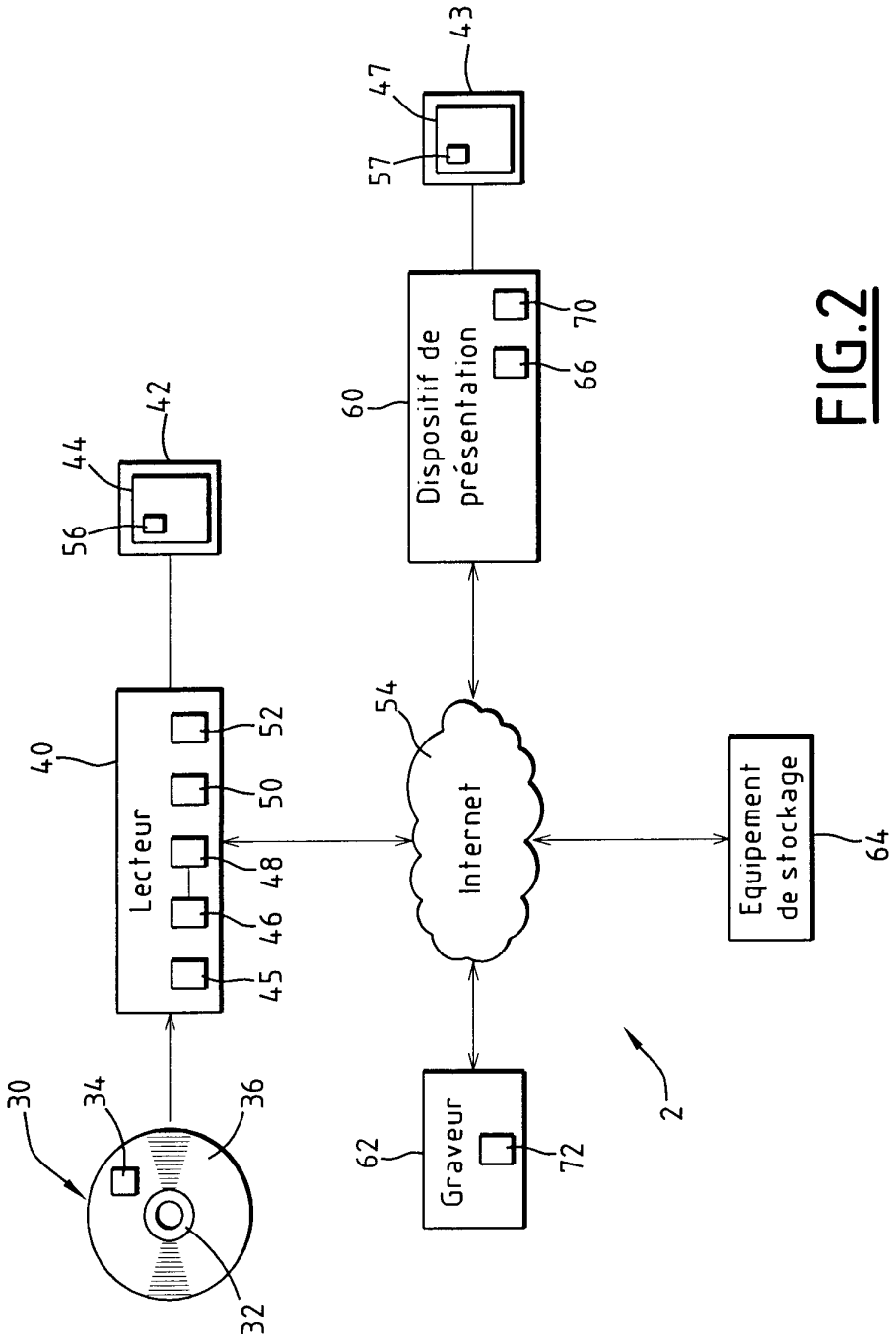

30
34
36
32
40
Lecteur
52
50
48
46
45
42
44
56
54
Internet
60
Dispositif de présentation
70
66
43
47
57
62
Graveur
72
Equipement de stockage
64
2

FIG.2

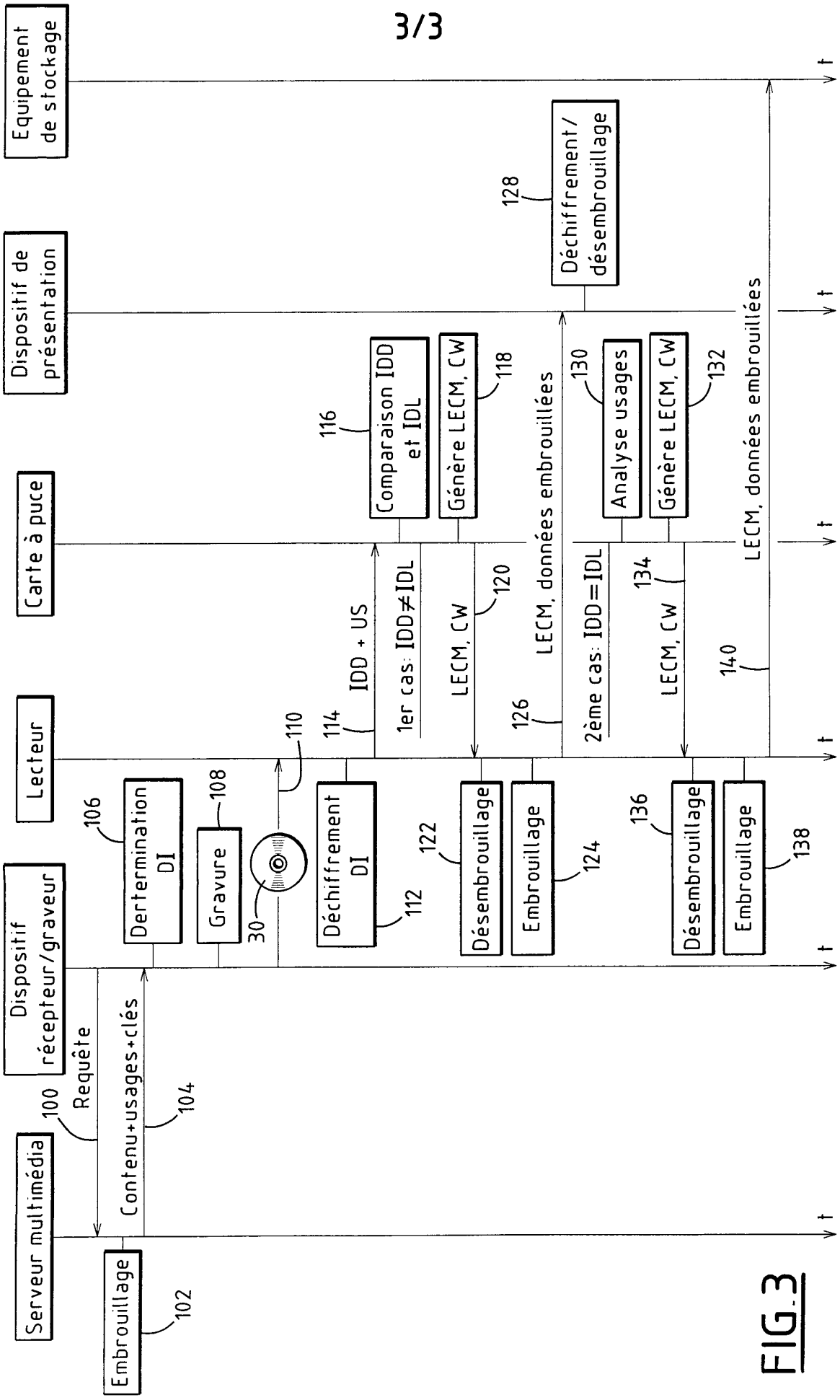

Serveur multimédia
Dispositif récepteur/graveur
Lecteur
Carte à puce
Dispositif de présentation
Equipement de stockage
Embrouillage
102
100
Requête
Contenu+usages+clés
104
Dertermination DI
106
Gravure
108
30
110
Déchiffrement DI
112
114
IDD + US
1er cas: IDD≠IDL
116
Comparaison IDD et IDL
Génère LECM, CW
118
LECM, CW
120
Désembrouillage
122
Embrouillage
124
LECM, données embrouillées
126
Déchiffrement/ désembrouillage
128
2ème cas: IDD=IDL
130
Analyse usages
Génère LECM, CW
132
134
LECM, CW
Désembrouillage
136
Embrouillage
138
140
LECM, données embrouillées
t

FIG.3

RÉPUBLIQUE FRANÇAISE

2892222

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

N° d'enregistrement national

FA 670678
FR 0510566

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		
X	FR 2 836 609 A (THOMSON LICENSING S.A) 29 août 2003 (2003-08-29) * le document en entier *	1-15	G11B20/00 G11B20/10 G06F12/14
X	US 2005/210261 A1 (KAMPERMAN FRANCISCUS LUCAS A.J ET AL) 22 septembre 2005 (2005-09-22)	1,2,13, 14	
A	* alinéas [0086], [0087] * * alinéas [0123], [0175] *	3-12,15	
X	EP 1 521 422 A (SAMSUNG ELECTRONICS CO., LTD) 6 avril 2005 (2005-04-06) * alinéas [0018], [0035] - [0037] *	1,2,13, 14	

DOMAINES TECHNIQUES RECHERCHÉS (IPC)
G11B
H04N
G06F

Date d'achèvement de la recherche	Examinateur
21 août 2006	Hermes, L

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)

ANNEXE AU RAPPORT DE RECHERCHE PRÉLIMINAIRE RELATIF A LA DEMANDE DE BREVET FRANÇAIS NO. FR 0510566 FA 670678

La présente annexe indique les membres de la famille de brevets relatifs aux documents brevets cités dans le rapport de recherche préliminaire visé ci-dessus.
Les dits membres sont contenus au fichier informatique de l'Office européen des brevets à la date du 21-08-2006
Les renseignements fournis sont donnés à titre indicatif et n'engagent pas la responsabilité de l'Office européen des brevets, ni de l'Administration française

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2836609 A	29-08-2003	AU 2003224212 A1	09-09-2003
		BR 0307779 A	07-12-2004
		CN 1640127 A	13-07-2005
		EP 1479234 A1	24-11-2004
		WO 03073761 A1	04-09-2003
		JP 2005522902 T	28-07-2005
		US 2005084109 A1	21-04-2005
US 2005210261 A1	22-09-2005	AU 2003228007 A1	02-12-2003
		CN 1656803 A	17-08-2005
		WO 03098931 A1	27-11-2003
		JP 2005526330 T	02-09-2005
EP 1521422 A	06-04-2005	CN 1604522 A	06-04-2005
		JP 2005108182 A	21-04-2005
		US 2005075986 A1	07-04-2005

EPO FORM P0465